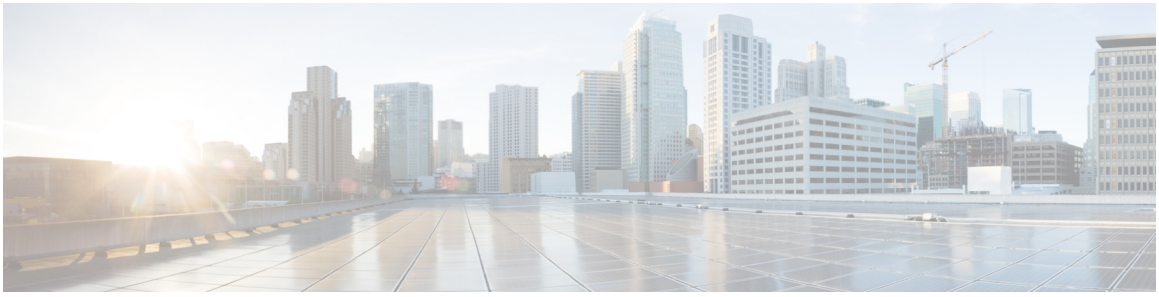
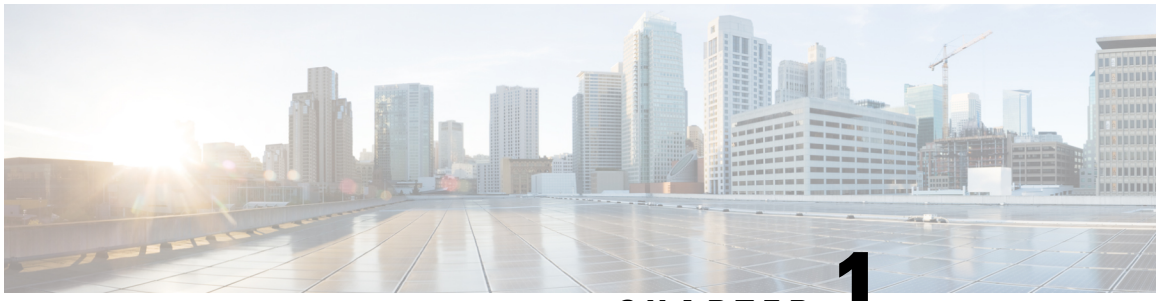
Cisco ASR 920 Series Aggregation Services Router Configuration Guide, Cisco IOS XE Everest 16.5.1

First Published: 2017-03-23

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



CONTENTS



CHAPTER 1

Getting Started With the Cisco ASR 920 Series Router

This chapter covers the following topics:

Overview

Cisco ASR 920 families of routers include :

- ASR 920-I (Indoor) [ASR-920-12CZ-A/ASR-920-12CZ-D]—This sub-family has fixed ENET interfaces (12 x 1 GE + 2 x 10GE) and dual power supplies (AC or DC).
- ASR 920-C (Compact) [ASR-920-4SZ-A/ASR-920-4SZ-D]—This sub-family of routers have a compact form factor and configurable ports: 4 x 1 GE or 4 x 10 GE or any combinations of 1 GE and 10 GE among the four ports available. In addition, there are 2 x 1 GE copper ports available.
- ASR 920-O (Outdoor) [ASR-920-10SZ-PD]—This sub-family is designed for deployment outdoors in an environment that is protected from rain and direct sunlight and provides cost optimized, and extended temperature range for business, residential, and mobile access services.
- ASR 920-F (Fixed) [ASR-920-24SZ-M/ASR-920-24TZ-M]—This sub-family with 1 RU form factor has fixed ENET interfaces (four 10GE and twenty-four 1GE Copper or SFP) and redundant modular power supplies (AC or DC).
- ASR 920-M (Modular) [ASR-920-24SZ-IM]—This sub-family with 1.5 RU form factor has fixed ENET interfaces (four 10GE and twenty-four 1GE Fiber), one modular interface, and redundant modular power supplies (AC or DC). The interface modules from ASR 900 family of routers can be leveraged for use with this model.
- ASR-920-12SZ-IM—Eight 1G copper ports, four SFP ports, and four 1G/10G Dual Rate ports one IM slot Power over Ethernet (PoE), and a global navigation satellite system (GNSS) port, with redundant AC or DC power supplies.

- ASR-920-12SZ-A/Cisco ASR-920-12SZ-D—This sub-family with 1 RU form factor has a single AC or DC fixed power supply with 12 (10G SFP+/1G SFP dual rate port) interfaces, Timing (1PPS/10MHz/ToD) interfaces, and a pluggable GNSS module.
- ASR-920-20SZ-M—This sub-family with 1 RU form factor has fixed ENET interfaces (four 10GE and twenty-four 1GE with four Copper ports) and redundant modular power supplies (AC or DC).

In addition to the 1G/10G interfaces, the Cisco ASR 920 Series Routers also have the following hardware interfaces for management, and timing and synchronization features:

- One Copper 10/100/1000Base-T LAN management port
- One BITS interface with RJ48 Connector
- One 1PPS or Time of Day port with RJ45 interface
- External Alarm interface with 4 Dry Contact Alarm inputs
- One RS-232 Console Port with USB A type connector

Note Due to the USB form factor, the flow control pins are not connected and the terminal server hosting the RS232 session must configure **no flow-control** or the console access to work correctly.

- One USB2.0 Console Port
- One USB2.0 Port for Mass Storage
- ZTP button for Zero Touch Provisioning

Caution A short press of the ZTP button starts the provisioning of the router. Pressing this button for 8 seconds or more leads to Powering off the System Power.

- Various LEDs for system and interface status
- The Cisco ASR-920-12SZ-IM Router also supports:
  - Power over Ethernet (PoE) port
  - Global navigation satellite system (GNSS) port

For more information, see the various Cisco ASR920 Series Routers hardware installation guides at http://www.cisco.com/c/en/us/support/routers/asr-920-series-aggregation-services-router/products-installation-guides-list.html.

All variants of the Cisco ASR 920 Series Router have 8MB of NOR flash, and 4GB of DRAM.

Table 1: Feature Comparison for Cisco ASR 920 Series Routers

Feature/Functionality	ASR-920-12CZ-A/D	ASR-920-4SZ-A/D	ASR-920-10SZ-PD	ASR-920-24SZ-M	ASR-920-24TZ-M	ASR-920-2
CPU operating at	P2020—1GHz	P2020—1GHz	P2020—1GHz	P2020—1.2GHz	P2020—1.2GHz	P2020—1

Feature/Functionality	ASR-920-12CZ-A/D	ASR-920-4SZ-A/D	ASR-920-10SZ-PD	ASR-920-24SZ-M	ASR-920-24TZ-M	ASR-92
DRAM	4GB	4GB	4GB	4GB	4GB	4GB
SD FLASH	2GB	2GB	2GB	2GB	2GB	2GB
1G-10G Dual Rate Ports	Supported	Supported	Supported	Not Supported	Not Supported	Not Su
BITS interface	Present	Present	Not Present	Not Present	Not Present	Preser
Time of Day port	Present	Present	Not Present	Not Present	Not Present	Preser
Auto-Media-Select Combo Port	Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Su
Copper Ports	Supported	Supported	Supported	Not Supported	Supported	Suppo
SFP Ports	Supported	Supported	Supported	Supported	Not Supported	Suppo
Smart SFP	Supported	Supported	Supported	Not Supported	Not Supported	Not Su
SFP+ Ports	Supported	Supported	Supported	Supported	Supported	Suppo
Copper SFP	Supported	Supported	Supported	Supported	Not Supported	Suppo
XFP Ports	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Suppo
ZTP Button	Supported	Supported	Supported	Not Supported	Not Supported	Not Su
PoE	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Su
GNSS	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Su

Restrictions

The Cisco ASR 920 Series Routers do not support the **hw-module** *slot/subslot* **reload** command.

Interface Naming

The following table shows the interface naming of the Cisco ASR-920-12CZ-A/ASR-920-12CZ-D ports:

1G SFP Only		1G Combo Port								10G SFP+/1G SFP[1]
1	3	5	7	9	11	5X	7X	9X	11X	13
0	2	4	6	8	10	4X	6X	8X	10X	12

[1] Ports 12 and 13 when operating in 1G Mode is operationally up only when the peer connecting interfaces are in Auto negotiation mode.

- Interfaces 0–3 are Gigabit Ethernet SFP only ports.
- Interfaces 4X–11X-Gigabit Ethernet are combo ports that support dual media—Copper and SFP. For more information, see the *Configuring Auto Media Sense on* Cisco ASR 920 Series Routers.
- Interfaces 0 to 11 are referred to as Gigabit Ethernet 0/0/0–GigabitEthernet 0/0/11 respectively.
- Interfaces 12 and 13 are dual rate ports. These ports support 1G or 10G mode depending on the optics (SFP or SFP+ respectively) installed in these ports.

Note Dual-Rate functionality is supported only with the Supported SFPs, listed in the *Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide*.

- Interfaces 12 and 13 are TenGigibitEthernet 0/0/12–TenGigabitEthernet 0/0/13. The interface name remains unchanged even if an SFP is installed in the port and the port is operating in 1G mode.
- Out of Band Management Network port is referred as interface Gig0.

The following table shows the interface naming of the Cisco ASR920-4SZ-A/ASR920-4SZ-D ports:

1G Cu Port	10G SFP+/1GSFP[2]	
1	3	5
0	2	4

[2] Ports 2, 3, 4, and 5 when operating in 1G Mode is operationally up only when the peer connecting interfaces are in Auto negotiation mode.

- Interfaces 0–1 are Copper only ports with RJ45 connector.
- Interfaces 0 and 1are referred to as Gigabit Ethernet 0/0/0–GigabitEthernet 0/0/1 respectively.
- Interfaces 2 to 5 are dual rate ports. These ports support 1G or 10G mode depending on the optics (SFP or SFP+ respectively) installed in these ports.

Note Dual-Rate functionality is supported only with the Supported SFPs, listed in the *Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide*.

- Interfaces 2 to 5 are named as TenGigibitEthernet 0/0/2–TenGigabitEthernet 0/0/5 respectively. The interface name remains unchanged even if an SFP is installed in the port and the port is operating in 1G mode.
- Out of Band Management Network port is referred as interface Gig0.

The following table shows the interface naming of the Cisco ASR-920-10SZ-PD ports:

1G Cu	1G SFP								10G SFP+	
1	-	-	-	-	-	-	-	-	-	-
0	2	3	4	5	6	7	8	9	10	11

- Interfaces 0–1 are Copper only ports with RJ45 connector.
- Interfaces 2-9 are Gigabit Ethernet SFP ports.
- Interfaces 10-11 are 10-Gigabit Ethernet SFP+ ports that support 10G mode.

The following table shows the interface naming of the Cisco ASR-920-24SZ-IM, Cisco ASR-920-24SZ-M, ASR-920-24TZ-M ports:

IM Slots (for Cisco ASR-920-24SZ-IM only)													
1G SFP/Cu[3]												10G SFP+	
1	3	5	7	9	11	13	15	17	19	21	23	25	27
0	2	4	6	8	10	12	14	16	18	20	22	24	26

[3] Ports 0 -23 are Copper ports for ASR-920-24TZ-M

- Interfaces 0–23 are Gigabit Ethernet SFP ports for ASR-920-24SZ-IM, ASR-920-24SZ-M, and Copper port for ASR-920-24TZ-M.
- Interfaces 24-27 are 10-Gigabit Ethernet SFP+ ports that support 10G mode.

The following table shows the interface naming of the Cisco ASR-920-12SZ-IM:

10G/1G SFP				1G SFP				1G Cu			
—				—				7	5	3	1
15	14	13	12	11	10	9	8	6	4	2	0

The following table shows the interface naming of the Cisco ASR-920-12SZ-A/Cisco ASR-920-12SZ-D ports:

10G SFP+/1G SFP					
1	3	5	7	9	11
0	2	4	6	8	10

- Interfaces 0–11 are dual rate ports. These ports support 1G or 10G mode depending on the optics (SFP or SFP+ respectively) installed in these ports.

The following table shows the interface naming of the Cisco ASR-920-20SZ-M ports:

1G Cu port		1G SFP port										10G SFP port	
1	3	5	7	9	11	13	15	17	19	21	23	25	27

1G Cu port		1G SFP port										10G SFP port	
0	2	4	6	8	10	12	14	16	18	20	22	24	26

- Interfaces 0–3 are Copper only ports with RJ45 connector.
- Interfaces 4-23 are Gigabit Ethernet SFP ports.
- Interfaces 24-27 are 10-Gigabit Ethernet SFP+ ports that support 10G mode.

All Interfaces with CU SFP, flap twice during router boot up. This behaviour is applicable to the following variants that support CU SFP:

- ASR-920-12CZ-A/D
- ASR-920-4SZ-A/D
- ASR-920-10SZ-PD
- ASR-920-24SZ-M
- ASR-920-24SZ-IM
- ASR-920-12SZ-IM
- ASR-920-20SZ-M

Interface Speed Based on Port Type

The following table shows the interface speed of the Cisco ASR-920-12SZ-A/Cisco ASR-920-12SZ-D:

Category	Cu Ports			SFP ports (With Fiber SFP plugged in)			SFP ports (With Copper SFP plugged in)			SFP+
Speed	**10M**	**100M**	**1G**	**10M**	**100M**	**1G**	**10M**	**100M**	**1G**	**10G**
10G Dual rate ports	NA	NA	NA	NA	NA	Yes	Not Supported	Not Supported	No	Yes

The following table shows the interface speed of the Cisco ASR-920-20SZ-M:

Category	Cu Ports			SFP ports (With Fiber SFP plugged in)			SFP ports (With Copper SFP plugged in)			SFP+
Speed	**10M**	**100M**	**1G**	**10M**	**100M**	**1G**	**10M**	**100M**	**1G**	**10G**
1G Copper /SFP ports	Yes	Yes	Yes	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Yes

Category	Cu Ports			SFP ports (With Fiber SFP plugged in)			SFP ports (With Copper SFP plugged in)			SFP+
10G Dual rate ports	NA	NA	NA	NA	NA	NA	NA	Not Supported	Not Supported	Yes

VCoP Optics Support

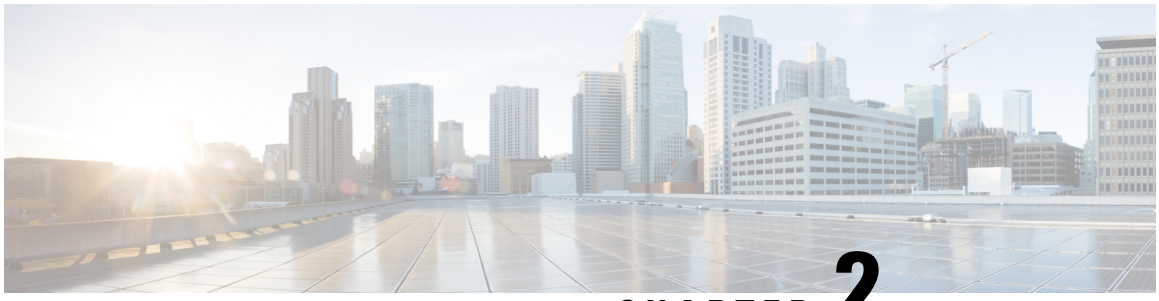
The following table indicates the GE/Dual rate ports that support VCoP optics.

Chassis	1 GE Port	Dual Rate 1 GE/10 GE port
ASR-920-10SZ-PD	3, 5, 7, and 9	NA
ASR-920-24SZ-IM[4]	1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, and 23	NA
ASR-920-12SZ-IM[5]	0 to 11	12 to 15
ASR-920-12CZ-A[6]	0, 1, 10, and 11	NA

[4] The Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M routers support a maximum of 12 VCoP smart SFPs and only on GE ports of the top row.

[5] The Cisco ASR-920-12SZ-IM router supports a maximum of 8 VCoP smart SFPs and on all GE and 10 GE ports.

[6] The Cisco ASR-920-12CZ-A/D supports a maximum of 4 VCoP smart SFPs on GE ports (0, 1, 10, and 11) with maximum ambient temperature of 65°C or it supports a maximum of 14 VCoP smart SFPs on all 12 GE + two 10 GE dual rate ports with maximum temperature of 55°C.



CHAPTER 2

Using Cisco IOS XE Software

This chapter provides information to prepare you to configure the Cisco ASR 920 Series Router:

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.

The table below 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 2: Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.
Diagnostic	The router boots up or accesses diagnostic mode in the following scenarios: • In some cases, diagnostic mode will be reached when the IOS process or processes fail. In most scenarios, however, the router will reload. • A user-configured access policy was configured using the **transport-map** command that directed the user into diagnostic mode. See the Console Port, Telnet, and SSH Handling chapter of this book for information on configuring access policies. • The router was accessed using a Route Switch Processor auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered and the router was configured to go into diagnostic mode when the break signal was received.	`Router(diag)#`	If the IOS process failing is the reason for entering diagnostic mode, the IOS problem must be resolved and the router rebooted to get out of diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI. If the router is accessed through the Route Switch Processor auxiliary port, access the router through another port. Accessing the router through the auxiliary port is not useful for customer purposes anyway.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

Accessing the CLI Using a Router Console

Note For more information about connecting cables to the router, see the *Connecting a Cisco ASR 920 Series Router to the Network* section in the Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide.

Note For information about installing USB devices drivers in order to use the USB console port, see the Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide.

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.

The table below lists the keyboard shortcuts for entering and editing commands.

Table 3: Keyboard Shortcuts

Keystrokes	Purpose
Ctrl-B or the **Left Arrow** key[7]	Move the cursor back one character
Ctrl-F orthe **Right Arrow** key1	Move the cursor forward one character
Ctrl-A	Move the cursor to the beginning of the command line
Ctrl-E	Move the cursor to the end of the command line
Esc B	Move the cursor back one word
Esc F	Move the cursor forward one word

[7] 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.

The table below lists the history substitution commands.

Table 4: History Substitution Commands

Command	Purpose
Ctrl-P or the **Up Arrow** key[8]	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the **Down Arrow** key1	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the **Up Arrow** key.
`Router# show history`	While in EXEC mode, list the last several commands you have just entered.

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

Getting Help

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

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

Table 5: Help Commands and Purpose

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

Finding Command Options Example

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

were in global configuration mode and wanted to see all the keywords or arguments for the **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.

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

Command	Comment

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

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

`Router(config)# gigabitethernet 0/0/1`	Enter interface configuration mode by specifying the serial interface that you want to configure using the **gigabitethernet** or **tengigabitethernet** global configuration command.

Command	Comment
Router(config-if)# ? Interface configuration commands: . . . ip Interface Internet Protocol config commands keepalive Enable keepalive lan-name LAN Name command llc2 LLC2 Interface Subcommands load-interval Specify interval for load calculation for an interface locaddr-priority Assign a priority group logging Configure logging for interface loopback Configure internal loopback on an interface mac-address Manually set interface MAC address mls mls router sub/interface commands mpoa MPOA interface configuration commands mtu Set the interface Maximum Transmission Unit (MTU) netbios Use a defined NETBIOS access list or enable name-caching no Negate a command or set its defaults nrzi-encoding Enable use of NRZI encoding ntp Configure NTP . . . Router(config-if)#	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.
Router(config-if)# ip ? Interface IP configuration subcommands: access-group Specify access control for packets accounting Enable IP accounting on this interface address Set the IP address of an interface authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp DVMRP interface commands hello-interval Configures IP-EIGRP hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures IP-EIGRP hold time . . . Router(config-if)# ip	Enter the command that you want to configure for the interface. This example uses the **ip** command. Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Command	Comment

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

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

`Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?`
`secondary Make this IP address a secondary address`
`<cr>`
`Router(config-if)# ip address 172.16.0.1 255.255.255.0`
	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.
	Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**.
	A <cr> is displayed; you can press **Enter** to complete the command, or you can enter another keyword.

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

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to re-enable IP routing, use the **ip routing** command. The Cisco IOS XE 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 XE 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 920 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 920 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
asr920-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
asr920-adventerprisek9.02.01.00.122-33.XNA.bin43262 -rwx        3172   Jul 2 2008 15:40:45
 -07:00  startup-config255497216 bytes total (40186880 bytes free)
```

Example 3: Copying Startup Configuration File to a TFTP Server

```
Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_asr-1002-confg]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)
```

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

Filtering Output from the show and more Commands

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

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

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

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

```
Router# show interface | include protocol
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.

Password Recovery

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

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

Before you Begin:

Make sure that the hyperterminal has the following settings:

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

SUMMARY STEPS

1. Use the power switch to turn off the router and then turn it on again.
2. Press **Break** on the terminal keyboard within 60 seconds of power up to put the router into ROMMON. In some cases Ctrl+Break key combination can be used.
3. Type **confreg 0x2142** at the ROMMON.
4. Type **reset** at the ROMMON.

5. The router will reload and prompt for configuration.Type **no** after each setup question, or press Ctrl-C to skip the initial setup procedure.
6. Type **enable** at the Router> prompt.
7. Reset the config-register from 0x2142 to 0x2102. To do so, type the following:

DETAILED STEPS

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

Step 2 Press **Break** on the terminal keyboard within 60 seconds of power up to put the router into ROMMON. In some cases Ctrl+Break key combination can be used.

Step 3 Type **confreg 0x2142** at the ROMMON.

Example:

```
1> confreg 0x2142
1>sync
```

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

Step 4 Type **reset** at the ROMMON.

Example:

```
2> reset
```

The router reboots, but ignores the saved configuration.

Step 5 The router will reload and prompt for configuration.Type **no** after each setup question, or press Ctrl-C to skip the initial setup procedure.

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

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

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

config-register *configuration_register_setting*

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

Example:

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

Finding Support Information for Platforms and Cisco Software Images

Cisco software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco software images are included in a release.

To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or the software release notes.

Using Cisco Feature Navigator

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

Using Software Advisor

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

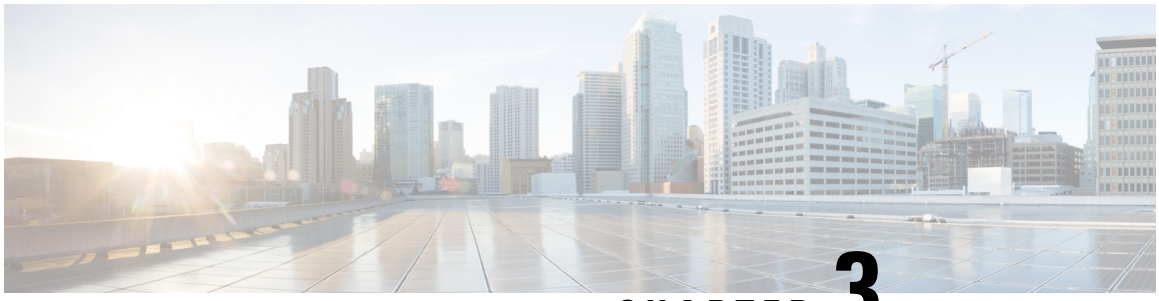
You must be a registered user on Cisco.com to access this tool.

Using Software Release Notes

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

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

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



CHAPTER 3

Using Zero Touch Provisioning

The Cisco ASR 920 Series Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, and ASR-920-10SZ-PD) provides you the option of having the router auto configure. Field technicians need only mount the router, connect to the power and attach cables in easily-accessible ports, then press the ZTP button on the front panel, to reset the router and initiate zero touch provisioning. This feature helps operators to reduce total cost of ownership (TCO) by simplifying the network deployment.

Note The Cisco ASR 920 Series Router (ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M) do not have a ZTP or Reset button.

Note Routers running ZTP must be able to connect to a DHCP server and Cisco Configuration Engine (CCE), download the configuration template, and begin operation, all at the press of a button.

Prerequisites for Using ZTP

- The Cisco ASR 920 Series Router must be running Cisco IOS-XE Release 3.13.0S or later.
- The interface connected to the CCE must be turned green.
- DHCP server should be configured to ensure reachability to the CCE and the TFTP server.
- Ports that are licensed through port licensing are disabled during the ZTP process. It is highly recommended that you connect to free ports that do not need a license to be enabled. For information on port licensing, see *Licensing 1G and 10G Ports on the Cisco ASR 920 Series Router* .

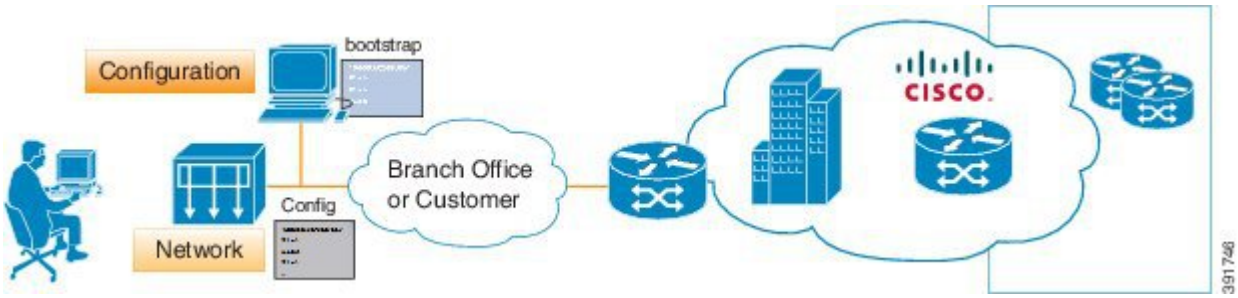
Caution Do not change the ROMMON configuration register to 0x0.

Restrictions for Using ZTP

- ZTP is not supported on the LAN Management port—Gig0 on the router. ZTP is supported only on the Ethernet interfaces such as 1—Gige, 10—Gige ports, and so on.
- ZTP is not initialized if the ZTP button is pressed for more than eight seconds. In this case, the router goes through a normal reload process.
- ZTP is also not initialized when the router is already reloading or if the router is in ROMMON prompt.
- When the ZTP process is initialized all previous logs in the buffer are cleared.
- DHCP declines addresses when loading DHCP configuration through TFTP. It is strongly recommended to have only the CNS configuration present on the configuration file to avoid tampering with the ZTP BDI.
- ZTP is not initialized if bootflash has files named as 'router-confg'.

Information About Using ZTP

Figure 1: Sample ZTP Topology



On the Cisco ASR 920 Series Routers, ZTP is triggered under any of the following conditions:

- A router without a start up configuration is powered on
- ZTP button is pressed (applicable on Cisco ASR 920 Series Router variants where the ZTP button is present on the front panel) or,
- The **write erase** and **reload** commands are executed (applicable on Cisco ASR 920 Series Router variants where the ZTP button is *not* present on the front panel)

Note The Cisco ASR 920 Series Routers (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, and ASR-920-10SZ-PD) have a ZTP button on the front panel.

The Cisco ASR 920 Series Routers (ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M) do *not* have a ZTP or Reset button.

```
Router# write erase
```

```
System configuration has been modified. Save? [yes/no]: no
Router# reload
```

Note If you type **yes** at the prompt, the system configuration is saved in the nvRAM and the ZTP process terminates.

After the ZTP process initializes, the following sequence is initiated:

1. The router detects the management VLAN and waits for any of the following data packets.
   - Broadcast (Gratuitous ARP)
   - ISIS hello packets
   - OSPF hello packets
   - IPv6 router advertisement packets
   - VRRP

Note The operations center can initiate any of the above packets over the network to establish a connection to the DHCP server.

2. When the first packet on any VLAN is detected, the router initiates a DHCP session to a DHCP server over that VLAN.
3. After a DHCP session is established, the router must establish a connection with the TFTP server through DHCP option 43 or DHCP option 150.
4. When connectivity to the TFTP server is established, the bootup process starts.

When the ZTP process initiates, the Cisco ASR 920 Series Router creates an Ethernet flow point (EFP) and associates a bridge domain interface (BDI) on the detected management VLAN.

The router creates the following configuration to establish a connection with the DHCP server and the TFTP server. The BDI created for this purpose has description **ZTP_BDI** configured under the BDI interface.

Caution Do not delete **ZTP_BDI**. Deleting this configuration results in loss of connectivity to the router and the ZTP process terminates.

Note Effective Cisco IOS-XE Release 3.14.0S, to stop the ZTP process when the ZTP button is accidentally pressed, use the **ztp disable** command in global configuration mode. However, if you long press the ZTP button, (more than 8 sec) ZTP is still initialized reload even though ZTP is disabled through the **ztp disable** command.

Example ZTP Configuration

Let us assume that GigabitEthernet0/0/1 is connected to the DHCP server and is used to connect to the CCE. VLAN ID 1000 is used as the management VLAN.

```
Router# show running-config int gi0/0/1
Building configuration...
Current configuration : 216 bytes
!
interface GigabitEthernet0/0/1
 no ip address
 media-type auto-select
 no negotiation auto
 service instance 12 ethernet
  encapsulation dot1q 1000
  rewrite ingress tag pop 1 symmetric
  bridge-domain 12
 !
end
!
interface BDI12
description ZTP_BDI
 ip address dhcp
end
```

Downloading the Initial Configuration

After the VLAN discovery process is completed, the configuration download process begins. The following sequence of events is initiated.

1. The Cisco ASR 920 Series Router sends DHCP discover requests on each Ethernet interface.
2. The DHCP server allocates and sends an IP address, TFTP address (if configured with option 150) or CE address (if configured with option 43), and default router address to the Cisco ASR 920 Series Router.
3. If the TFTP option (150) is present, the Cisco ASR 920 Series Router requests a bootstrap configuration that can be stored in any of the following files: network-confg, router-confg, ciscortr.cfg, or cisconet.cfg.
4. The bootstrap configuration (including CE IP address and port) is sent from the TFTP server to the Cisco ASR 920 Series Router.
5. An HTTP request is sent from the Cisco ASR 920 Series Router to the CE server.
6. After verification of the router's details, the CE downloads the configuration.

DHCP Server

The following is a sample configuration to set up a Cisco router as a DHCP server:

```
ip dhcp excluded-address 30.30.1.6
ip dhcp excluded-address 30.30.1.20 30.30.1.255
!
ip dhcp pool mwrdhcp
network 30.30.1.0 255.255.255.0
option 150 ip 30.30.1.6
default-router 30.30.1.6
```

This configuration creates a DHCP pool of 30.30.1.*x* addresses with 30.30.1.0 as the subnet start. The IP address of the DHCP server is 30.30.1.6. Option 150 specifies the TFTP server address. In this case, the DHCP and TFTP server are the same.

The DHCP pool can allocate from 30.30.1.1 to 30.30.1.19 with the exception of 30.30.1.6, which is the DHCP server itself.

TFTP Server

The TFTP server stores the bootstrap configuration file.

The following is a sample configuration (network– confg file):

```
hostname test-router
!
cns trusted-server all-agents 30.30.1.20
cns event 30.30.1.20 11011 keepalive 60 3
cns config initial 30.30.1.20 80
cns config partial 30.30.1.20 80
cns id hostname
cns id hostname event
cns id hostname image
cns exec 80
logging buffered 20000
!
end
```

30.30.1.20 is the IP address of the CE server and 80 is the port number of the configure service.

Cisco Configuration Engine Server

The CCE server application is installed on a Linux system. In the above example, the Cisco ASR 920 Series Router recognizes the CNS configuration and retrieves the complete configuration from the CCE server. For more information, see http://www.cisco.com/c/en/us/products/cloud-systems-management/configuration-engine/index.html

Note You need a username and password to download the CCE application. Contact ask-ce@cisco.com for credentials.

Once the application is installed and the IP addresses are set, the CCE server can be accessed on providing a username and password.

Note Ensure that the CNS ID is the hardware-serial number and that it matches with the CCE server.

ZTP LED Behavior

On Cisco ASR 920 Series Routers (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, and ASR-920-10SZ-PD):

Process	PWR LED	STAT LED
Press ZTP button	Green	Blinking Amber
Loading image	Blinking Green/Red	OFF

Process	PWR LED	STAT LED
Image loaded	Green	Green
ZTP process running	Green	Blinking Amber

On Cisco ASR 920 Series Routers (ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M), using the **write erase** and **reload** commands:

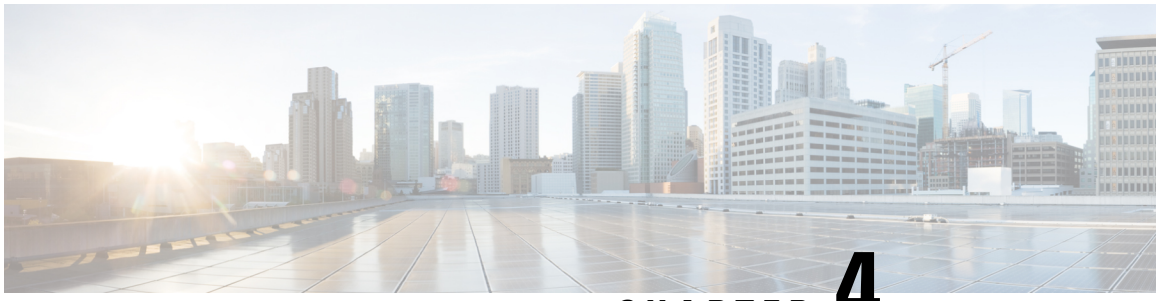
Process	PWR LED	STAT LED
Loading image	Blinking Green/Red	OFF
Image loaded	Green	Green
ZTP process running	Green	Blinking Amber

Verifying the CNS Configuration

Use the following commands to verify the CNS configuration:

On the Cisco ASR 920 Series Router:

- **show cns event connection**
- **show cns image connection**
- **show cns image inventor**



CHAPTER 4

Using Dual Rate Ports

Dual rate ports support both SFP and SFP+ optic modules.

Note Dual rate ports are not supported on Cisco ASR 920 Series Router (ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M).

See the **Supported SFP** chapter in the *Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide* .

Restrictions for Dual Port

For more information on licensing, see, *Activating Port Upgrade and Bulk Port License on Cisco ASR 920 Series Router.*

- When a dual rate port operates in 1G mode, autonegotiation is forced on the interface. For the link to be operationally up, ensure that the peer device is also configured with autonegotiation.
- If a 10G license is installed and activated for a dual rate port and an SFP is installed in that port, the interface comes up in 1G mode.
- If a 10G license is installed and activated for a dual rate port and an SFP+ is installed in that port, the interface comes up in 10G mode.
- If a 10G license is not installed for particular port but an SFP is installed on that port, the interface comes up in 1G mode.
- If sufficient 10G licenses or bulk port licenses are not available or activated for a port and an SFP+ is installed in that port, the 10G mode is not enabled and the interface will be in **link down state** . The following system warning message is displayed:

```
Warning: SFP+ inserted at port 5 tengig license not in use
```

  - However, if the 10G license is installed and activated after the insertion of the SFP+ the interface comes up in 10G mode automatically.

Note Do not issue another license command until the previous license command is processed completely. As part of the license command, multiple dual port EEM scripts will be running. These scripts, in turn, copy the port configuration. After executing completely, the previous configuration is restored. However, if you change the port configuration while the command is still executing, changes will not be in effect.

- If an activated 10G license is uninstalled or deactivated for a port with SFP+, the interface is initialized to 1G mode and 10G interfaces is administratively down.
- Dual rate interfaces in 1G mode cannot be bundled with another 1G port under a port channel interface. However, two dual rate interfaces of the same bandwidth can be bundled together. For example,
  - Interface Te0/0/11 and Interface Gig0/0/3 cannot be bundled in a port channel interface even if interface Te 0/0/11 is operating in 1G mode
  - Interface Te0/0/11 and Interface Te0/0/12 can be bundled together under a port channel interface provided they have the same bandwidth (1G or 10G).
- After changing an SFP on a dual rate port, you must wait for approximately three minutes before inserting another SFP in that port.
- In case of ASR-920-10SZ-PD and ASR-920-12CZ-A:
  - The maximum default VTY lines supported by Cisco IOS XE is 5, and atleast 2 VTY (VTY 0 and 1) lines must be kept free for the dual rate EEM script to work as stated in the general EEM configuration guidelines at *Embedded Event Manager Configuration Guide*.
- In case of ASR-920-4SZ-D and ASR-920-12SZ-IM:
  - The maximum default VTY lines supported by Cisco IOS XE is 5, and atleast 4 VTY lines must be kept free for the dual rate EEM script to work as stated in the general EEM configuration guidelines at *Embedded Event Manager Configuration Guide*.

    Note Ensure that the VTY used for the dual rate EEM script is not used by any other transport protocols such as SSH, Telnet.

    If AAA is configured on the VTY used by the dual rate EEM script, then it might take time to authorize each command, thus causing timeout issues.

    If more than 5 VTYs are required, you can increase the number of VTY lines by running the **vty line 0** n command where range 0 to n represents the total number of VTY lines permitted on the router.
  - Copper SFPs are not supported in dual rate ports for ASR920-12SZ-IM.
- Dual rate EEM script triggers DHCP renegotiation. The **dualrate_eem_policy.tcl** script is triggered when there is a 10G to 1G optics change or vice versa in a dual rate front panel interface.

Prerequisites for Dual Port

When a dual rate port operates in 1G mode, auto negotiation is forced on the interface. For the link to be operationally up, ensure that the peer device is also configured with auto negotiation.

Whenever there is a physical swap of optics from 1G to 10G or vice-versa on Cisco ASR 920 Series Routers (ASR-920-12CZ-A, ASR-920-4SZ-A, ASR-920-12SZ-IM, and ASR-920-10SZ-PD), a system internal EEM script is triggered to program the hardware registers. However configuration such as AAA/TACACS can cause the EEM script (dualrate_eem_policy) to timeout with following error.

```
%HA_EM-6-LOG: Mandatory.dualrate_eem_policy.tcl: 1Process Forced Exit- MAXRUN timer expired
```

Ensure the following procedure for the devices that are configured with AAA authentication for their VTY access:

1. AAA or TACACS server must authenticate the devices by ensuring:
    1. the reachability
    2. the correct username credentials configured for EEM (*refer point-3 below*)

Note If the mentioned criteria fails, then the EEM script prompts MAXRUN Timeout Error.

2. Avoid MAXRUN timeout error by bypassing the authorization.
    1. Unconfigure the current policy using the following command.

       ```
       no event manager policy Mandatory.dualrate_eem_policy.tcl type system
       ```

    2. Reconfigure the policy with Authorization bypass using the following command.

       ```
       event manager policy Mandatory.dualrate_eem_policy.tcl type system authorization bypass
       ```

3. Ensure correct authorization of EEM with TACACS.

   Ensure EEM script can pick the username from the following command.

   ```
   event manager session cli username <Username privilege 15>
   ```

   Example:

   ```
   event manager session cli username Cisco_user1 privilege 15
   ```

   The matching username (here, *Cisco_user1*) should be configured in TACACS.

Information About Dual Port

This feature offers the flexibility of retaining the existing 1G connections, and upgrading to a 10G connection by installing the SFP+ modules when required. For more information, see Restrictions .

The router can detect the removal of an SFP and an insertion of an SFP+ module, or the removal of an SFP+ and an insertion of an SFP module, and trigger mode change events in the system. Depending on the event type, the events generate the following messages:

```
%IOSXE_SPA-6-DUAL_RATE_CHANGE: TenGigabitEthernet0/0/13: MODE_10G
%IOSXE_SPA-6-DUAL_RATE_CHANGE: TenGigabitEthernet0/0/13: MODE_1G
```

The above events in turn, trigger the following actions:

- Current running configuration is saved to a temporary file on the bootflash: on the router.

Note Ensure that at least 10MB of free space is available on the bootflash:, else the script and dual rate functionality itself may fail.

- Configurations are changed to default values on the interface.
- Interface is shut down.
- Running configuration (stored in bootflash:) is re-applied.
- If the interface was previously in administratively up state, it is brought up.
- If the running configuration was the same as the start up configuration, the configuration is saved after the OIR of the SFP/SFP+.

Note It is highly recommended that you wait for the interfaces to be administratively up before performing a subsequent OIR.

Note Features such as, QoS that rely on the bandwidth of the interface for service policy configuration may need to be reconfigured as the previously-configured service policy may no longer be applicable. Perform a careful verification of such features and consider reconfiguring them as required.

Note Since the configuration are reapplied on detection of change of SFP type, depending on the size of the configuration on the router, the reapplication of configuration may take some time. It is recommended that you wait for 60 seconds before verifying the configuration.

Use the following command to debug failures and collect EEM debug logs:

debug event manager tcl cli_lib

Verifying the Interface Mode

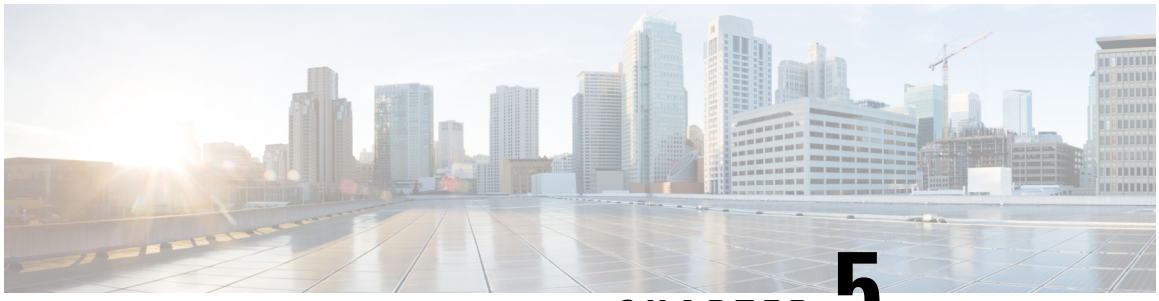
To verify the mode change (1G/10G), interface speed and media type inserted, run the following command:

```
Router# show interface tenGigabitEthernet 0/0/5

TenGigabitEthernet0/0/5 is up, line protocol is up
  Hardware is 2xGE-4x10GE-FIXED, address is badb.adba.fb85 (bia badb.adba.fb85)
  Internet address is 10.1.3.1/24
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 10000Mbps, link type is force-up, media type is 10GBase-SR
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:13:56, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo


Router# show interface GigabitEthernet 0/0/7
TenGigabitEthernet0/0/5 is up, line protocol is up
  Hardware is 2xGE-4x10GE-FIXED, address is badb.adba.fb85 (bia badb.adba.fb85)
  Internet address is 10.1.3.1/24
  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 force-up, media type is ZX
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:13:56, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```



CHAPTER 5

Console Port, Telnet, and SSH Handling

Console Port Overview

The console port on the 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 router.

For information on accessing the router using the console port, see the Cisco ASR 920 Hardware Installation Guide.

Connecting Console Cables

For information about connecting console cables to the Cisco ASR 920 Series Router, see the *ASR 920 Series Aggregartion Services Router 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 *ASR 920 Series Aggregartion Services Router Hardware Installation Guide*.

Console Port Handling Overview

Users using the console port to access the router are automatically directed to the IOS XE 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 XE command-line interface, the user is directed into diagnostic mode by default if the non-RPIOS sub-packages can be accessed.

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

Telnet and SSH Overview

Telnet and Secure Shell (SSH) on the router can be configured and handled like Telnet and SSH on other Cisco platforms. For information on traditional Telnet, see the **line** command in the *Cisco IOS Terminal Services Command Reference guide* located at http://www.cisco.com/en/US/docs/ios/12_2/termserv/command/reference/trflosho.html#wp1029818.

For information on configuring traditional SSH, see the *Secure Shell Configuration Guide*.

The router also supports persistent Telnet. Persistent Telnet allows 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 provides 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 XE process has failed.

Persistent Telnet

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 router that is not using persistent Telnet, the only method of accessing the router is through the console port.

With persistent Telnet 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 introduces the ability to access the router via diagnostic mode when the IOS process is not active.

Configuring a Console Port Transport Map

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type console** *transport-map-name* **Example:** `Router(config)# transport-map type console consolehandler`	Creates and names a transport map for handling console connections, and enter transport map configuration mode.
Step 4	**connection wait** [**allow interruptible**	**none**] **Example:** `Router(config-tmap)# connection wait none` **Example:**	Specifies how a console connection will be handled using this transport map: • **allow interruptible**—The console connection waits for an IOS vty line to become available, and also allows user to enter diagnostic mode by interrupting a console connection waiting for the IOS vty line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The console connection immediately enters diagnostic mode.

Step 5	banner [diagnostic	wait] banner-message
		Example:
		`Router(config-tmap)# banner diagnostic X`
		`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 console transport map configuration.
			• **diagnostic**—Creates a banner message seen by users directed into diagnostic mode as a result of the console transport map configuration.

	Command or Action	Purpose
		• **wait**—Creates a banner message seen by users waiting for the IOS vty to become available. • *banner-message*—The banner message, which begins and ends with the same delimiting character.
Step 6	exit **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	**transport type console** *console-line-number* **input** *transport-map-name* **Example:** `Router(config)# transport type console 0 input consolehandler`	Applies the settings defined in the transport map to the console interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** comm and.

Examples

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

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

Configuring Persistent Telnet

This task describes how to configure persistent Telnet on the router.

Before you begin

For a persistent Telnet connection to access an IOS vty line on the 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. **enable**
2. **configure terminal**

3. **transport-map type persistent telnet** *transport-map-name*
4. **connection wait** [**allow** {**interruptible**}| **none** {**disconnect**}]
5. banner [diagnostic | wait] banner-message
6. **transport interface gigabitethernet 0**
7. exit
8. transport type persistent telnet input *transport-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type persistent telnet** *transport-map-name* **Example:** `Router(config)# transport-map type persistent telnet telnethandler`	Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** {**interruptible**}| **none** {**disconnect**}] **Example:** `Router(config-tmap)# connection wait none`	Specifies how a persistent Telnet connection will be handled using this transport map: • **allow**—The Telnet connection waits for an IOS vty line to become available, and exits the router if interrupted. • **allow interruptible**—The Telnet connection waits for the IOS vty line to become available, and also allows user to enter diagnostic mode by interrupting a Telnet connection waiting for the IOS vty line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The Telnet connection immediately enters diagnostic mode. • **none disconnect**—The Telnet connection does not wait for the IOS vty line and does not enter diagnostic mode, so all Telnet connections are rejected if no vty line is immediately available in IOS.

	Command or Action	Purpose

Step 5	banner [diagnostic | wait] banner-message
	Example:
	`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.
		• **diagnostic**—creates a banner message seen by users directed into diagnostic mode as a result of the persistent Telnet configuration.
		• **wait**—creates a banner message seen by users waiting for the vty line to become available.
		• *banner-message*—the banner message, which begins and ends with the same delimiting character.

Step 6	**transport interface gigabitethernet 0** **Example:** `Router(config-tmap)# transport interface gigabitethernet 0`	Applies the transport map settings to the Management Ethernet interface (interface gigabitethernet 0). Persistent Telnet can only be applied to the Management Ethernet interface on the router. This step must be taken before applying the transport map to the Management Ethernet interface.
Step 7	exit **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 8	transport type persistent telnet input *transport-map-name* **Example:** `Router(config)# transport type persistent telnet input telnethandler`	Applies the settings defined in the transport map to the Management Ethernet interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type persistent telnet** comm and.

Examples

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

A diagnostic and a wait banner are also configured.

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

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

```
--Waiting for IOS Process-- X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

Viewing Console Port, SSH, and Telnet Handling Configurations

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

In the following example, a console port 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

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 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

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 :
```

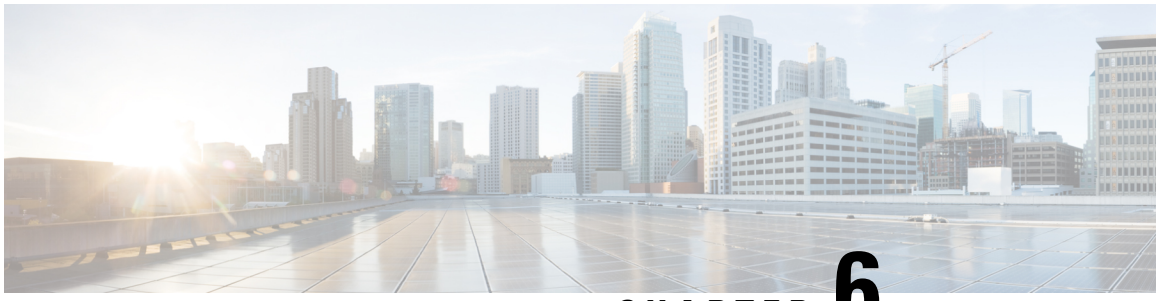
The **show platform software configuration access policy** output is given both before the new transport map is enabled and after the transport map is enabled so the changes to the SSH configuration are illustrated in the output.

```
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 :
```

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.
- Applying a transport map to a Management Ethernet interface with active Telnet or SSH sessions can disconnect the active sessions. Removing a transport map from an interface, however, does not disconnect any active Telnet or SSH sessions.
- Configuring the diagnostic and wait banners i s optional but recommended. The banners are especially useful as indicators to users of the status of their Telnet or SSH attempts.



CHAPTER 6

Using the Management Ethernet Interface

The Cisco ASR 920 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 Cisco ASR 920 Series Router has a Management Ethernet interface.
- 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, on page 44.

Gigabit Ethernet Port Numbering

The Gigabit Ethernet Management port is always GigabitEthernet0.

The port can be accessed in configuration mode like any other port on the Cisco ASR 920 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 920 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 920 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.

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 920 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 920 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.

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
```

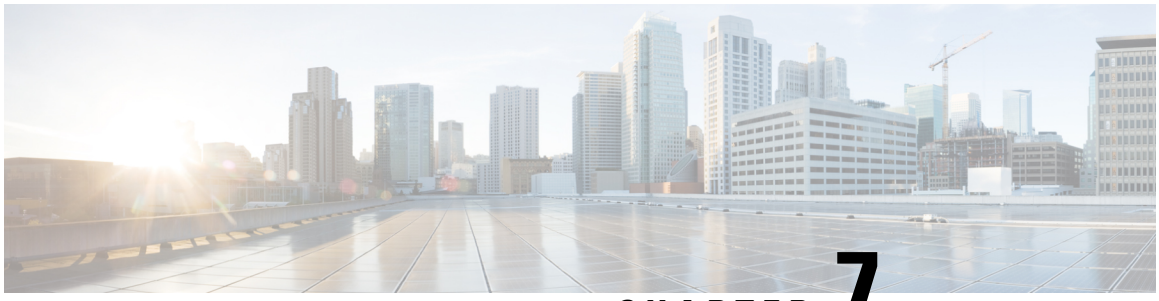
Tacacs+ Server Group Example

```
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
```



CHAPTER 7

Out of Band Management Through USB Modem

Effective Cisco IOS XE Release 3.15.0S, the Cisco ASR 920 Series Router provides out-of-band connectivity to manage remotely-deployed cell site routers using the 3G or 4G cellular network through the USB modem (also called the dongle). This OOB connectivity gives the service providers the ability to securely manage their remote cell site routers at anytime from anywhere. This feature also eliminates the need for the onsite or remote IT staff to handle outages.

Out of Band Management feature is not supported in Cisco IOS XE Everest 16.5.1.

Prerequisites for the OOB Management Through USB Modem

- The Local Mobility Anchor (LMA) must be a Cisco ASR 1000 Series Router.
- The Mobile Access Gateway (MAG) must be the Cisco ASR 920 Series Router (ASR-920-12CZ-A/D, ASR-920-4SZ-A/D, or ASR 920-10SZ-PD).
- The dongle can be inserted only in the USB Memory port of the Cisco ASR 920 Series Router.

Restrictions for the OOB Management Through USB Modem

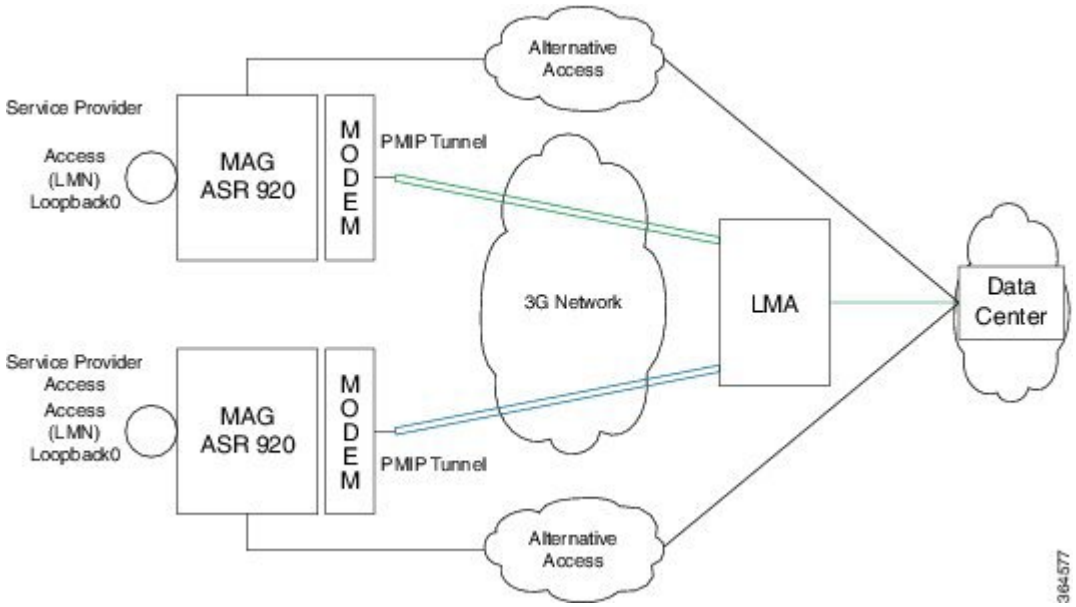
For Cisco IOS-XE Release 3.15.0S:

- Multi-VRF is not supported on the Cisco ASR 1000 Series Router.
- Only UDP PMIPv6 tunnels are supported between the LMA and MAG.
- Only the following dongle are supported:
  - Reliance (ZTE: model- AC2739)
  - Airtel 4G (Huawei: model-E3272)
  - TATA DoCoMo (ZTE: model-MF190)
- OOB Management using USB Modem works only when the advancemetroipaccess license is enabled.

- Starting from Cisco IOS-XE 3.15.0S release, you cannot configure or remove an virtual interface, virtualPPP-4001, manually.

Information About the OOB Management Through USB Modem

Figure 2: Sample Topology for OOB Management



Note By default, the management interface remains in administratively down state until the dongle in inserted and the feature is enabled.

In the above topology, the LMA assigns an IP address to the LMN. The USB modem receives its IP address from the Service Provider. A UDP tunnel is established between the LMA and MAG through the proxy mobile IPv6 (PMIPv6) protocol.

- Proxy Mobile IPv6 technology—Provides network-based IP mobility management to a mobile node without requiring the participation of the mobile node in any mobility-related signaling. The network is responsible for managing IP mobility on behalf of the host.
- MAG—Manages mobility-related signaling for a mobile node attached to its access link. It is the first layer 3 attachment node for the mobile clients.

The major functions of MAG are:

-
  - Assigning an IP address to the loopback address given by the LMA (when LMA assigns an IP address dynamically)
  - Assigning an IP address to the loopback address and sending an update to LMA (in case of static IP address)
  - Tunneling the traffic to the corresponding LMA.
- LMA—is the topological anchor point for the MAG

The LMA is responsible for assigning addresses to MAG and managing it.

In Cisco IOS-XE 3.15.0S, LMA is hosted on the Cisco ASR1000 Series Router.

Configuring the Management Interface on the MAG

SUMMARY STEPS

1. **platform usb modem** *username password*
2. **interface loopback** *loopback-id*
3. **ip route** *prefix mask* {*ip-address*} **virtualPPP-4001**
4. **exit**
5. ipv6 unicast-routing
6. **ipv6 mobile pmipv6-domain** *domain-name*
7. **encap udptunnel**
8. **lma** *lma-id*
9. **ipv4-address** *ip-address*
10. **exit**
11. **nai** *user@realm*
12. **lma** *lma-id*
13. **ipv6 mobile pmipv6-mag** *mag-id* **domain** *domain-name*
14. address {ipv4 ipv4-address | ipv6 ipv6-address | dynamic}
15. **roaming interface** *type number* **priority** *priority-value* **egress-att** *access-tech-type* **label** *egress-label*
16. **interface loopback** *loopback-id*
17. **interface GigabitEthernet** *slot/subslot*
18. **lma** *lma-id domain-name*
19. ipv4-address *ipv4-address*
20. **auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** *ascii-string* | **hex** *hex-string*}
21. **logical-mn** *network-access-identifier*
22. **address** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **dynamic**}
23. **home interface** *type*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**platform usb modem** *username password*	Enables the dongle on the MAG. The *username* and *password* are the mobile numbers of the dongle (without the zero prefix).
Step 2	**interface loopback** *loopback-id*	Creates an interface loopback.
Step 3	**ip route** *prefix mask* {*ip-address*} **virtualPPP-4001**	Creates a route to reach the LMA through the dongle interface (virtual pp interface).
Step 4	**exit**	Exits the interface.

	Command or Action	Purpose
Step 5	ipv6 unicast-routing	Enables IPv6 routing.
Step 6	**ipv6 mobile pmipv6-domain** *domain-name*	Configures common parameters valid across the domain—a logical grouping of the MAG and LMA. Creates a PMIPv6 domain and configures it by using the configuration from the LMA
Step 7	**encap udptunnel**	Configures the UDP tunnel encapsulation between the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA).
Step 8	**lma** *lma-id*	Configures an LMA within the PMIPv6 domain and enters PMIPv6 domain LMA configuration mode.
Step 9	**ipv4-address** *ip-address*	Configures an IPv4 address for the LMA within the PMIPv6 domain.
Step 10	**exit**	Exits the interface
Step 11	**nai** *user@realm*	Configures a network access identifier (NAI) for the mobile node (MN) within the PMIPv6 domain and enters PMIPv6 domain mobile node configuration mode.
Step 12	**lma** *lma-id*	Configures an LMA for the MN.
Step 13	**ipv6 mobile pmipv6-mag** *mag-id* **domain** *domain-name*	Enables the MAG service on the dongle, configures the PMIPv6 domain for the MAG, and enters MAG configuration mode.
Step 14	address {ipv4 ipv4-address | ipv6 ipv6-address | dynamic}	Configures an IPv4, an IPv6, or dynamic address for a MAG or to configure an IPv4 or an IPv6 address on an LMA.
Step 15	**roaming interface** *type number* **priority** *priority-value* **egress-att** *access-tech-type* **label** *egress-label*	Specifies an interface as a roaming interface for a Mobile Access Gateway (MAG) and set its parameters
Step 16	**interface loopback** *loopback-id*	Creates an interface loopback.
Step 17	**interface GigabitEthernet** *slot/subslot*	The local routing ACL's are not populated, which affects the locally generated/destined data packets. This command ensures the issue does not arise.
Step 18	**lma** *lma-id domain-name*	Configures the LMA for the MAG and enters MAG-LMA configuration mode.
Step 19	ipv4-address *ipv4-address*	Configures the IPv4 address for the LMA within MAG, for the MAG with LMA, or for the LMA or MAG within the Proxy Mobile IPv6 (PMIPv6) domain.
Step 20	**auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** *ascii-string* | **hex** *hex-string*}	Configures authentication for the PMIPv6 domain.

	Command or Action	Purpose
		Note This authentication should match that at the LMA side, otherwise the UDP tunnel will not be established.
Step 21	**logical-mn** *network-access-identifier*	Enables the mobile router functionality in MAG.
Step 22	**address** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **dynamic**}	Configures an IPv4, an IPv6, or dynamic address for a MAG or LMA.
Step 23	**home interface** *type*	Enables the MAG service on the specified interface.

Configuration Example: MAG Configuration with Dynamic IP Address on Logical MN Interface

```
Router(config)# platform usb modem 1234567890
 1234567890
Router(config)# interface loopback 1
Router(config-if)# exit
Router(config)# ipv6 unicast-routing
Router(config)# ip route 0.0.0.0 0.0.0.0 Virtual-PPP4001
Router(config)# ipv6 mobile pmipv6-domain D1
Router(config-ipv6-pmipv6-domain)# encap udptunnel
Router(config-ipv6-pmipv6-domain)# lma LMA1
Router(config-ipv6-pmipv6-domain-lma)# ipv4-address 173.39.88.101
Router(config-ipv6-pmipv6-domain-lma)# exit
Router(config-ipv6-pmipv6-domain)# nai MN5@cisco.com
Router(config-ipv6-pmipv6-domain-mn)# lma LMA1
Router(config-ipv6-pmipv6-domain-mn)# exit
Router(config-ipv6-pmipv6-domain)# ipv6 mobile pmipv6-mag M1 domain D1
Router(config-ipv6-pmipv6-mag)# address dynamic
Router(config-ipv6-pmipv6mag-addr-dyn)# roaming interface Virtual-PPP4001 priority 1
egress-att 3g label etyr
Router(config-ipv6-pmipv6mag-addr-dyn)# interface loopback1
Router(config-ipv6-pmipv6mag-intf)# interface GigabitEthernet0/0/1
Router(config-ipv6-pmipv6mag-intf)# lma LMA1 D1
Router(config-ipv6-pmipv6mag-lma)# ipv4-address 173.39.88.101
Router(config-ipv6-pmipv6mag-lma)# auth-option spi 67 key ascii key1
Router(config-ipv6-pmipv6mag-lma)# logical-mn MN5@cisco.com
Router(config-ipv6-pmipv6mag-logicalmn)# address dynamic
Router(config-ipv6-pmipv6mag-logicalmn)# home interface loopback1
```

Configuration Example: MAG Configuration with Static IP Address on Logical MN Interface

```
Router(config)# platform usb modem 1234567890
 1234567890
Router(config)# interface loopback 1
Router(config-if)# ip address 10.10.10.1 255.255.255.0
Router(config-if)# exit
Router(config)# ipv6 unicast-routing
Router(config)# ip route 0.0.0.0 0.0.0.0 Virtual-PPP4001
Router(config)# ipv6 mobile pmipv6-domain D1
Router(config-ipv6-pmipv6-domain)# encap udptunnel
```

```
Router(config-ipv6-pmipv6-domain)# lma LMA1
Router(config-ipv6-pmipv6-domain-lma)# ipv4-address 173.39.88.101
Router(config-ipv6-pmipv6-domain-lma)# exit
Router(config-ipv6-pmipv6-domain)# nai MN5@cisco.com
Router(config-ipv6-pmipv6-domain-mn)# lma LMA1
Router(config-ipv6-pmipv6-domain-mn)# exit
Router(config-ipv6-pmipv6-domain)# ipv6 mobile pmipv6-mag M1 domain D1
Router(config-ipv6-pmipv6-mag)# address dynamic
Router(config-ipv6-pmipv6mag-addr-dyn)# roaming interface Virtual-PPP4001 priority 1
egress-att 3g label etyr
Router(config-ipv6-pmipv6mag-addr-dyn)# interface loopback1
Router(config-ipv6-pmipv6mag-intf)# interface GigabitEthernet0/0/1
Router(config-ipv6-pmipv6mag-intf)# lma LMA1 D1
Router(config-ipv6-pmipv6mag-lma)# ipv4-address 173.39.88.101
Router(config-ipv6-pmipv6mag-lma)# auth-option spi 67 key ascii key1
Router(config-ipv6-pmipv6mag-lma)# logical-mn MN5@cisco.com
Router(config-ipv6-pmipv6-mag-logicalmn)# home interface loopback1
```

Configuring the LMA

SUMMARY STEPS

1. **ip local pool** *pool-name low-ip-address high-ip-address*
2. **ipv6 mobile pmipv6-domain** *domain-name*
3. **auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** *ascii-string* | **hex** *hex-string*}
4. **encap udptunne**l
5. **nai** *user@realm*
6. **network** *network-name*
7. **ipv6 mobile pmipv6-lma** *lma-id* **domain** *domain-name* [**force**]
8. **address ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **dynamic**}
9. **dynamic mag learning**
10. **network** *network-name*
11. **pool ipv4** *name* **pfxlen** *length*
12. **ip route** *prefix mask interface-name*
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ip local pool** *pool-name low-ip-address high-ip-address*	Configures a pool of IP addresses from which the LMA assigns an IP address to the MAG.
Step 2	**ipv6 mobile pmipv6-domain** *domain-name*	Creates a PMIPv6 domain.
Step 3	**auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** *ascii-string* | **hex** *hex-string*}	Configures authentication for the PMIPv6 domain. **Note** This authentication should match that at the MAG side, otherwise the UDP tunnel will not be established.

	Command or Action	Purpose
Step 4	**encap udptunne**l	Configures the UDP tunnel encapsulation between the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA).
Step 5	**nai** *user@realm*	Configures a network access identifier (NAI) for the mobile node (MN) within the PMIPv6 domain and enters PMIPv6 domain mobile node configuration mode. **Note** Multiple MAGs can be added in the LMA.
Step 6	**network** *network-name*	Associates a network, to which an IPv4 or IPv6 pool can be configured, with an LMA.
Step 7	**ipv6 mobile pmipv6-lma** *lma-id* **domain** *domain-name* [**force**]	Enables the LM) service on the router and configures the Proxy Mobile IPv6 (PMIPv6) domain for the LMA.
Step 8	**address ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **dynamic**}	Configures an IPv4, an IPv6, or dynamic address for a MAG or LMA.
Step 9	**dynamic mag learning**	Enables the LMA to accept PMIPv6 signaling messages from any MAG that is not locally configured.
Step 10	**network** *network-name*	Associates a network, to which an IPv4 or IPv6 pool can be configured, with an LMA.
Step 11	**pool ipv4** *name* **pfxlen** *length*	Specifies the name of the IPv4 address pool, from which a home address is allocated to a mobile node (MN), in the LMA.
Step 12	**ip route** *prefix mask interface-name*	Creates a route to reach the MAG through the dongle interface.
Step 13	**exit**	Exits the interface.

Configuration Example

```
ip local pool v4pool 10.10.10.0 10.10.10.254
!
ipv6 mobile pmipv6-domain D1
 auth-option spi 64 key ascii 100
 encap udptunnel
 nai MN5@cisco.com
  network net1
ipv6 mobile pmipv6-lma LMA1 domain D1
 address ipv4 173.39.88.101
 dynamic mag learning
 network net1
  pool ipv4 v4pool pfxlen 24
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/2
exit
```

Verifying the Configuration

MAG Call Setup

On the MAG:

```
ASR920-MAG# show ipv6 mobile pmipv6 mag binding
Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, Nai: MN5@cisco.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: Loopback1
        [Binding][MN]: Hoa: 10.10.10.1, Att: 4, llid: MN5@cisco.com
        [Binding][MN]: HNP: 0
        [Binding][MN][LMA]: Id: LMA1
        [Binding][MN][LMA]: Lifetime: 3600
        [Binding][MN]: Yes
        [Binding][MN][PATH]: interface: Virtual-PPP4001, Label: etyr
                State: PATH_ACTIVE
                Tunnel: Tunnel0
                Refresh time: 300(sec), Refresh time Remaining: 272(sec)
----------------------------------------
```

On the LMA:

```
ASR1000-LMA# show ipv6 mobile pmipv6 lma binding
Total number of bindings: 1
----------------------------------------
[Binding][MN]: State: BCE_ACTIVE
[Binding][MN]: Domain: D1, NAI: MN5@cisco.com
[Binding][MN]: HOA: 10.10.10.1, Prefix: 24
[Binding][MN]: HNP: 0
[Binding][MN][PEER]: Default Router: 10.10.10.0
        [Binding][MN]: ATT: WLAN (4)
                [Binding][MN][PEER1]:LLID: MN5@cisco.com
                [Binding][MN][PEER1]: Id: dynamic_mag165
                [Binding][MN][PEER1]: Lifetime: 3600(sec)
                [Binding][MN][PEER1]: Lifetime Remaining: 3538(sec)
                [Binding][MN][PEER1]: Tunnel: Tunnel0
                [Binding][MN][GREKEY]: Upstream: 1, Downstream: 0
----------------------------------------
```

Note If the LMA has bindings to multiple MAGs, use the following command to view a specific MAG:**show ipv6 mobile pmipv6 LMA binding nai MN5@cisco.com**.

MAG Data Path

- To verify the dynamic tunnel created between the MAG and the LMA:

show interface tunnel *tunnel-number*

- To verify dongle interface status (virtual ppp interface) and tunnel status:

show ip interface brief

```
ASR920-MAG# show ip int brief | i Virtual-PPP4001
Virtual-PPP4001        106.216.155.17  YES unset  up                    up
ASR920-MAG# show ip int brief | i Tunnel
Tunnel0                    106.216.155.17  YES unset   up                    up
```

Note Addresses assigned to the MN should be from the local pool configured in the LMA.

- To verify dynamic route map created in MAG:

show route-map dynamic

Debug Commands

The following debugs can be used to debug the call flow information and events.

- **debug ipv6 mobile mag events**
- **debug ipv6 mobile mag info**
- **debug ipv6 mobile mag api**

To view the packet level information messages, use

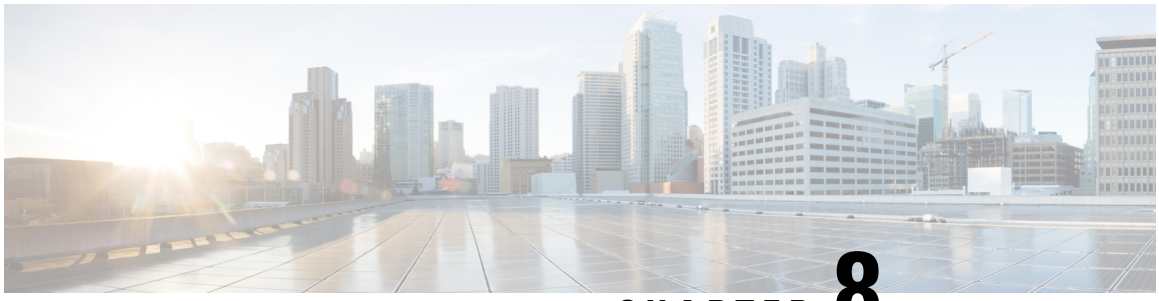
- **debug ipv6 mobile packets**

To clear the PMIPv6 bindings and statistics:

- **clear ipv6 mobile pmipv6 mag binding all**
- **clear ipv6 mobile pmipv6 mag binding nai** *MN-nai*

Related Documents

For more information on mobility commands, see the *Cisco IOS IP Mobility Command Reference*.



CHAPTER 8

Power Over Ethernet

Effective Cisco IOS XE Release 3.16S, the Cisco ASR-920-12SZ-IM Aggregation Services Router supports Power over Ethernet (PoE). PoE is the ability for any LAN switching infrastructure to provide power over a copper Ethernet cable to an endpoint or powered device.

Prerequisites for PoE

- Cisco ASR-920-12SZ-IM Aggregation Services Router supports multiple variants of power supplies. When using the AC power supplies, approximately 180 watts is used for PoE functionality, which can be shared by all eight available copper Ethernet ports.
- PoE is applicable only on the following ports: Gi0/0/0 to Gi 0/0/7
- When using DC power supplies, PoE is supported only if the input feed to the power-supply is 48 volts.

Restrictions for PoE

- Configuring a port as a static port pre-provisions power for that port. This power is deducted from the central power pool. It is, therefore, advisable to configure a port as an auto port.
- PoE does not support interface modules (IMs).
- The system allocates 180 W of static power. However, if a component or device tries to draw power over 180 W, the Cisco ASR-920-12SZ-IM Router silently reloads.

Information About PoE

The Cisco ASR-920-12SZ-IM Router uses the inline power as well as a global pool of power to power the modules, fans and other subsystems in the router. This power is alloted to all the powered devices detected on a first-come-first-serve basis. However, but if many devices are connected, and a new device is added to

the system, the system may run out of power to allot to the new device. Over-subscription of power could also result in tripping the power supplies and bringing down modules or even the entire router. In such cases, PoE can manage power allocation.

Note In the Cisco ASR-920-12SZ-IM Router, the dual power supplies function in redundant power mode.

PoE supports the following two modes of operations:

- Automatic—The automatic mode supports POE, POE+, and UPoE power negotiations up to the maximum power specified by the these different standards. UPoE is a Cisco proprietary standard, which can draw up to 60 W of power and supports LLDP negotiations. To enable UPoE mode, ensure that LLDP is not only enabled globally but also at the port level.
- Four-Pair Forced—This mode is enabled through the command line interface and can be used for third-party PoE devices that may need more than 30 Watts of power, but are not expected to have the Layer-2 power negotiation protocol, such as LLDP.

PoE License

PoE can be enabled only through the PoE license. As the PoE ports are controlled by the Port License, you must enable the PoE Port License as well as the PoE license to use this feature. Once you install the PoE license and enable the feature, the router attempts to detect and classify PoE on those PoE ports that are in ADMIN_UP state and the link state in DOWN state.

Installing the PoE License

To install or upgrade a license by using the **license install** command, you must have already received the license file from the Cisco Product License Registration portal at www.cisco.com/go/license (or you already backed up the license by using the **license save** command).

```
Router# license install bootflash:upoe.lic
Installing licenses from "bootflash:upoe.lic"
Installing...Feature:UPOE...Successful:Not Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
```

For more information on installing licenses, see Configuring the Cisco IOS Software Activation Feature.

How to Configure the PoE

SUMMARY STEPS

1. In the global config mode, select the interface to configure.
2. To determine how inline power is applied to the device on the specified port, use the power inline command:
3. If the interfaces tries to draw more power than negotiated through LLDP, the **power inline police action errdisable** command sets the port to errdisable mode.
4. Exit the configuration mode by running:

DETAILED STEPS

Step 1 In the global config mode, select the interface to configure.

Example:

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

Step 2 To determine how inline power is applied to the device on the specified port, use the power inline command:

Example:

```
Router(config-if)# power inline
```

Use one of the following options with the above command:

auto—Enables the device discovery protocol and applies power to the device, if found.

four-pair—Enables the four-pair mode.

never—Disables the device discovery protocol and stops supplying power to the device.

police—Enables inline power policing; optional if entering the no form of the command. Default is disabled.

static—High priority PoE interface. The Cisco ASR-920-12SZ-IM Router preallocates power to the interface, even when nothing is connected, guaranteeing that there will be power for the interface. You can specify the maximum wattage that is allowed on the interface using the **power inline static max value** command. If you do not specify a wattage, the switch preallocates the hardware-supported maximum value of 60 W. If the switch does not have enough power for the allocation, the command will fail, after which you must execute the **shut/no shut** command to initiate the detection of the powered device.

max—(Optional) This parameter configures the maximum power that a powered device can draw.

Step 3 If the interfaces tries to draw more power than negotiated through LLDP, the **power inline police action errdisable** command sets the port to errdisable mode.

Example:

```
Router(config-if)# power inline police action errdisable
```

Step 4 Exit the configuration mode by running:

Example:

```
Router(config-if)# end
Router(config)# end
Router#
```

Verifying the PoE Configuration

- The following is a sample output of the **show power** command:

```
Router# show power
Power Summary Maximum
```

```
(in Watts) Used Available
---------------------- ---- ---------
Inline Power 0.0 180
```

- The following is a sample output of the **show power inline** command:

```
Router# show power inline
Available:180.0(w)  Used:15.4(w)  Remaining:164.6(w)
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         15.4    Ieee PD             0     60.0
Gi0/0/1   auto   off        0.0     n/a                 n/a   60.0
Gi0/0/2   auto   off        0.0     n/a                 n/a   60.0
Gi0/0/3   auto   off        0.0     n/a                 n/a   60.0
Gi0/0/4   auto   off        0.0     n/a                 n/a   60.0
Gi0/0/5   auto   off        0.0     n/a                 n/a   60.0
Gi0/0/6   auto   off        0.0     n/a                 n/a   60.0
Gi0/0/7   auto   off        0.0     n/a                 n/a   60.0
Router# show power inline GigabitEthernet 0/0/0
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         15.4    Ieee PD             0     60.0
Router# show power inline gigabitethernet 0/0/0 detail
Interface: Gi0/0/0
Inline Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee
Police: off
Power Allocated
Admin Value: 60.0
Power drawn from the source: 0.0
Power available to the device: 0.0
Actual consumption
Measured at the port: 0.0
Maximum Power drawn by the device since powered on: 0.0
Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0
```

- The following is a sample output for port policing using the **show power inline police** commands:

```
Router# show power inline police
Available:180.0(w)  Used:15.4(w)  Remaining:164.6(w)
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi0/0/0   auto   on         none       n/a        n/a    0.0
Gi0/0/1   auto   off        none       n/a        n/a    n/a
Gi0/0/2   auto   off        none       n/a        n/a    n/a
Gi0/0/3   auto   off        none       n/a        n/a    n/a
Gi0/0/4   auto   off        none       n/a        n/a    n/a
Gi0/0/5   auto   off        none       n/a        n/a    n/a
Gi0/0/6   auto   off        none       n/a        n/a    n/a
Gi0/0/7   auto   off        none       n/a        n/a    n/a
--------- ------ ---------- ---------- ---------- ------ -----
Totals:                                                  0.0
```

```
Router# show power inline police GigabitEthernet 0/0/1
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi0/0/1   auto   on         errdisable ok         17.2   16.7
```

Debugging the PoE Configuration

- Use the following command to troubleshoot the PoE Configuration

```
Router# debug inline power
```

- Use the following commands to verify if the PoE license is enabled:

```
Router# show license detail
Index: 1 Feature: UPOE Version: 1.0
License Type: Permanent
License State: Active, Not in Use
License Count: Non-Counted
License Priority: Medium
Store Index: 0
Store Name: Primary License Storage
Index: 2 Feature: advancedmetroipaccess Version: 1.0
License Type: Permanent
License State: Active, Not in Use, EULA accepted
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 4 days
Period used: 0 minute 0 second
License Count: Non-Counted
License Priority: Low
Store Index: 0
Store Name: Built-In License Storage
Index: 3 Feature: metroaccess Version: 1.0
License Type: Permanent
License State: Active, Not in Use, EULA accepted
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 3 days
Period used: 0 minute 36 seconds
License Count: Non-Counted
License Priority: Low
Store Index: 2
Store Name: Built-In License Storage
Index: 4 Feature: metroipaccess Version: 1.0
License Type: Permanent
License State: Active, Not in Use, EULA accepted
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 4 days
Period used: 0 minute 0 second
License Count: Non-Counted
License Priority: Low
Store Index: 1
Store Name: Built-In License Storage
Router# show license feature
Feature name Enforcement Evaluation Subscription Enabled RightToUse
advancedmetroipaccess yes yes no no no
metroipaccess yes yes no no no
metroaccess no yes no no no
atm yes yes no no no
oc3 yes yes no no no
oc12 yes yes no no no
1588 yes yes no no no
```

```
1GEupgradelicense yes no no no no
10GEupgradelicense yes no no no no
12portGE4port10GE yes no no no no
gps yes no no no no
upoe yes no no no no
ipsec yes no no no no
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
802.3af	The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power to each device.
802.3at	The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power.

MIBs

MIB	MIBs Link
• POWER-ETHERNET-MIB • CISCO-POWER-ETHERNET-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

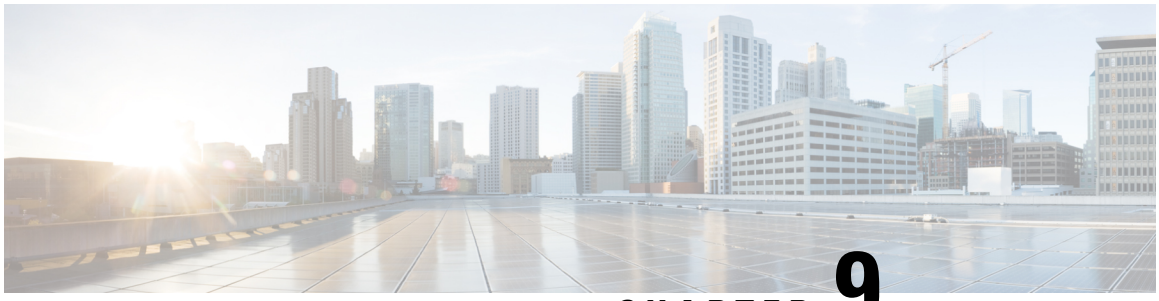
Feature Information for Power Over Ethernet

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

Note The table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 6: Feature Information for Phrase Based on Module Title

Feature Name	Releases	Feature Information
Power Over Ethernet	Cisco IOS-XE Release 3.16.0S	In this release, this feature was introduced on the Cisco ASR-920-12SZ-IM Aggregation Services Router.



CHAPTER 9

Configuring T1/E1 Interfaces

Effective Cisco IOS-XE Release 3.14.0S, the Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M Aggregation Services Router supports the following types of interface modules (IMs):

- 8x1G Cu IM (A900-IMA8T)
- 8xT1/E1 IM (A900-IMA8D)
- 1x10G IM (A900-IMA1Z)
- 2x10G IM (A900-IMA2Z)

Effective Cisco IOS-XE Release 3.16S, the Cisco ASR-920-12SZ-IM Aggregation Services Router supports the following types of interface modules (IMs):

- A900-IMA8T
- A900-IMA8S
- A900-IMA8D
- A900-IMA16D
- A900-IMA1X

This chapter provides information about configuring the T1/E1 interface module on the Cisco ASR 920 Series Router. 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 920 Series Router.

Limitations

This section describes the software limitations that apply when configuring the T1/E1 interface module on the Cisco ASR 920 Series Router.

- The Cisco ASR 920 Series Router does not support ATM and IMA on T1/E1 interface modules.
- The Cisco ASR 920 Series Router only supports the following BERT patterns: 2^11, 2^15, 2^20-O153, and 2^20-QRSS.
- When TDM is inserted in the Cisco ASR 920 Series Router, it should be activated by running the **hw-module subslot** *slot-number/subslot-number* **activate** command in EXEC mode.

This command removes the following ports from front panel and brings up the respective IMs:

- • Slots 20–23 for T1E1 IMs
  • Slot 16–23 for copper IMs

Once the TDM is activated, you must reload the router to bring up the T1/E1 interface module.

Note The above command is not required to bring up the 8X1G Cu, 1x10G and 2x10G IMs.

- To recover the front panel ports from the IMs, run the **hw-module subslot** *slot-number/subslot-number* **deactivate** command in EXEC mode.
- The above activation and deactivation commands assume that the correct IM is inserted in its corresponding slot. If an IM inserted in a different slot than what is activated, the IM does not come up and the corresponding front panel interfaces are removed.
- front panel interfaces will be removed)
- L2TPv3 encapsulation is not supported on the Cisco ASR 920 Series Router.
- CEM on access BDI in core is not supported.
- Any change in the card type requires a router reload. To change the card type, the current card type must be unconfigured, then the router must be reloaded, and then the new card type must be changed.
- The Payload calculation per unit for T1/E1 interface module is:
  - Framed E1 / T1 with no. of time slots less than 4 –> Payload = 4 x no. of time slots
  - Framed E1 / T1 with no. of timeslots greater than or equal 4 –> Payload = 2 x no. of time slots
  - Unframed T1, C11 –> Payload = 48 (2 x 24 (all slots))
  - Unframed E1, C12 –> Payload = 64 (2 x32 (all slots))
- Channelization is not supported for serial interfaces. However, channelization is supported for CEM at the DS0 level.

Note A card type change cannot be applied when the interface module is booting up. You must wait until after the interface module is administratively up.

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.

Activating the IMs

SUMMARY STEPS

1. Verify that the correct IM is inserted properly in IM slot
2. Shut down all interfaces that are active in system and which will be removed during the IM activation process.
3. Wait for a minute.
4. Default all interfaces that will be removed from the system.
5. Activate the correct IM type that is preset in the IM slot.

DETAILED STEPS

Step 1 Verify that the correct IM is inserted properly in IM slot

Step 2 Shut down all interfaces that are active in system and which will be removed during the IM activation process.

- Slots 20–23 for T1E1 IMs
- Slot 16–23 for copper IMs

Step 3 Wait for a minute.

Step 4 Default all interfaces that will be removed from the system.

Step 5 Activate the correct IM type that is preset in the IM slot.

Deactivating the IMs

SUMMARY STEPS

1. Verify that IM is in 'OK' state.
2. Using the **no interface** *interface-name* command, remove all the Virtual Interfaces associated with the IM. These include MPLS TP tunnels, TE tunnels, BDI interface, Port-Channel interface and so on.
3. Shut down all pluggable IM interfaces in system.
4. Wait for a minute.
5. Default all pluggable IM interfaces in the system.
6. Deactivate the pluggable IMs.

DETAILED STEPS

Step 1 Verify that IM is in 'OK' state.

Step 2 Using the **no interface** *interface-name* command, remove all the Virtual Interfaces associated with the IM. These include MPLS TP tunnels, TE tunnels, BDI interface, Port-Channel interface and so on.

Step 3 Shut down all pluggable IM interfaces in system.

Step 4 Wait for a minute.

Step 5 Default all pluggable IM interfaces in the system.

Step 6 Deactivate the pluggable IMs.

Setting the Card Type

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

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

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

SUMMARY STEPS

1. Router# **configure terminal**
2. Router(config)# **card type** {**e1** | **t1**} *slot subslot*
3. Router(config)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **card type** {**e1** | **t1**} *slot subslot*	Sets the serial mode for the interface module: • t1—Specifies T1 connectivity of 1.536 Mbps. B8ZS is the default linecode for T1. • e1—Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 1.984 Mbps in framed mode and 2.048 Mbps in unframed E1 mode. • *slot subslot* —Specifies the location of the interface module.
Step 3	Router(config)# **exit**	Exits configuration mode and returns to the EXEC command interpreter prompt.

Configuring the Controller

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

SUMMARY STEPS

1. Router# **configure terminal**
2. Router(config)# **controller** {**t1** | **e1**} *slot/port*
3. Router(config-controller)# clock source {internal | line}
4. Router(config-controller)# linecode {ami | b8zs | hdb3}

5. **For T1 Controllers:**
6. **cablelength** {**long** | **short**}
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **controller** {**t1** | **e1**} *slot/port*	Selects the controller to configure and enters controller configuration mode. • t1—Specifies the T1 controller. • e1—Specifies the E1 controller. • *slot/port*—Specifies the location of the interface. **Note** The slot number is always 0 and subslot number is always 1.
Step 3	Router(config-controller)# clock source {internal | line}	Sets the clock source. **Note** The clock source is set to internal if the opposite end of the connection is set to line and the clock source is set to line if the opposite end of the connection is set to internal. • internal—Specifies that the internal clock source is used. • line—Specifies that the network clock source is used. This is the default for T1 and E1.
Step 4	Router(config-controller)# linecode {ami | b8zs | hdb3}	Selects the linecode type. • ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers. • b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for T1 controller only. This is the default for T1 lines. • hdb3—Specifies high-density binary 3 (HDB3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Step 5	**For T1 Controllers:**
	Example:
	`Router(config-controller)# framing {sf | esf}`
	Example:
	`Router(config-controller)# framing {crc4 | no-crc4}`
		For E1 Controllers:
		Selects the framing type.
		• sf—Specifies Super Frame as the T1 frame type.
		• esf—Specifies Extended Super Frame as the T1 frame type. This is the default for E1.
		• crc4—Specifies CRC4 as the E1 frame type. This is the default for E1.
		• no-crc4—Specifies no CRC4 as the E1 frame type.

	Command or Action	Purpose
Step 6	**cablelength** {**long** | **short**} **Example:** `Router(config-controller)# cablelength long`	To fine-tune the pulse of a signal at the receiver for an E1 cable, use the **cablelength** command in controller configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits configuration mode and returns to the EXEC command interpreter prompt.

Verifying Controller Configuration

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

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

Optional Configurations

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

Configuring Framing

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

SUMMARY STEPS

1. Router# **configure terminal**
2. Router(config)# **controller** {*t1* | *e1*} **slot/port**
3. **For T1 controllers**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **controller** {*t1* | *e1*} **slot/port**	Selects the controller to configure. • t1—Specifies the T1 controller. • e1—Specifies the E1 controller. • slot/port—Specifies the location of the controller. **Note** The slot number is always 0 and subslot number is always 1.

Step 3	**For T1 controllers**
	Example:
	`Router(config-controller)# framing {sf | esf}`
	Example:
	`Router(config-controller)# framing {crc4 | no-crc4}`
		For E1 controllers
		Sets the framing on the interface.
		• sf—Specifies Super Frame as the T1 frame type.
		• esf—Specifies Extended Super Frame as the T1 frame type. This is the default for T1.
		• crc4—Specifies CRC4 frame as the E1 frame type. This is the default for E1.
		• no-crc4—Specifies no CRC4 as the E1 frame type.

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

Verifying Framing Configuration

Use the show controllers command to verify the framing configuration:

```
Router# show controllers t1 0/1 brief
T1 0/1 is up.
  Applique type is A900-IMA16D
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is ESF, Line Code is B8ZS
, Clock Source is Line.
  Data in current interval (740 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

Setting an IP Address

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

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

SUMMARY STEPS

1. Router(config)# **interface serial** *slot/port*
2. Router(config-if)# ip address *address mask*
3. Router(config)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface serial** *slot/port*	Selects the interface to configure from global configuration mode. • *slot*—**Specifies the slot in which the T1/E1 interface module is installed.** • *port* —Specifies the location of the controller. The port range for T1 and E1 is 0 to 1.
Step 2	Router(config-if)# ip address *address mask*	Sets the IP address and subnet mask. • *address* —Specify the IP address. • *mask* —Specify the subnet mask.
Step 3	Router(config)# **exit**	Exits configuration mode and returns to the EXEC command interpreter prompt.

What to do next

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

Configuring Encapsulation

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

Note L2TPv3 encapsulation is not supported on theCisco ASR 920 Series Routers.

To set the encapsulation method, use the following commands:

SUMMARY STEPS

1. Router# **configure terminal**
2. Router(config)# **interface serial** *slot/port*
3. Router(config-if)# **encapsulation** *encapsulation-type* {**hdlc** | **ppp**}
4. Router(config)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **interface serial** *slot/port*	Selects the interface to configure from global configuration mode. • *slot*—**Specifies the slot in which the T1/E1 interface module is installed.** • *port* —Specifies the location of the controller. The port range for T1 and E1 is 0 to 1.
Step 3	Router(config-if)# **encapsulation** *encapsulation-type* {**hdlc** | **ppp**}	Set the encapsulation method on the interface. • hdlc—High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. • ppp—Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.
Step 4	Router(config)# **exit**	Exits configuration mode and returns to the EXEC command interpreter prompt.

Verifying Encapsulation

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

```
Router#  show  interfaces  serial
  0/1
Serial0/1 is up, line protocol is up
  Hardware is Multichannel T1
  MTU 1500 bytes, BW 1536 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC
, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
60 packets input, 8197 bytes, 0 no buffer
Received 39 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
64 packets output, 8357 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions
```

Configuring the CRC Size for T1 Interfaces

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

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

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

SUMMARY STEPS

1. Router# **configure terminal**
2. Router(config)# **interface serial** *slot/port*
3. Router(config-if)# **crc** {**16** | **32**}
4. Router(config)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **interface serial** *slot/port*	Selects the interface to configure from global configuration mode. • *slot*—**Specifies the slot in which the T1/E1 interface module is installed.** • *port* —Specifies the location of the controller. The port range for T1 and E1 is 0 to 1.
Step 3	Router(config-if)# **crc** {**16** | **32**}	Selects the CRC size in bits. • 16—16-bit CRC. This is the default. • 32—32-bit CRC. **Note** Moving from CRC 16 to 32 bit (and vice-versa) is not supported.
Step 4	Router(config)# **exit**	Exits configuration mode and returns to the EXEC command interpreter prompt.

Verifying the CRC Size

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

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

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# **copy running-config startup-config**	Writes the new configuration to NVRAM.

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

Troubleshooting E1 and T1 Controllers

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

Setting a Loopback on the E1 Controller

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

Command	Purpose
Router# **configure terminal**	Enters global configuration mode.

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

Setting a Loopback on the T1 Controller

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

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

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

Table 7: Loopback Descriptions

Loopback	Description
loopback local	Loops the incoming receive signal back out to the transmitter. You can specify whether to use the **line** or **payload**.
loopback network	Loops the inbound traffic back to the network. You can specify whether to use **line** or **payload.**
loopback remote iboc	Attempts to set the far-end T1 interface into line loopback. This command sends an in-band bit-oriented code to the far-end to cause it to go into line loopback. This command is available when using ESF or SF framing mode.

Loopback	Description
network line	Loops the incoming signal back in the interface module using the line loopback mode of the framer. The framer does not reclock or reframe the incoming data. All incoming data is received by the interface module driver.
network payload	Loops the incoming signal back using the payload loopback mode of the framer. The framer reclocks and reframes the incoming data before sending it back out to the network. When in payload loopback mode, an all 1s data pattern is received by the local HDLC receiver, and the clock source is automatically set to line (overriding the **clock source** command). When the payload loopback is ended, the clock source returns to the last setting selected by the **clock source** command.

Running Bit Error Rate Testing

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

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

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

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

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

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

The following keywords list different BERT keywords and their descriptions.

Table 8: BERT Pattern Descriptions

Keyword	Description
1s	Repeating pattern of ones (...111...).
2^15	Pseudo-random O.151 test pattern that is 32,768 bits in length.
2^23	Pseudo-random 0.151 test pattern that is 8,388,607 bits in length.

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

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

Note BERT is supported only on controllers with channel-group configured. If CEM, IMA, or ATM are configured on controller, the BERT option is disabled.

Note When BERT is running, the serial interface of that controller will be made down till BERT is complete.

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

- After you terminate the test using the **no bert** command
- After the test runs completely

Monitoring and Maintaining the T1/E1 Interface Module

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

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

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

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 920 Series Router configuration settings, you can use the **show interfaces serial** and the **show controllers serial** commands to get detailed information on a per-port basis for your T1/E1 interface module.

Verifying Per-Port Interface Status

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

```
Router# show interfaces serial 0/1/x
Serial0/1/x is up, line protocol is up
  Hardware is ASR900-IMA8D
  Internet address is 79.1.1.2/16
  MTU 1500 bytes, BW 1984 Kbit, DLY 20000 usec,
     reliability 255/255, txload 240/255, rxload 224/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Last input 3d21h, output 3d21h, output hang never
  Last clearing of ''show interface'' counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 2998712
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1744000 bits/sec, 644 packets/sec
  5 minute output rate 1874000 bits/sec, 690 packets/sec
     180817311 packets input, 61438815508 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
     180845200 packets output, 61438125092 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions no alarm present
  Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags 2
```

Configuration Examples

This section includes the following configuration examples:

Example: Framing and Encapsulation Configuration

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

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 2/0/0
!
! Specify the framing method
!
Router(config-controller)# framing esf
!
! Exit controller configuration mode and return to global configuration mode
```

```
!
Router(config-controller)# exit
!
! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 0/1/x
!
! Specify the encapsulation protocol
!
Router(config-if)# encapsulation ppp
!
! Exit interface configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

Example: CRC Configuration

The following example sets the CRC size for the interface:

```
! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 0/1/x
!
! Specify the CRC size
!
Router(config-if)# crc 32
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

Example: Facility Data Link Configuration

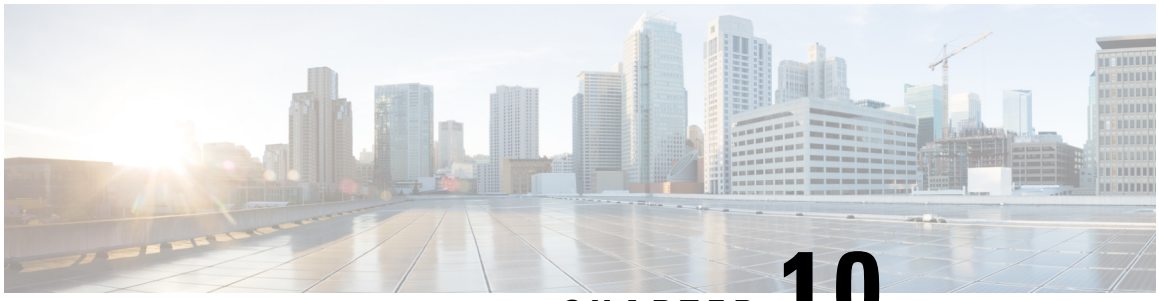
The following example configures Facility Data Link:

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 0/1/x
!
! Specify the FDL specification
!
Router(config-controller)#
fdl ansi
!
! Exit controller configuration mode and return to global configuration mode
!
Router(config-controller)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

Example: Invert Data on the T1/E1 Interface

The following example inverts the data on the serial interface:

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



CHAPTER 10

Installing and Upgrading Software

This chapter describes how to update software on the Cisco ASR 920 Series Router.

Upgrading Field Programmable Hardware Devices

Cisco IOS XE on Cisco ASR 920 Series Routers (ASR-920-24SZ-IM and ASR-920-12SZ-IM) support upgradeable firmware for field programmable hardware devices such as interface modules (IMs) and upgrades IM FPGA when ever there is an upgrade.

Cisco ASR 920 Series Router upgrades the HOFPGA when required and is indicated to the user through logs. 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 920 Series Router.

File Systems on the Cisco ASR 920 Series Router

The table below provides a list of file systems that can be seen on the Cisco ASR 920 Series Router.

Table 9: File Systems

File System	Description
bootflash:	The boot flash memory file system.
cns:	The Cisco Networking Services file directory.
nvram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.

File System	Description
system:	The system memory file system, which includes the running configuration.
bin:	The archive file system.
tmpsys:	The temporary system files file system.
usb[0-1]:	The Universal Serial Bus (USB) flash drive file systems.

If you see a file system not listed in the table above, enter the **?** help option or see the **copy** command reference for additional information on that file system.

Restrictions

When you migrate to Cisco IOS-XE Release 3.18 SP, HOFPGA upgrade is mandatory and not optional. The router works for few minutes after the first reboot is complete and starts a second reboot without a notice.

System Requirements

The following sections describe the system requirements for the Cisco ASR 920 Series Router software:

Memory Recommendations

These are the recommendation for the routers for the Cisco IOS XE 3S images and packages:

- DRAM Memory—4 GB
- Software Image—asr920-universalk9_npe.bin—270 MB (ASR 920-24SZ-IM)
- Software Image—asr920-universalk9_npe.bin—300 MB (ASR 920-12SZ-IM)

ROMmon Version Requirements

Following are the recommended release versions for all ROMmon upgradeable components. For more information about ROMmon images, see Release Notes.

- ROMmon Release 15.6(24r)S for router ASR-920-12SZ-IM
- ROMmon Release 15.6(31r)S for routers ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD, ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M

Bootflash Space Requirements

The dual-rate functionality requires a minimum of 10 MB available space in bootflash memory on Cisco ASR 920 Series Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD), and ASR-920-12SZ-IM .

Determining the Software Version

The Cisco IOS XE image is stored as a bin file in a directory that is named with the Cisco IOS XE release. The image is stored on the system board bootflash device (bootflash:).

Note If you try to copy or archive upgrade beyond the bootflash memory capacity, the action aborts.

You can use the **show version** privileged EXEC command to see the software version that is running on your router. The second line of the display shows the version.

You can also use the **dir bootflash:** privileged EXEC command to see the names of other software images that you might have stored in bootflash.

Cisco IOS XE 3S to Cisco IOS Version Number Mapping

Each version of Cisco IOS XE 3S has an associated Cisco IOS version. The table below lists these mappings for Release 3.13.0S and forward.

Table 10: Cisco IOS XE 3S to Cisco IOS Version Number Mapping

Cisco IOS XE 3S Version	Cisco IOS Version
3.13.0S	15.4(3)S
3.14.0S	15.5(1)S

The Cisco ASR 920 Series Router does not support IOS XE versions prior to 3.13.0S.

Autogenerated Files and Directories

The table below provides a list and descriptions of autogenerated files on the Cisco ASR 920 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 11: 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.

File or Directory	Description
core files	The bootflash/core directory is the storage area for .core files. **Caution** 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 XE failure. **Caution** Do not erase or move the tracelog directory.

Upgrading the Router Software

Downloading an Image

Download the image to the bootflash. For information on downloading images see, Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S.

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

Note Before upgrading from Cisco IOS XE 3.13.0S to 3.14.0S, we recommend that you disable the following CLI on Cisco ASR 920 Series Router: platform trace runtime slot 0 bay 0 process iomd module all-modules level info

The Cisco ASR 920 Series Routers are shipped with the latest software image installed. Follow the instructions in this section if you need to reinstall or upgrade the software image.

Before installing your router software, make sure that you have archived copies of the current Cisco IOS XE release and the Cisco IOS XE release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS XE image and until you have verified that the new Cisco IOS XE image works properly in your network.

Cisco routinely removes old Cisco IOS XE versions from Cisco.com. See End of Sale and End of Life Products at this URL: http://www.cisco.com/en/US/products/sw/iosswrel/prod_category_end_of_life.html.

You can copy the software image file on the bootflash memory to the appropriate TFTP directory on a host by using the **copy bootflash: tftp:** privileged EXEC command. You can also configure the router as a TFTP server to copy files from one router to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the “Basic File Transfer Services Commands” section of the Cisco IOS Configuration Fundamentals Command Reference at this URL: http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

This procedure is for copying the combined bin file to the router. You copy the file to the router from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

SUMMARY STEPS

1. Locate the software image file:
2. Download the image to a TFTP server and make sure that the server is properly configured.
3. Log into the router through the console port or a Telnet session.
4. If Gigabit Ethernet (GE) port 0 is used as management interface, check the connectivity to TFTP server using the following CLI:
5. Download the image file from the TFTP server to the router by entering this privileged EXEC command:
6. Set the image path in the boot variables and configure the router to autoboot as follows:
7. Verify the boot variables set on the router using the following CLI:
8. Save the configuration and reload the router.

DETAILED STEPS

Step 1 Locate the software image file:

a) If you are a registered customer, go to this URL and log in: http://software.cisco.com/download/navigator.html.
b) Navigate to **Routers** > **Service Provider Edge Routers**.
c) Navigate to your router model.
d) Click IOS XE Software, then select the latest IOS XE release.

Note When you select a crypto graphic image, you must also accept the terms and conditions of using crypto graphic images.

Step 2 Download the image to a TFTP server and make sure that the server is properly configured.

Step 3 Log into the router through the console port or a Telnet session.

Step 4 If Gigabit Ethernet (GE) port 0 is used as management interface, check the connectivity to TFTP server using the following CLI:

```
Router# ping vrf Mgmt-intf tftp-server-address
```

For more information about assigning an IP address and default gateway to the router, refer to the software configuration guide for this release.

Step 5 Download the image file from the TFTP server to the router by entering this privileged EXEC command:

```
Router# copy tftp://location/directory/filename.bin bootflash:
```

- For // location, specify the IP address of the TFTP server.
- For / directory / image-name .bin, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 192.0.2.1 and to overwrite the image on the router:

```
Router# copy tftp://192.0.2.1/image-name.bin bootflash:
```

The installation process extracts the bin file with all the files and the IOS XE image, and sets the BOOT directory to the created directory in bootflash memory. The process takes approximately 5 to 10 minutes, and at some stages might appear to have stopped.

Step 6 Set the image path in the boot variables and configure the router to autoboot as follows:

```
Router# configure terminal
Router(config)# config-register 0x2102 (! 0x2102 sets the router for autoboot)
Router(config)# boot system bootflash:image-name.bin (! sets the image to be loaded in the next
reload)
```

Step 7 Verify the boot variables set on the router using the following CLI:

```
Router# show bootvar
BOOT variable = bootflash:asr920-universalk9_npe.bin,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0 (! will be 0x2102 at next reload)
```

Step 8 Save the configuration and reload the router.

```
Router# reload
```

After the installation, the router is running the universal image. To install a purchased license with increased capabilities, see Software Activation Configuration Guide (Cisco ASR 920 Series). To purchase a license, contact Cisco.

Upgrading the ROMMON on the Cisco ASR 920 Series Router

The Cisco ASR 920 Series Router has two ROMMON regions (ROM0 and ROM1). We recommend that the upgrade is performed on both the regions.

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

Follow the procedure to upgrade the ROMMON image:

SUMMARY STEPS

1. Check the router bootup ROMMON region (ROM0 or ROM1). The example, shows the router boots up from ROM0 region.
2. Copy the ROMMON image to the bootflash on the router.
3. Use the upgrade rom-monitor filename bootflash:asr920-rommon-15.4.3r.S4-upgrade.pkg R0 command to upgrade the version.
4. Reload the router.
5. Reload the router again to confirm bootup from upgraded ROMMON region ROM1.
6. Repeat Step 3 to Step 5 to update the other region on the RSP (ROM0) region in this procedure).

DETAILED STEPS

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

Example:

```
Router# show rom-monitor r0
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2014 by cisco Systems, Inc.
```

Step 2 Copy the ROMMON image to the bootflash on the router.

Example:

```
Router# copy tftp://location/directory/asr920-rommon-15.4.3r.S4-upgrade.pkg bootflash:
```

Step 3 Use the upgrade rom-monitor filename bootflash:asr920-rommon-15.4.3r.S4-upgrade.pkg R0 command to upgrade the version.

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

Step 4 Reload the router.

Example:

```
Router# upgrade rom-monitor filename bootflash:asr920-rommon-15.4.3r.S4-upgrade.pkg r0
Upgrade rom-monitor on Route-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 712184b6ef336f40263222175255f475
Burning upgrade partition...
1966080+0 records in
1966080+0 records out
CChecking upgrade partition...
1966080+0 records in
1966080+0 records out
Upgrade flash partition MD5 signature is 712184b6ef336f40263222175255f475
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.
```

Step 5 Reload the router again to confirm bootup from upgraded ROMMON region ROM1.

Example:

```
Router# reload
System configuration has been modified. Save? [yes/no]: y
Building configuration...
[OK]
Proceed with reload? [confirm]
Jul 24 09:56:34.510: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.Jul
24 15:27:03.205 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with reload chassis
 code
System Bootstrap, Version 12.2(20140211:085836) [pbalakan-sb_romver_16 130], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2012 by cisco Systems, Inc.
Compiled Fri 28-Mar-14 18:57 by pbalakan-sb_romver_16
```

```
Boot ROM1
Last reset cause: RSP-Board
```

Step 6 Repeat Step 3 to Step 5 to update the other region on the RSP (ROM0) region in this procedure).

Note We recommend that both region ROM0 a.ndROM1 are upgraded.

Verifying the Upgrade

Use the show platform command to verify the ROMMON upgrade.

```
Router# show platform
Chassis type: ASR-920-12CZ-A
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      12xGE-2x10GE-FIXED  ok                    00:18:41
R0        ASR-920-12CZ-A      ok, active            00:20:39
F0                            ok, active            00:20:39
P0        ASR920-PSU0         ok                    never
P1        ASR920-PSU1         ps, fail              never
P2        ASR920-FAN          ok                    never
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        14080701            15.4(3r)S4
F0        14080701            15.4(3r)S4
```

Use the show rom-monitor r0 command to check the rommon version on the router.

```
Router# show rom-monitor r0
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2014 by cisco Systems, Inc.
```

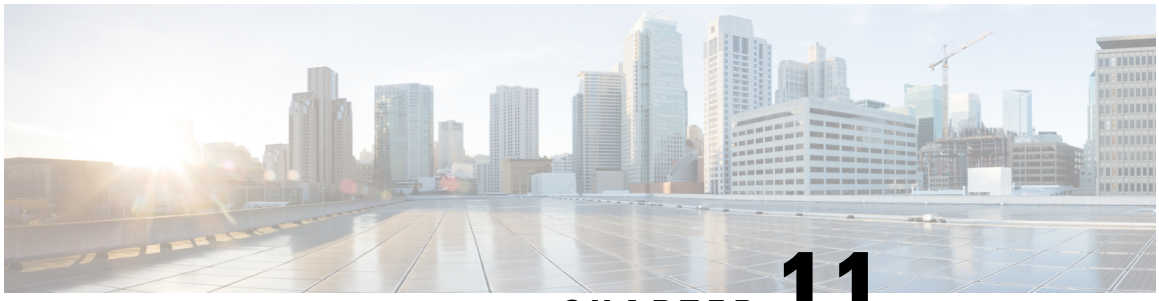
Software Upgrade Example

The following section provide a sample of software upgrade on the Cisco ASR 920 Series Router.

```
Router# show bootvar
BOOT variable = bootflash:asr920-universalk9_npe.bin,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0 (will be 0x2102 at next reload)
Router# reload
Proceed with reload? [confirm]
*Nov 14 04:29:15.051: %SYS-5-RELOAD: Reload requested by vmalshet on console. Reload Reason:
 Reload Command.Nov 14 04:29:38.446 R0/0: %PMAN-5-EXITACTION: Process manage
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2014 by cisco Systems, Inc.
Compiled Fri 20-Jun-14 17:24 by alnguyen
Boot ROM1
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Located asr920-universalk9_npe.bin
```

```
Image size 266349176 inode num 27, bks cnt 65027 blk size 8*512
################################################################################################################################################
Boot image size = 266349176 (0xfe02a78) bytes
Package header rev 0 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
        calculated 424f2b4a:ea7da21d:397efd55:db10f40e:7a6250e8
        expected   424f2b4a:ea7da21d:397efd55:db10f40e:7a6250e8
Image validated
Passing control to the main image..
%IOSXEBOOT-4-DEBUG_CONF: (rp/0): File /bootflash/debug.conf is absent, ignoring
             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, ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version
 15.5(20141015:140327) [v155_1_s_xe314_throttle-sourdutt-xe314_cortina 184]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 28-Oct-14 13:46 by sourdutt
Cisco IOS-XE software, Copyright (c) 2005-2014 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.
 Tmpdisk creation successful, status = 0
flashfs[16]: 0 files, 1 directories
flashfs[16]: 0 orphaned files, 0 orphaned directories
flashfs[16]: Total bytes: 1935360
flashfs[16]: Bytes used: 1024
flashfs[16]: Bytes available: 1934336
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.
cisco ASR-920-12CZ-A (Freescale P2020) processor (revision 1.0 GHz) with 687183K/6147K bytes
 of memory.
Processor board ID CAT1748U1GQ
12 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
1328927K bytes of SD flash at bootflash:.
Press RETURN to get started!
Router# show version
Cisco IOS XE Software, Version 2014-10-28_13.50_sourdutt
Cisco IOS Software, ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version
```

```
 15.5(20141015:140327) [v155_1_s_xe314_throttle-sourdutt-xe314_cortina 184]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 28-Oct-14 13:46 by sourdutt
Cisco IOS-XE software, Copyright (c) 2005-2014 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.
ROM: IOS-XE ROMMON
StrikerI uptime is 21 minutes
Uptime for this control processor is 25 minutes
System returned to ROM by reload
System image file is "bootflash:asr920-universalk9_npe.bin"
Last reload reason: Reload Command
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.
License Level: advancedmetroipaccess
License Type: Smart License
Next reload license Level: advancedmetroipaccess
cisco ASR-920-12CZ-A (Freescale P2020) processor (revision 1.0 GHz) with 687183K/6147K bytes
 of memory.
Processor board ID CAT1748U1GQ
12 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
1328927K bytes of SD flash at bootflash:.
Configuration register is 0x2102
```



CHAPTER 11

Activating or Deactivating Interface Module

This chapter provides information about activating or deactivating interface module (IM) on the Cisco ASR-920-24SZ-IM and Cisco ASR-920-12SZ-IM Routers. For more information about the commands used in this chapter, see the *Cisco IOS XE 3S Command References*.

Note The router does not support swapping of the TDM interface modules to Gigabit Ethernet modules on the Cisco ASR 920 Router and vice-versa. If the TDM interface module is swapped with the Gigabit Ethernet module in the same slot or vice-versa, the router must be reloaded.

Overview

Cisco ASR-920-24SZ-IM Router supports the following IMs in Cisco IOS XE Release 3.14S:

- 8-port 10/100/1000 Ethernet Interface Module (A900-IMA8T)
- 1-port 10GE XFP Interface Module (A900-IMA1X)
- 2-port 10GE SFP+/XFP Interface Module (A900-IMA2Z)
- 8-port RJ48C T1/E1 Interface Module (A900-IMA8D)
- 16-port T1/E1 Interface Module (A900-IMA16D)
- 32-port T1/E1 Interface Module (A900-IMA32D)
- 4-port OC3/STM1 or 1 port OC12/STM4 Interface Module (A900-IMA4OS)
- Combo 8-port 10/100/1000 and 1 port 10GE Interface Module (A900-IMA8T1Z)

Cisco ASR-920-12SZ-IM Router supports the following IMs in Cisco IOS XE Release 3.14S:

- 8-port 10/100/1000 Ethernet Interface Module (A900-IMA8T)
- 8-port SFP Gigabit Ethernet Interface Module (A900-IMA8S)
- 8-port RJ48C T1/E1 Interface Module (A900-IMA8D)
- 16-port T1/E1 Interface Module (A900-IMA16D)
- 32-port T1/E1 Interface Module (A900-IMA32D)
- 1-port 10GE XFP Interface Module (A900-IMA1X)
- 2-port 10GE SFP+/XFP Interface Module (A900-IMA2Z)
- Combo 8-port 10/100/1000 and 1 port 10GE Interface Module (A900-IMA8T1Z)
- Combo 8 SFP GE and 1-port 10GE IM (A900-IMA8S1Z)
- 4-port OC3/STM1 or 1-port OC12/STM4 Interface Module (A900-IMA4OS)

For information on installing and removing the IMs, see the *Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M Aggregation Services Router Hardware Installation Guide*.

The router does not support swapping of the TDM interface modules to Gigabit Ethernet modules. If the TDM interface module is swapped with the Gigabit Ethernet module in the same slot or vice-versa, the router must be reloaded.

Prerequisites for Activating an IM

- IM must be installed in the router
- IM must not be in admin down mode
- To activate 8x1G Cu IM or 8xT1/E1 IM, you must give up the following ports on the router front panel:
  - 16 to 23 for Cu IM
  - 20 to 23 for T1/E1 IM
- To activate a TDM IM you must reload the router. Without reloading the router, the IM or associated front panel ports can not be used. If reload is aborted, the ports 20 to 23 remain disabled and IM remains in Out-of-Service (OOS) state until the next reload.

Restrictions for Activating an IM

- You cannot activate an IM when activate or deactivate commands are running in the background. The activate process usually completes in two minutes.
- Activating an incorrect IM type results in the IM OOS state.
- **write erase** does not disable activated IM. To disable the IM, you must use the **hw-module subslot** command.

Activating an IM

Note This section is applicable only to the 8x1G Cu IM or 8xT1/E1 IMs. There is no impact to the front panel ports to bring up or bring down the 1x10G and 2x10G IMs.

Before using the IM, you must activate the IM.

Step 1 Verify that the correct IM is inserted in the IM slot.

Step 2 Shut down all active interfaces to be removed in IM activation (8x1G Cu IM or 8xT1/E1 IM). See Prerequisites for Activating an IM, on page 96, for active interfaces to be shut down.

Step 3 Wait for a minute.

Step 4 Default all interfaces to be removed from the router.

Step 5 Execute the following command to activate the IM present in the IM slot.

hw-module subslot slot-number/subslot-number activate

- slot-number—Specifies the chassis slot number where the IM is installed.
- subslot-number—Specifies the chassis subslot number where IM is installed.

Note The activate CLI operations run in the background.

Note The following ports on the router are relinquished when activating 8x1G Cu IM or 8xT1/E1 IM:

- 16 to 23 for Cu IM
- 20 to 23 for T1/E1 IM

Prerequisites for Deactivating an IM

- IM must be installed in the router
- IM must not be in admin down mode

Restrictions for Deactivating an IM

- You cannot deactivate an IM when activate or deactivate commands are running in the background. The deactivation process usually completes in two minutes.
- You cannot use write erase to disable activated IM. To disable the activated IM, you must use CLI.
- Deactivating an IM by specifying an incorrect IM type or without an IM installed in the router can cause hardware or software resource issues. In this case, you must reload the router to reclaim the front panel ports and other ASIC related resources.
- You must reload the router to complete the activate/deactivate process.

Note Activation or deactivation of 8x1G Cu IM does not require a router reload.

- The **hw-module subslot default** command is not supported on TDM and OC-3 interface module.

Deactivating an IM

Note This section is applicable only to the 8-port 1G Cu IM or 8-port T1/E1 IMs. There is no impact to the front panel ports to bring up or bring down the 1-port 10G and 2-port 10G IMs.

Before removing the IM from the router, you must deactivate the IM.

SUMMARY STEPS

1. Verify that the correct IM is in OK state in the router.
2. Remove all virtual interfaces (using the **no interface** *interface-name* command) that are associated with the IM. These interfaces include MPLS TP tunnels, TE tunnels, BDI interface, and Port-Channel interface.
3. Shut down all pluggable IM interfaces in the router.
4. Wait for a minute.
5. Default all pluggable IM interfaces in the router.
6. Execute the following command to deactivate the IM present in the IM slot:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Verify that the correct IM is in OK state in the router.	
Step 2	Remove all virtual interfaces (using the **no interface** *interface-name* command) that are associated with the IM. These interfaces include MPLS TP tunnels, TE tunnels, BDI interface, and Port-Channel interface.	
Step 3	Shut down all pluggable IM interfaces in the router.	
Step 4	Wait for a minute.	
Step 5	Default all pluggable IM interfaces in the router.	
Step 6	Execute the following command to deactivate the IM present in the IM slot:	**hw-module subslot slot-number/subslot-number deactivate** • slot-number—Specifies the chassis slot number where the IM is installed. • subslot-number—Specifies the chassis subslot number where IM is installed. **Note** The deactivate CLI operations run in the background.

	Command or Action	Purpose
		Note The following ports on the router are recovered when deactivating 8-port 1G Cu IM or 8-port T1/E1 IM: • 16 to 23 for Cu IM • 20 to 23 for T1/E1 IM

Sample Configuration and Verification Examples for Activation or Deactivation of IMs

The following sections provide sample configuration and verification example for activating or deactivating the following IMs:

Sample Configuration and Verification of Activating an 8-port 1G Cu IM (A900-IMA8T)

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
*Nov 20 09:31:44.532: %LINK-5-CHANGED: Interface GigabitEthernet0/0/19, changed state to
administratively down
*Nov 20 09:31:44.536: %LINK-5-CHANGED: Interface GigabitEthernet0/0/20, changed state to
administratively down
*Nov 20 09:31:44.541: %LINK-5-CHANGED: Interface GigabitEthernet0/0/21, changed state to
administratively down
*Nov 20 09:31:44.542: %LINK-5-CHANGED: Interface GigabitEthernet0/0/22, changed state to
administratively down
*Nov 20 09:31:44.547: %LINK-5-CHANGED: Interface GigabitEthernet0/0/23, changed state to
administratively down
Router(config-if-range)# exit
Router(config)# exit
```

The following example shows how to activate an 8-port 1G Cu IM (A900-IMA8T) on the Cisco ASR-920-24SZ-IM Router:

```
Router# hw-module
*Nov 20 09:31:53.361: %SYS-5-CONFIG_I: Configured from console by consolesu

Router# hw-module subslot 0/1 activate A900-IMA8T

Command will disable & default configs in module 0 (16-23). Proceed ? [confirm]
Changed ACTIVATED IM: ASR900_IMA8T
Router#
*Nov 20 09:32:11.112: %IOSXE-1-PLATFORM:kernel: Board info b500002
*Nov 20 09:32:11.359: %TRANSCEIVER-6-REMOVED:iomd:  Transceiver module removed from
GigabitEthernet0/0/23
*Nov 20 09:32:11.369: %IOSXE_RP_ALARM-6-INFO: ASSERT None GigabitEthernet0/0/23
*Nov 20 09:32:21.743: %SPA_OIR-6-ONLINECARD: SPA (A900-IMA8T) online in subslot 0/1
*Nov 20 09:32:23.639: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/0, changed state to down
*Nov 20 09:32:23.652: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/1, changed state to down
*Nov 20 09:32:23.692: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/2, changed state to down
*Nov 20 09:32:23.697: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/3, changed state to down
*Nov 20 09:32:23.702: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/4, changed state to down
```

```
*Nov 20 09:32:23.706: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/5, changed state to down
*Nov 20 09:32:23.711: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/6, changed state to down
*Nov 20 09:32:23.711: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/7, changed state to down
```

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      24xGE-4x10GE-FIXED  ok                    05:31:32
 0/1      A900-IMA8T          ok                    00:00:39
R0        ASR-920-24SZ-IM     ok, active            05:33:14
F0                            ok, active            05:33:14
P0        ASR920-PSU0         ok                    05:31:56
P1        ASR920-PSU1         N/A                   never
P2        ASR920-FAN          ok                    05:31:55
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        01491802            15.4(3r)S4
F0        01491802            15.4(3r)S4
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/4   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/5   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/6   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/7   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/8   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/9   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/10  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/11  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/12  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/13  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/14  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/15  unassigned      YES NVRAM  down                  down
Te0/0/24               unassigned      YES NVRAM  administratively down down
Te0/0/25               unassigned      YES NVRAM  administratively down down
Te0/0/26               unassigned      YES NVRAM  administratively down down
Te0/0/27               unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1/0   unassigned      YES unset  down                  down
GigabitEthernet0/1/1   unassigned      YES unset  down                  down
GigabitEthernet0/1/2   unassigned      YES unset  down                  down
GigabitEthernet0/1/3   unassigned      YES unset  down                  down
GigabitEthernet0/1/4   unassigned      YES unset  down                  down
GigabitEthernet0/1/5   unassigned      YES unset  down                  down
GigabitEthernet0/1/6   unassigned      YES unset  down                  down
GigabitEthernet0/1/7   unassigned      YES unset  down                  down
GigabitEthernet0       7.23.21.156     YES NVRAM  up                    up
BDI243                 unassigned      YES NVRAM  down                  down
Router#
```

Sample Configuration and Verification for Deactivating an 8-port 1G Cu IM (A900-IMA8T)

The following example displays system environment information for system components for the Cisco ASR-920-24SZ-IM Router:

```
Router# show environment
Number of Critical alarms:  0
Number of Major alarms:     0
Number of Minor alarms:     0
Slot    Sensor       Current State       Reading
----    ------       -------------       -------
 P0    PEM Iout          Normal           7 A
 P0    PEM Vout          Normal           12 V DC
 P0    PEM Vin           Normal           230 V AC
 P0    Temp: Temp 1      Normal           51 Celsius
 P2    Temp: FC PWM      Fan Speed 65%    38 Celsius
 R0    VADM1: VX1        Normal           997 mV
 R0    VADM1: VX2        Normal           1046 mV
 R0    VADM1: VX3        Normal           997 mV
 R0    VADM1: VP1        Normal           3283 mV
 R0    VADM1: VP2        Normal           1796 mV
 R0    VADM1: VP3        Normal           1197 mV
 R0    VADM1: VP4        Normal           1768 mV
 R0    VADM1: VH         Normal           12317 mV
 R0    VADM1: AUX1       Normal           3840 mV
 R0    VADM1: AUX2       Normal           6958 mV
 R0    Temp: CYLON       Normal           60 Celsius
 R0    Temp: FPGA        Normal           49 Celsius
 R0    Temp: Outlet      Normal           47 Celsius
 R0    VADM2: VX1        Normal           995 mV
 R0    VADM2: VX2        Normal           973 mV
 R0    VADM2: VX3        Normal           754 mV
 R0    VADM2: VP1        Normal           2495 mV
 R0    VADM2: VP2        Normal           1495 mV
 R0    VADM2: VP3        Normal           1497 mV
 R0    VADM2: VH         Normal           12296 mV
```

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      24xGE-4x10GE-FIXED  ok                    05:37:55
 0/1      A900-IMA8T          ok                    00:07:02
R0        ASR-920-24SZ-IM     ok, active            05:39:37
F0                            ok, active            05:39:37
P0        ASR920-PSU0         ok                    05:38:19
P1        ASR920-PSU1         N/A                   never
P2        ASR920-FAN          ok                    05:38:18
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        01491802            15.4(3r)S4
F0        01491802            15.4(3r)S4
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
```

```
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/4   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/5   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/6   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/7   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/8   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/9   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/10  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/11  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/12  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/13  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/14  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/15  unassigned      YES NVRAM  down                  down
Te0/0/24               unassigned      YES NVRAM  administratively down down
Te0/0/25               unassigned      YES NVRAM  administratively down down
Te0/0/26               unassigned      YES NVRAM  administratively down down
Te0/0/27               unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1/0   unassigned      YES unset  down                  down
GigabitEthernet0/1/1   unassigned      YES unset  down                  down
GigabitEthernet0/1/2   unassigned      YES unset  down                  down
GigabitEthernet0/1/3   unassigned      YES unset  down                  down
GigabitEthernet0/1/4   unassigned      YES unset  down                  down
GigabitEthernet0/1/5   unassigned      YES unset  down                  down
GigabitEthernet0/1/6   unassigned      YES unset  down                  down
GigabitEthernet0/1/7   unassigned      YES unset  down                  down
GigabitEthernet0       7.23.21.156     YES NVRAM  up                    up
BDI243                 unassigned      YES NVRAM  down                  down
Router#
```

The following example shows how to deactivate 8x1G Cu IM (A900-IMA8T)) on the Cisco ASR-920-24SZ-IM Router:

```
Router# hw-module subslot 0/1 deactivate
Command will default configs in module 1. Proceed ? [confirm]
Changed ACTIVATED IM: 24xGE-4x10GE-FIXED
Router#
*Nov 20 09:40:16.844: %SPA_OIR-6-OFFLINECARD: SPA (A900-IMA8T) offline in subslot 0/1
*Nov 20 09:40:16.844: %IOSXE_OIR-6-SOFT_STOPSPA: SPA(A900-IMA8T) stopped in subslot 0/1,
interfaces disabled
*Nov 20 09:40:17.457: %TRANSCEIVER-6-INSERTED:iomd:  transceiver module inserted in
GigabitEthernet0/0/23
*Nov 20 09:41:32.364: %IOSXE_RP_ALARM-6-INFO: CLEAR None GigabitEthernet0/0/23
Router#
```

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      24xGE-4x10GE-FIXED  ok                    05:40:54
 0/1      A900-IMA8T          stopped               00:01:55
R0        ASR-920-24SZ-IM     ok, active            05:42:36
F0                            ok, active            05:42:36
P0        ASR920-PSU0         ok                    05:41:19
P1        ASR920-PSU1         N/A                   never
P2        ASR920-FAN          ok                    05:41:18
Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
R0        01491802            15.4(3r)S4
```

```
F0        01491802            15.4(3r)S4
Router#
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/4   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/5   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/6   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/7   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/8   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/9   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/10  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/11  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/12  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/13  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/14  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/15  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/16  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/17  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/18  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/19  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/20  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/21  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/22  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/23  unassigned      YES NVRAM  down                  down
Te0/0/24               unassigned      YES NVRAM  administratively down down
Te0/0/25               unassigned      YES NVRAM  administratively down down
Te0/0/26               unassigned      YES NVRAM  administratively down down
Te0/0/27               unassigned      YES NVRAM  administratively down down
GigabitEthernet0       7.23.21.156     YES NVRAM  up                    up
BDI243                 unassigned      YES NVRAM  down                  down
```

Sample Configuration and Verification of Activating 8-port T1/E1 IM (A900-IMA8D)

The following example shows how to activate 8-port T1/E1 IM (A900-IMA8D) on the Cisco ASR-920-24SZ-IM Router:

```
Router# hw-module subslot 0/1 activate A900-IMA8D
Command will disable &amp;amp; default configs in module 0 (20-23). Proceed ? [confirm]
System reload is required for act/deact of TDM IMs. Proceed with reload ?[confirm]

Changed ACTIVATED IM: ASR900_IMA16D

*Nov 20 09:47:08.155: %TRANSCEIVER-6-REMOVED:iomd:  Transceiver module removed from
GigabitEthernet0/0/23
*Nov 20 09:47:08.875: %IOSXE_RP_ALARM-6-INFO: ASSERT None GigabitEthernet0/0/23  [OK]
Proceed with reload? [confirm]

*Nov 20 09:47:22.275: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.Nov 20 09:47:56.304 R0/0:
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2014 by cisco Systems, Inc.
```

```
Compiled Fri 20-Jun-14 17:24 by alnguyen

PEX up stream Vendor ID[0x860610b5]
PEX down stream vendor ID [0x860610b5]
Boot ROM1
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Located asr920.bin
Image size 266457720 inode num 23, bks cnt 65054 blk size 8*512

################################################################

Boot image size = 266457720 (0xfe1d278) bytes
Package header rev 0 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
        calculated 872ac9f3:08808feb:9690e7e4:d68c5dc0:18191823
        expected   872ac9f3:08808feb:9690e7e4:d68c5dc0:18191823
Image validated
Passing control to the main image..


              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, ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version
 15.5(20141114:175558) [v155_1_s_xe314_throttle-hargurra-psu 104
Copyright (c) 1986-2014 by Cisco Systems, Inc.

Compiled Sat 15-Nov-14 00:09 by hargurra

Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License (&quot;GPL&quot;) 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 &quot;License Notice&quot; file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
Tmpdisk creation successful, status = 0
flashfs[16]: 0 files, 1 directories
flashfs[16]: 0 orphaned files, 0 orphaned directories
flashfs[16]: Total bytes: 1935360
flashfs[16]: Bytes used: 1024
flashfs[16]: Bytes available: 1934336
Changed ACTIVATED IM: ASR900_IMA16D
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.

cisco ASR-920-24SZ-IM (Freescale P2020) processor (revision 1.2 GHz) with 687112K/6147K
bytes of memory.
Processor board ID CAT1707V01N
20 Gigabit Ethernet interfaces
4 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
1328927K bytes of SD flash at bootflash:.

Press RETURN to get started!

Authentication passed
PLATFORM:kernel: Board info b500002
*Nov 20 09:53:23.315: %SPA_OIR-6-ONLINECARD: SPA (A900-IMA8D) online in subslot 0/1[OK]
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/4   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/5   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/6   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/7   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/8   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/9   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/10  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/11  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/12  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/13  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/14  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/15  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/16  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/17  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/18  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/19  unassigned      YES NVRAM  down                  down
Te0/0/24               unassigned      YES NVRAM  administratively down down
Te0/0/25               unassigned      YES NVRAM  administratively down down
Te0/0/26               unassigned      YES NVRAM  administratively down down
Te0/0/27               unassigned      YES NVRAM  administratively down down
GigabitEthernet0       7.23.21.156     YES NVRAM  up                    up
BDI243                 unassigned      YES NVRAM  down                  down
```

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM

Slot      Type                State                 Insert time (ago)
```

```
--------- ------------------- --------------------- -----------------
 0/0      24xGE-4x10GE-FIXED  ok                    00:15:26
 0/1      A900-IMA8D         ok                    00:15:26
R0        ASR-920-24SZ-IM     ok, active            00:17:14
F0                            ok, active            00:17:14
P0        ASR920-PSU0         ok                    00:15:52
P1        ASR920-PSU1         N/A                   never
P2        ASR920-FAN          ok                    00:15:51

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        01491802            15.4(3r)S4
F0        01491802            15.4(3r)S4
Router#
```

Sample Configuration and Verification of Deactivating 8-port T1/E1 IM (A900-IMA8D)

The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      24xGE-4x10GE-FIXED  ok                    05:37:55
 0/1      A900-IMA8T          ok                    00:07:02
R0        ASR-920-24SZ-IM     ok, active            05:39:37
F0                            ok, active            05:39:37
P0        ASR920-PSU0         ok                    05:38:19
P1        ASR920-PSU1         N/A                   never
P2        ASR920-FAN          ok                    05:38:18
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        01491802            15.4(3r)S4
F0        01491802            15.4(3r)S4
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/4   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/5   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/6   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/7   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/8   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/9   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/10  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/11  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/12  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/13  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/14  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/15  unassigned      YES NVRAM  down                  down
Te0/0/24               unassigned      YES NVRAM  administratively down down
Te0/0/25               unassigned      YES NVRAM  administratively down down
Te0/0/26               unassigned      YES NVRAM  administratively down down
Te0/0/27               unassigned      YES NVRAM  administratively down down
```

```
GigabitEthernet0/1/0   unassigned      YES unset  down                  down
GigabitEthernet0/1/1   unassigned      YES unset  down                  down
GigabitEthernet0/1/2   unassigned      YES unset  down                  down
GigabitEthernet0/1/3   unassigned      YES unset  down                  down
GigabitEthernet0/1/4   unassigned      YES unset  down                  down
GigabitEthernet0/1/5   unassigned      YES unset  down                  down
GigabitEthernet0/1/6   unassigned      YES unset  down                  down
GigabitEthernet0/1/7   unassigned      YES unset  down                  down
GigabitEthernet0       7.23.21.156     YES NVRAM  up                    up
BDI243                 unassigned      YES NVRAM  down                  down
Router#
```

The following example shows how to deactivate 8-port T1/E1 IM (A900-IMA8D) on the Cisco ASR-920-24SZ-IM Router:

```
Router# hw-module subslot 0/1 deactivate

Command will default configs in module 1. Proceed ? [confirm]
System reload is required for act/deact of TDM IMs. Proceed with reload ?[confirm]
Changed ACTIVATED IM: 24xGE-4x10GE-FIXED[OK]
Proceed with reload? [confirm]
*Nov 20 10:17:16.968: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.Nov 20 10:17:49.956 R0/0: %PMAN-5-EXITACTION: Process manager
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2014 by cisco Systems, Inc.
Compiled Fri 20-Jun-14 17:24 by alnguyen
PEX up stream Vendor ID[0x860610b5]
PEX down stream vendor ID [0x860610b5]
Boot ROM1
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Located asr920.bin
Image size 266457720 inode num 23, bks cnt 65054 blk size 8*512

################################################

Boot image size = 266457720 (0xfe1d278) bytes
Package header rev 0 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 872ac9f3:08808feb:9690e7e4:d68c5dc0:18191823
expected 872ac9f3:08808feb:9690e7e4:d68c5dc0:18191823
Image validated
Passing control to the main image..
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, ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version
 15.5(20141114:175558) [v155_1_s_xe314_throttle-hargurra-psu 104]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Sat 15-Nov-14 00:09 by hargurra
Cisco IOS-XE software, Copyright (c) 2005-2014 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.

Tmpdisk creation successful, status = 0
flashfs[16]: 0 files, 1 directories
flashfs[16]: 0 orphaned files, 0 orphaned directories
flashfs[16]: Total bytes: 1935360
flashfs[16]: Bytes used: 1024
flashfs[16]: Bytes available: 1934336
Changed ACTIVATED IM: 24xGE-4x10GE-FIXED
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.
cisco ASR-920-24SZ-IM (Freescale P2020) processor (revision 1.2 GHz) with 687112K/6147K
bytes of memory.

Processor board ID CAT1707V01N
24 Gigabit Ethernet interfaces
4 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
1328927K bytes of SD flash at bootflash:.
SETUP: new interface GigabitEthernet0/0/20 placed in "shutdown" state
SETUP: new interface GigabitEthernet0/0/21 placed in "shutdown" state
SETUP: new interface GigabitEthernet0/0/22 placed in "shutdown" state
SETUP: new interface GigabitEthernet0/0/23 placed in "shutdown" state
Press RETURN to get started!

Authentication passed
*Nov 20 10:23:14.107: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM[OK]
*Nov 20 10:23:29.665: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
*Nov 20 10:23:29.666: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco licensing cloud
 restored
*Nov 20 10:24:14.037: %SPA_OIR-6-ONLINECARD: SPA (24xGE-4x10GE-FIXED) online in subslot 0/0
```

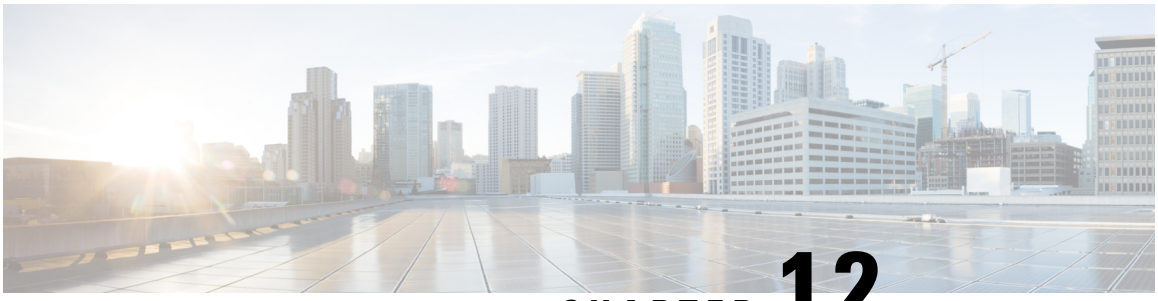
The following example displays platform information for the Cisco ASR-920-24SZ-IM Router:

```
Router# show platform
Chassis type: ASR-920-24SZ-IM
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
 0/0      24xGE-4x10GE-FIXED  ok                    05:40:54
 0/1      A900-IMA8T          stopped               00:01:55
R0        ASR-920-24SZ-IM     ok, active            05:42:36
F0                            ok, active            05:42:36
P0        ASR920-PSU0         ok                    05:41:19
P1        ASR920-PSU1         N/A                   never
P2        ASR920-FAN          ok                    05:41:18
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
R0        01491802            15.4(3r)S4
```

```
F0        01491802            15.4(3r)S4
Router#
```

The following example displays sample output for interfaces on the Cisco ASR-920-24SZ-IM Router:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/4   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/5   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/6   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/7   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/8   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/9   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/10  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/11  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/12  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/13  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/14  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/15  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/16  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/17  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/18  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/19  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/20  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/21  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/22  unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/23  unassigned      YES NVRAM  down                  down
Te0/0/24               unassigned      YES NVRAM  administratively down down
Te0/0/25               unassigned      YES NVRAM  administratively down down
Te0/0/26               unassigned      YES NVRAM  administratively down down
Te0/0/27               unassigned      YES NVRAM  administratively down down
GigabitEthernet0       7.23.21.156     YES NVRAM  up                    up
BDI243                 unassigned      YES NVRAM  down                  down
```



CHAPTER 12

Configuring Ethernet Interfaces

This chapter provides information about configuring the Gigabit Ethernet interface on the Cisco ASR 920 Series Router.

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

Effective Cisco IOS-XE Release 3.16S, the Cisco ASR-920-12SZ-IM Aggregation Services Router was added to the Cisco ASR 920 Series Routers family.

Note On the Cisco ASR-920-12SZ-IM Aggregation Services Router, ports from 12 through 15 can operate at either 1G or 10G, and operates in a mutually exclusive way. You cannot insert both 1G and 10G together. If you insert IG IMs (A900-IMA8T1Z, A900-IMA8S1Z, A900-IMA8T, A900-IMA8S), the dual rate port supports only 10G.

Configuring an Interface

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

SUMMARY STEPS

1. Router# **configure terminal**

2. Do one of the following:
   - Router(config)# **interface gigabitethernet** *slot/port*
   -
   - Router(config)# **interface tengigabitethernet** *slot/port*
3. **no negotiation auto**
4. **speed**{ **10** | **100** | **1000**}
5. Router(config-if)# **carrier-delay down msec** *value*
6. Router(config-if)# **carrier-delay up msec** *value*
7. Router(config-if)# **ip address** *ip-address mask* {**secondary**} | **dhcp** {**client-id** *interface-name*} {**hostname** *host-name*}]
8. Router(config-if)# **mtu** *bytes*
9. Router(config-if)# **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Do one of the following: • Router(config)# **interface gigabitethernet** *slot/port* • • Router(config)# **interface tengigabitethernet** *slot/port*	Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where: • *slot/port* —The location of the interface. See Specifying the Interface Address on an Interface, on page 113. **Note** The slot number is always 0.
Step 3	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	(Optional) Disables automatic negotitation. **Note** Use the **speed** command only when the mode is set to no negotiation auto.
Step 4	**speed**{ **10**	**100**	**1000**} **Example:** `Router(config-if)# speed 1000`	(Optional) Specifies the speed for an interface to transmit at 10, 100, and 1000 Mbps (1 Gbps), where the default is 1000 Mbps.
Step 5	Router(config-if)# **carrier-delay down msec** *value*	(Optional) Sets the router to signal within the specified time delay, when an interface goes down, where: • *down*—Time delay for signalling when the interface goes down.
Step 6	Router(config-if)# **carrier-delay up msec** *value*	(Optional) Sets the router to signal within the specified time delay, when an interface should be up again, where: • *up*—Time delay before an interface should be up again. You must wait for atleast 2 msec before bring the interface up again, this is to protect against link flaps.

	Command or Action	Purpose
Step 7	Router(config-if)# **ip address** *ip-address mask* {**secondary**} | **dhcp** {**client-id** *interface-name*} {**hostname** *host-name*}]	Sets a primary or secondary IP address for an interface that is using IPv4, where: • *ip-address* —The IP address for the interface. • *mask* —The mask for the associated IP subnet. • **secondary**—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. • **dhcp**—Specifies that IP addresses will be assigned dynamically using DHCP. • **client-id** *interface-name*—Specifies the client identifier. The *interface-name* sets the client identifier to the hexadecimal MAC address of the named interface. • **hostname** *host-name*—Specifies the hostname for the DHCP purposes. The *host-name* is the name of the host to be placed in the DHCP option 12 field.
Step 8	Router(config-if)# **mtu** *bytes*	(As Required) Specifies the maximum packet size for an interface, where: • *bytes*— The maximum number of bytes for a packet. The default is 1500 bytes; the range is from 1500 to 9216.
Step 9	Router(config-if)# **no shutdown**	Enables the interface.

Specifying the Interface Address on an Interface

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

- slot—The chassis slot number in the Cisco ASR 920 Series Router of the interface.

Note The interface slot number is always 0.

- subslot—The subslot of the interface. Interface subslots are always 0.
- port—The number of the individual interface port on an interface.

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

Modifying the Interface MTU Size

Note The Cisco ASR 920 Series Router supports only eight unique MTUs.

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 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 4-byte header, and each MPLS label adds a 4-byte header (*n* labels x 4 bytes).

For the Gigabit Ethernet interface on the Cisco ASR 920 Series Router, the default MTU size is 1500 bytes. The maximum configurable MTU is 9216 bytes. The interface 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)# mtu bytes`	Configures the maximum packet size for an interface, where: • *bytes*— Specifies the maximum number of bytes for a packet. The default is 1500 bytes and the maximum configurable MTU is 9216 bytes.

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

Verifying the MTU Size

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

The following example shows an MTU size of 1500 bytes for interface port 0 (the first port) on the Gigabit Ethernet interface in slot 0 of the router:

```
Router# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is down, line protocol is down
Hardware is 8xGE-4x10GE-FIXED, address is 6073.5cff.8080 (bia 6073.5cff.8080)
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)
```

Configuring the Encapsulation Type

The encapsulation supported by the interfaces is IEEE 802.1Q and IEEE 802.1ad 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 920 Series Router* document.

Configuring Autonegotiation on an Interface

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

For the Gigabit Ethernet interfaces on the Cisco ASR 920 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.

Enabling Autonegotiation

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

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

Disabling Autonegotiation

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

Speed and duplex configurations can be advertised using autonegotiation. 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)# no negotiation auto`	Disables autonegotiation on Gigabit Ethernet interfaces. No advertisement of flow control occurs.

Configuring Carrier Ethernet Features

For information about configuring an Ethernet interface as a layer 2 Ethernet virtual circuit (EVC) or Ethernet flow point (EFP), see 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# copy running-config startup-config`	Writes the new configuration to NVRAM.

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

Shutting Down and Restarting an Interface

You can shut down and restart any of the interface ports on an interface 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 interfaces; you can remove them at any time.

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

Command	Purpose
`Router(config-if)# shutdown`	Restarts, stops, or starts an interface.

To shut down an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# shutdown`	Disables an interface.

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

Command	Purpose
`Router(config-if)# no shutdown`	Restarts a disabled interface.

Verifying the Interface Configuration

Besides using the **show running-configuration** command to display your Cisco ASR 920 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.

Verifying Per-Port Interface Status

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

The following example provides sample output for interface port 0 on the interface located in slot 1 of the Cisco ASR 920 Series Router:

```
Router# show interface gigabitEthernet 0/0/7
GigabitEthernet0/0/7 is up, line protocol is up
Hardware is 8xGE-4x10GE-FIXED, address is 6073.5cff.8087 (bia 6073.5cff.8087)
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 on
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

Verifying Interface Status

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

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

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

Command	Purpose
`Router# show hw-module slot/subslot transceiver port idprom`	Displays information for the transceiver identification programmable read only memory (idprom). **Note** Transceiver types must match for a connection between two interfaces to become active.

Command	Purpose
`Router# show hw-module slot/subslot transceiver port idprom status`	Displays information for the transceiver initialization status. **Note** The transmit and receive optical power that is 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# show hw-module slot/subslot transceiver port idprom dump`	Displays a dump of all EEPROM content that is stored in the transceiver.

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

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

```
Router# show hw-module subslot 0/0 transceiver 9 idprom
IDPROM for transceiver GigabitEthernet0/0/0:Description = SFP optics (type 3) Transceiver
Type: = GE SX (19) Product Indentifier (PID) = FTRJ8519P1BNL-C6Vendor Revision = ASerial
Number (SN) = FNS1037R8DHVendor Name = CISCO-FINISARVendor OUI (IEEE company ID) = 00.90.65
 (36965)CLEI code = IPUIALJRAACisco part number = 10-2143-01Device State = Enabled.Date
code (yy/mm/dd) = 06/09/14Connector type = LC.Encoding = 8B10BNRZNominal bitrate = GE (1300
 Mbits/s) Minimum bit rate as % of nominal bit rate = not specifiedMaximum 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 0/0 transceiver 2 idpromIDPROM for transceiver
GigabitEthernet0/0/2:Description = SFP optics (type 3) Transceiver Type: = GE CWDM 1490
(28) Product Indentifier (PID) = FWDM-16217D49CSCVendor Revision = CSerial Number (SN) =
FNS10500HA9Vendor Name = CISCO-FINISARVendor OUI (IEEE company ID) = 00.90.65 (36965)CLEI
code = CNTRVX0FAACisco part number = 10-1884-01Device State = Enabled.Date code (yy/mm/dd)
 = 06/12/12Connector type = LC.Encoding = 8B10BNRZNominal bitrate = (2700 Mbits/s) Minimum
 bit rate as % of nominal bit rate = not specifiedMaximum bit rate as % of nominal bit rate
 = not specified
```

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

```
Router# show
 hw-module subslot 2/2 transceiver 9 idprom brief
IDPROM for transceiver TenGigabitEthernet0/0/9:
Description = SFP or SFP+ optics (type 3)
Transceiver Type: = SFP+ 10GBASE-SR (273)
Product Identifier (PID) = SFP-10G-SR
Vendor Revision = 1
Serial Number (SN) = JUS1803G2FT
Vendor Name = CISCO-JDSU
Vendor OUI (IEEE company ID) = 00.01.9C (412)
CLEI code = COUIA8NCAA
Cisco part number = 10-2415-03
Device State = Enabled.
Date code (yy/mm/dd) = 14/01/18
Connector type = LC.
Encoding = 4b5b
NRZ
Manchester
```

```
Nominal bitrate = (10300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
```

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

```
Router# show hw-module subslot 0/3 transceiver 9 status

The Transceiver in slot 0 subslot 0 port 9 is enabled.
Module temperature = +24.773 C
Transceiver Tx supply voltage = 3291.3 mVolts
Transceiver Tx bias current = 6024 uAmps
Transceiver Tx power = -2.3 dBm
Transceiver Rx optical power = -2.9 dBm
```

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

```
Router# show hw-module subslot 0/0 transceiver 9 idprom dump
IDPROM for transceiver GigabitEthernet0/0/0:Description = SFP optics (type 3) Transceiver
Type: = GE SX (19) Product Indentifier (PID) = FTRJ8519P1BNL-C6Vendor Revision = ASerial
Number (SN) = FNS1037R8DHVendor Name = CISCO-FINISARVendor OUI (IEEE company ID) = 00.90.65
 (36965)CLEI code = IPUIALJRAACisco part number = 10-2143-01Device State = Enabled.
SFP IDPROM Page 0xA0:000: 03 04 07 00 00 00 01 00 00 00010: 00 01 0D 00 00 00 37 1B 00
00020: 43 49 53 43 4F 2D 46 49 4E 49030: 53 41 52 20 20 20 00 00 90 65040: 46 54 52 4A 38
35 31 39 50 31050: 42 4E 4C 2D 43 36 41 20 20 20060: 03 52 00 74 00 1A 00 00 46 4E070: 53
31 30 33 37 52 38 44 48 20080: 20 20 20 20 30 36 30 39 31 34090: 20 20 58 80 01
SFP IDPROM Page 0xA2:000: 6D 00 E3 00 67 00 F3 00 98 58010: 69 78 90 88 71 48 1D 4C 01
F4020: 17 70 03 E8 25 19 02 F5 25 19030: 04 A9 E3 EE 01 DF 8F C5 02 EC040: 00 00 00 00 00
00 00 00 00 00050: 00 00 00 00 00 00 00 00 00 00060: 00 00 00 00 00 00 00 00 3E 5D070: 01
79 C0 5B AC 86 01 00 00 00080: 00 AA FF FD 01 00 00 00 01 00090: 00 00 00 00 00 3A 1B 70
80 D8100: 00 62 00 28 00 22 00 00 00 00110: 82 F8 05 40 00 00 05 40 00 00120: 00 00 00 00
00 00 00 01 49 50130: 55 49 41 4C 4A 52 41 41 31 30140: 2D 32 31 34 33 2D 30 31 56 30150:
31 20 89 FB 55 00 00 00 00 78160: 00 00 00 00 00 00 00 00 00 00 00170: 00 00 00 00 00 00 00
00 00 00180: 00 00 00 00 00 00 00 00 00 00190: AA AA 53 46 50 2D 47 45 2D 53200: 20 20 20
20 20 20 20 20 20 20210: 20 20 00 00 00 00 00 00 00 00220: 00 00 00 A2 00 00 00 00 00 00230:
 00 00 00 00 00 00 00 00 00 00240: 00 00 00 00 00 00 00 00 00 00 40250: 00 40 00 00 00 00Router#
```

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

Configuring LAN/WAN-PHY Controllers

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

Note WAN-PHY Mode is not currently supported on the Cisco ASR 920 Series Router.

Configuring the LAN-PHY Mode

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

SUMMARY STEPS

1. **show controllers wanphy** *0/0/1*
2. **configure terminal**
3. **hw-module subslot** *slot/subslot* **enable LAN**
4. exit
5. **show controllers wanphy 0/0/1**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**hw-module subslot** *slot/subslot* **enable LAN** **Example:** `Router(config)# hw-module subslot 0/1 enable LAN`	Configures the LAN PHY mode for the 1-Port 10-Gigabit Ethernet LAN/WAN PHY SPA.
Step 4	exit **Example:**	Exits global-configuration (config) mode and enters privilege-exec mode.

	Command or Action	Purpose
	`Router(config)# exit`	

Step 5	**show controllers wanphy 0/0/1**
	Example:
	`Router# show controllers wanphy 0/0/1`
	`TenGigabitEthernet0/0/1`
	`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 1-Port 10-Gigabit Ethernet LAN/WAN PHY SPA.

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

Note WAN-PHY Mode is not supported on the Cisco ASR 920 Series Router.

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.

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

Configuration Examples

This section includes the following configuration examples:

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

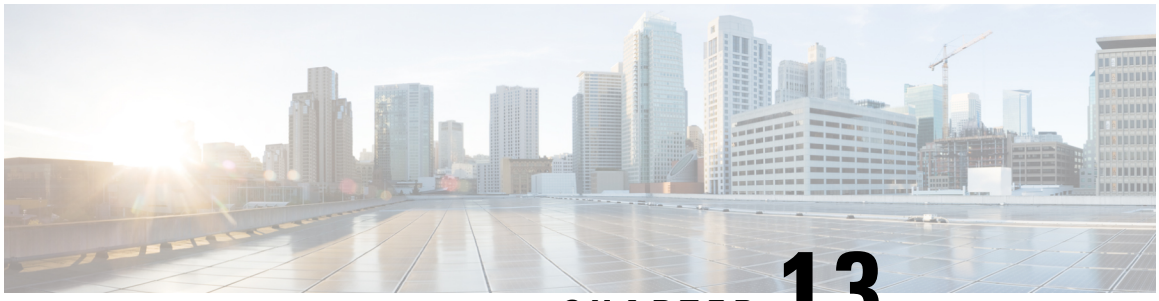
```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 0/0/1
!
! Configure the interface MTU.
!
Router(config-if)# mtu 9216
```

VLAN Encapsulation

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

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitEthernet 0/0/5
!
! Specify the interface address
!
Router(config-if)# service instance 10 ethernet
!
! Configure dot1q encapsulation and specify the VLAN ID.
!
Router(config-if-srv)# 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 see the Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3S.



CHAPTER 13

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

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

- Power failure or removal of power supply cable

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

Prerequisites for Dying Gasp Support

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

Restrictions for Dying Gasp Support

- The dying gasp feature is not supported if you remove the power supply unit (PSU) from the system.
- SNMP trap is sent only on power failure or removal of power supply cable.
- The dying gasp support feature cannot be configured using CLI. To configure hosts using SNMP, refer to the SNMP host configuration examples below.
- In the case of power loss on the Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M Aggregation Services Routers running Cisco IOS-XE Release 3.14.0S and the Cisco ASR-920-12SZ-IM running the Cisco IOS-XE Release 3.16.0S, dying gasp packets are sent to peer routers. However, the system state is not captured in the system logs (syslogs) or SNMP traps.

- The SNMP servers are configured in ascending order. The SNMP server host configured with the lowest IP address has precedence.

Example: Configuring SNMP Community Strings on a Router

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

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

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

Example: Configuring SNMP-Server Host Details on the Router Console

Specifying the recipient of a SNMP notification operation:

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

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

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

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

Environmental Settings on the Network Management Server

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

The following example shows SNMP trap configuration on three hosts:

Configuration example for the first host:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)# snmp-server host 7.0.0.149 vrf Mgmt-intf version 2c public udp-port 6264
```

Configuration example for the second host:

```
Router(config)#
Router(config)# snmp-server host 7.0.0.152 vrf Mgmt-intf version 2c public udp-port 9988
```

Configuration example for the third host:

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

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

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

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

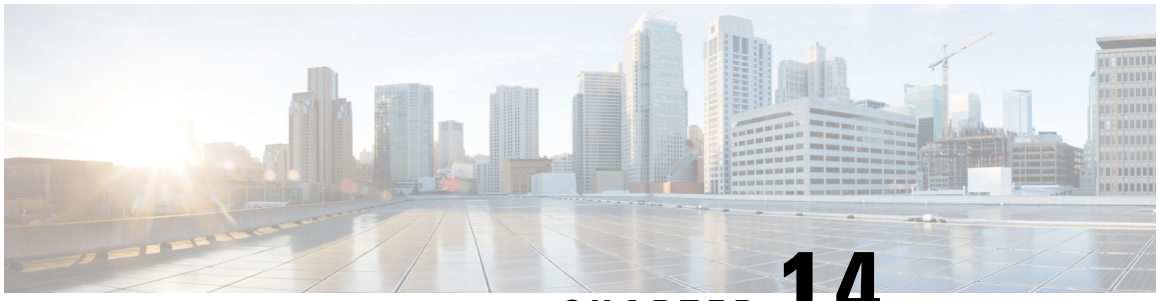
Message Displayed on the Peer Router on Receiving Dying Gasp Notification

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

Displaying SNMP Configuration for Receiving Dying Gasp Notification

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

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



CHAPTER 14

Configuring Pseudowire

This chapter provides information about configuring pseudowire features on the Cisco ASR 920 Series Router.

Pseudowire Overview

Effective Cisco IOS-XE Release 3.18S:

- BGP PIC with TDM Pseudowire is supported on the ASR 920 routers with RSP2 modules.
- BGP PIC for Pseudowires, with MPLS Traffic Engineering is supported on the ASR 920 router with RSP2 modules.

The following sections provide an overview of pseudowire support on the Cisco ASR 920 Series Router.

Limitations

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

- Channel associated signaling (CAS) is not supported on the T1/E1 and OC-3 interface modules.
- BGP PIC is not supported for MPLS/LDP over MLPPP and POS in the core.
- BGP PIC is not supported for Multi-segment Pseudowire or Pseudowire switching.
- BGP PIC is not supported for VPLS and H-VPLS.
- BGP PIC is not supported for IPv6.
- If BGP PIC is enabled, Multi-hop BFD should not be configured using the **bfd neighbor fall-over bfd** command.

- If BGP PIC is enabled, **neighbor** *ip-address* **weight** *weight* command should not be configured.
- If BGP PIC is enabled, **bgp nexthop trigger delay 6** under the **address-family ipv4** command and **bgp nexthop trigger delay 7** under the **address-family vpnv4** command should be configured. For information on the configuration examples for BGP PIC–TDM, see Example: BGP PIC with TDM-PW Configuration.
- If BGP PIC is enabled and the targeted LDP for VPWS Xconnect services are established over BGP, perform the following tasks:
  - Configure Pseudowire-class (pw-class) with encapsulation “mpls”.
  - Configure **no status control-plane route-watch** under the pw-class.
  - Associate the pw-class with the VPWS xconnect configurations.

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

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

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 920 Series Router implementation of EoMPLS PWs is compliant with the RFC 4447 and 4448 standards.

The Cisco ASR 920 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.

CEM Configuration

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.

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), on page 136 sections.

CEM 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 920 Series Router.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	controller {t1 | e1} *slot/port* **Example:** `Router(config)# controller t1 1/0`	Enters controller configuration mode. • Use the slot and port arguments to specify the slot number and port number to be configured. **Note** The slot number is always 0.
Step 4	**cem-group group-number** {**unframed** | **timeslots** *timeslot*} **Example:** **`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. • The **group-number** keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30. • Use the **unframed** keyword to specify that a single CEM channel is being created including all time slots and the framing structure of the line. • Use the **timeslots** keyword and the *timeslot* argument to specify the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.
Step 5	**end** **Example:**	Exits controller configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config-controller)# end`	

Using CEM Classes

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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class cem** *cem-class*
4. Router(config-cem-class)# **payload-size 512**
5. Router(config-cem-class)# exit
6. Router(config)# interface cem 0/0
7. Router(config-if-cem)# **exit**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class cem** *cem-class* **Example:** `Router(config)# class cem mycemclass`	Creates a new CEM class

	Command or Action	Purpose

Step 4	Router(config-cem-class)# **payload-size 512**
	Example:
	`Router(config-cem-class)# dejitter-buffer 10`
	Example:
	`Router(config-cem-class)# idle-pattern 0x55`
		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)# exit	Returns to the config prompt.

Step 6	Router(config)# interface cem 0/0
	Example:
	`Router(config-if)# no ip address`
	Example:
	`Router(config-if)# cem 0`
	Example:
	`Router(config-if-cem)# cem class mycemclass`
	Example:
	`Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls`
		Configure the CEM interface that you want to use for the new CEM class.
		Note The use of the **xconnect** command can vary depending on the type of pseudowire you are configuring.

Step 7	Router(config-if-cem)# **exit** **Example:** `Router(config-if)#`	Exits the CEM interface.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

Configuring CEM Parameters

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

Configuring Payload Size (Optional)

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

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

- E1 = 256 bytes
- T1 = 192 bytes
- DS0 = 32 bytes

Default payload sizes for a structured CEM channel depend on the number of time slots that constitute the channel. Payload size (L in bytes), number of time slots (N), and packetization delay (D in milliseconds) have the following relationship: L = 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.

Setting the Dejitter Buffer Size

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

Setting an Idle Pattern (Optional)

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

Enabling Dummy Mode

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

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

Setting a Dummy Pattern

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

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

Shutting Down a CEM Channel

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

Configuring Structure-Agnostic TDM over Packet (SAToP)

Follow these steps to configure SAToP on the Cisco ASR 920 Series Router:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller [T1|E1] 0/4**
4. **cem-group group-number** {**unframed** | **timeslots** *timeslot* }
5. Router(config)# **interface CEM0/4**
6. Router(config-if)# **xconnect 30.30.30.2 304 encapsulation mpls**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**controller [T1|E1] 0/4** **Example:** `Router(config-controller)# controller t1`	Configures the T1 or E1 interface.
Step 4	**cem-group group-number** {**unframed** | **timeslots** *timeslot* } **Example:** `Router(config-if)# cem-group 4 unframed`	Assigns channels on the T1 or E1 circuit to the CEM channel. This example uses the **unframed** parameter to assign all the T1 timeslots to the CEM channel.
Step 5	Router(config)# **interface CEM0/4** **Example:**	Defines a CEM group.

	Command or Action	Purpose

	`Router(config-if)# no ip address`
	Example:
	`Router(config-if)# cem 4`	

Step 6	Router(config-if)# **xconnect 30.30.30.2 304 encapsulation mpls**	Binds an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 304 to the remote peer 30.30.2.304.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

What to do next

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 920 Series Router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **controller [e1|t1] 0/0**
4. Router(config-controller)# **cem-group 5 timeslots 1-24**
5. Router(config-controller)# **exit**
6. Router(config)# **interface CEM0/5**
7. Router(config-if-cem)# **xconnect 30.30.30.2 305 encapsulation mpls**
8. Router(config-if-cem)# **exit**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Router(config)# **controller [e1|t1] 0/0** **Example:** `Router(config-controller)#`	Enters configuration mode for the E1 or T1 controller.
Step 4	Router(config-controller)# **cem-group 5 timeslots 1-24**	Assigns channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the **timeslots** parameter to assign specific timeslots to the CEM channel.
Step 5	Router(config-controller)# **exit** **Example:** `Router(config)#`	Exits controller configuration.
Step 6	Router(config)# **interface CEM0/5** **Example:** `Router(config-if-cem)# cem 5`	Defines a CEM channel.
Step 7	Router(config-if-cem)# **xconnect 30.30.30.2 305 encapsulation mpls**	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. **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.**
Step 8	Router(config-if-cem)# **exit** **Example:** `Router(config)#`	Exits the CEM interface.
Step 9	**exit** **Example:** `Router(config)# exit`	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 920 Series Router supports EoMPLS pseudowires on EVC interfaces.

For more information about Ethernet over MPLS Pseudowires, see Transportation of Service Using Ethernet over MPLS, on page 130. 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 920 Router.

Follow these steps to configure an Ethernet over MPLS Pseudowire on the Cisco ASR 920 Series Router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **service instance** *number* **ethernet** [*name*]
5. **encapsulation** {**default** | **dot1q** | **priority-tagged** | **untagged**}
6. **xconnect** *peer-ip-address vc-id* {**encapsulation** {**l2tpv3** [**manual**] | **mpls** [**manual**]} | **pw-class** *pw-class-name* }[**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet 0/0/4`	Specifies the port on which to create the pseudowire and enters interface configuration mode. Valid interfaces are physical Ethernet ports.
Step 4	**service instance** *number* **ethernet** [*name*] **Example:** `Router(config-if)# service instance 2 ethernet`	Configure an EFP (service instance) and enter service instance configuration) mode. • The *number* is the EFP identifier, an integer from 1 to 4000.

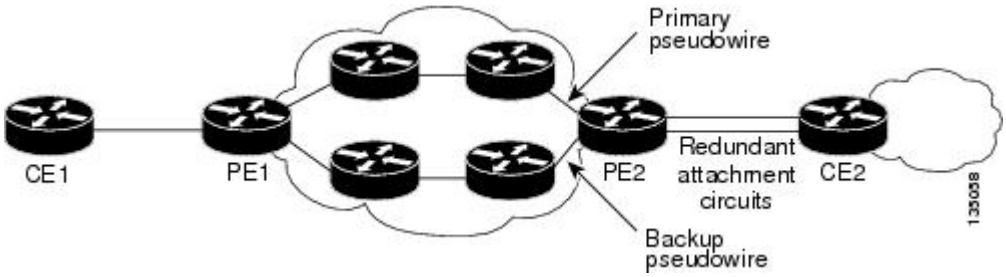
	Command or Action	Purpose
		• (Optional) **ethernet** *name* is the name of a previously configured EVC. You do not need to use an EVC name in a service instance. **Note** You can use service instance settings such as encapsulation, dot1q, and rewrite to configure tagging properties for a specific traffic flow within a given pseudowire session. For more information, see Configuring Ethernet Virtual Connections on the Cisco ASR 920 Router.
Step 5	**encapsulation** {**default** | **dot1q** | **priority-tagged** | **untagged**} **Example:** `Router (config-if-srv)# encapsulation dot1q 2`	Configure encapsulation type for the service instance. • **default**—Configure to match all unmatched packets. • **dot1q**—Configure 802.1Q encapsulation. • **priority-tagged**—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7. • **untagged**—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation.
Step 6	**xconnect** *peer-ip-address vc-id* {**encapsulation** {**l2tpv3** [**manual**] | **mpls** [**manual**]} | **pw-class** *pw-class-name* }[**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}] **Example:** `Router (config-if-srv)# xconnect 10.1.1.2 101 encapsulation mpls`	Binds the Ethernet port interface to an attachment circuit to create a pseudowire. This example uses virtual circuit (VC) 101 to uniquely identify the PW. Ensure that the remote VLAN is configured with the same VC. **Note** When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as **ip route 10.30.30.2 255.255.255.255 10.2.3.4**.
Step 7	**exit** **Example:** `Router(config)# exit`	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 920 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.

The figure below shows an example of pseudowire redundancy.

Figure 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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation mpls**
5. **gigabitethernet** *slot/port*
6. Router(config)# **backup delay** *enable-delay* {*disable-delay* | **never**}
7. Router(config-if)# **xconnect 1.1.1.2 101 encapsulation mpls**
8. Router(config)# **backup peer** *peer-router-ip-address vcid* [**pw-class** *pw-class name*]
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class** [*pw-class-name*] **Example:** `Router(config)# pseudowire-class mpls`	Specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.

	Command or Action	Purpose
Step 4	**encapsulation mpls** **Example:** `Router(config-pw-class)# encapsulation mpls`	Specifies MPLS encapsulation.
Step 5	**gigabitethernet** *slot/port* **Example:** `Router(config)# gigabitethernet 0/0/1`	Enters configuration mode for the serial interface. **Note** The slot number is always 0.
Step 6	Router(config)# **backup delay** *enable-delay* {*disable-delay* | **never**}	Configures the backup delay parameters. Where: • *enable-delay* —Time before the backup PW takes over for the primary PW. • *disable-delay* —Time before the restored primary PW takes over for the backup PW. • **never**—Disables switching from the backup PW to the primary PW.
Step 7	Router(config-if)# **xconnect 1.1.1.2 101 encapsulation mpls**	Binds the Ethernet port interface to an attachment circuit to create a pseudowire.
Step 8	Router(config)# **backup peer** *peer-router-ip-address vcid* [**pw-class** *pw-class name*]	Defines the address and VC of the backup peer.
Step 9	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.

Sample Configurations

The following sections contain sample pseudowire configurations.

Example: CEM Configuration

The following example shows how to add a T1 interface to a CEM group as a part of a SAToP pseudowire configuration.

This section displays a partial configuration intended to demonstrate a specific feature.

```
controller T1 0/0/0
 framing unframed
 clock source internal
 linecode b8zs
 cablelength short 110
 cem-group 0 unframed
```

```
interface CEM0/0/0
 no ip address
 cem 0
  xconnect 18.1.1.1 1000 encapsulation mpls
```

Example: Ethernet over MPLS

PE 1 Configuration

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

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

PE 2 Configuration

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

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

Example: BGP PIC with TDM-PW Configuration

This section lists the configuration examples for BGP PIC with TDM and TDM–Pseudowire.

The below configuration example is for BGP PIC with TDM:

```
router bgp 1
neighbor 18.2.2.2 remote-as 1
neighbor 18.2.2.2 update-source Loopback0
neighbor 18.3.3.3 remote-as 1
neighbor 18.3.3.3 update-source Loopback0
!
address-family ipv4
```

```
  bgp additional-paths receive
  bgp additional-paths install
  bgp nexthop trigger delay 6
  neighbor 18.2.2.2 activate
  neighbor 18.2.2.2 send-community both
  neighbor 18.2.2.2 send-label
  neighbor 18.3.3.3 activate
  neighbor 18.3.3.3 send-community both
  neighbor 18.3.3.3 send-label
  neighbor 26.1.1.2 activate
exit-address-family
!
address-family vpnv4
  bgp nexthop trigger delay 7
  neighbor 18.2.2.2 activate
  neighbor 18.2.2.2 send-community extended
  neighbor 18.3.3.3 activate
  neighbor 18.3.3.3 send-community extended
exit-address-family
```

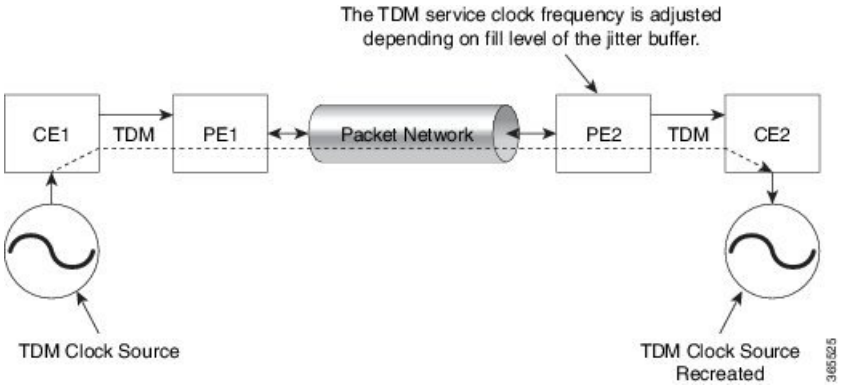
The below configuration example is for BGP PIC with TDM PW:

```
pseudowire-class pseudowire1
encapsulation mpls
control-word
no status control-plane route-watch
status peer topology dual-homed
!
Interface CEM0/0/0
cem 1
   xconnect 17.1.1.1 4101 encapsulation mpls pw-class pseudowire1
```

Adaptive Clock Recovery (ACR)

Adaptive Clock Recovery (ACR) is an averaging process that negates the effect of random packet delay variation and captures the average rate of transmission of the original bit stream. ACR recovers the original clock for a synchronous data stream from the actual payload of the data stream. In other words, a synchronous clock is derived from an asynchronous packet stream. ACR is a technique where the clock from the TDM domain is mapped through the packet domain, but is most commonly used for Circuit Emulation (CEM).

Effective Cisco IOS XE Everest 16.5.1, ACR is supported on the 8-port T1/E1 interface module.



Benefits of ACR for 8 T1/E1 Interface Module

- Customer-edge devices (CEs) can have different clocks from that of the Provide-edge devices (PEs). Every T1/E1 interface module supports eight pseudowires (or the derived clocks).

Prerequisites for ACR Configuration in 8 T1/E1 Interface Module

- Ensure that CEM is configured before configuring the adaptive clock recovery.
- The following must be configured before configuring the ACR:
  - The remote Customer Equipment and the remote Provider Edge device. These can be configured by using the clock source internal and the clock source line commands under the T1/E1 controller.
  - The controller on the local Customer Equipment connected to the ACR router by using the **clock source line**command.
  - PRC or PRS reference clock from a GPS reference to the remote Customer Equipment or remote CEM Provider Edge device.

Restrictions for ACR on 8 T1/E1 Interface Module

- ACR is supported only on the 8-port T1/E1 interface module (A900-IMA8D). It is not supported on the 16-port T1/E1 interface module (A900-IMA16D), the 32-port T1/E1 interface module (A900-IMA32D), or the 4-port OC3 interface module (A900-IMA4OS).
- ACR is supported only for unframed CEM (SAToP) and for fully-framed CEM (CESoPSN). Fully-framed refers to all the timeslots of T1 (1-24) or E1 (1-31) interfaces.
- ACR is supported only for CEM circuits with MPLS PW encapsulation. ACR is not supported for CEM circuits with UDP or IP PW encapsulation.
- The clock recovered by an ACR clock for a CEM circuit is local to that CEM circuit. The recovered clock cannot be introduced to another circuit and also cannot be introduced to the system clock as a frequency input source.
- The clock ID should be unique for the entire device.
- When a CEM group is configured, dynamic change in clock source is not allowed.
- Physical or soft IM OIR causes the APS switchover time to be higher (500 to 600 ms). Shut or no shut of the port and removal of the active working or protect also cause the APS switchover time to be high.

  To overcome these issues, force the APS switchover.

Configuring ACR for T1 Interfaces for SAToP

To configure the clock on T1/E1 interfaces for SAToP in controller mode:

```
enable
configure terminal
controller t1 0/4/3
clock source recovered 15
cem-group 20 unframed
exit
```

To configure the clock recovery on T1/E1 interfaces in global configuration mode:

```
recovered-clock 0 4
clock recovered 15 adaptive cem 3 20
exit
```

Note The clock source recovered configuration on the controller must be completed before configuring the clock recovery in global configuration mode.

Note On the controller, the clock source should be configured before CEM group is configured.

Note Follow a similar procedure to configure to configure CEM ACR for E1 Interfaces for SAToP. Also, follow a similar procedure to configure CEM ACR for T1 and E1 Interfaces for CESoPSN. Use **cem-group** *circuit-id* **timeslots** <*1-24*> | <*1-31*> command instead of **cem-group** *circuit-id unframed* command for the configuration depending on T1 or E1 controller.

To remove the clock configuration in ACR, you must remove the recovery clock configuration in global configuration mode, then remove the CEM circuit, and finally remove the clock source recovered configuration under the controller.

Verifying the ACR Configuration of T1 Interfaces for SAToP

Important Notes

- When multiple ACR clocks are provisioned and if the core network or PSN traffic load primarily has fixed packet rate and fixed size packets, the states of one or more ACR clocks might flap between Acquiring and Acquired states and might not be stable in Acquired state.

  This happens because of the "beating" phenomenon and is documented in *ITU-T G.8261 - Timing and synchronization aspects in packet networks*.

  This is an expected behavior.

- After an ACR clock is provisioned and starts recovering the clock, a waiting period of 15-20 minutes is mandatory before measuring MTIE for the recovered clock.

  This behavior is documented in *ITU-T G.8261 Timing and synchronization aspects in packet networks Appendix 2*.

- When the input stream of CEM packets from the core network or PSN traffic is lost or has many errors, the ACR clock enters the HOLDOVER state. In this state, the ACR clock fails to provide an output clock on the E1/T1 controller. Hence, during the HOLDOVER state, MTIE measurement fails.

  This is an expected behavior.

- When the clock output from the clock master or GPS reference flaps or fails, the difference in the characteristics between the holdover clock at the source device and the original GPS clock may result in the ACR algorithm failing to recover clock for a transient period. The MTIE measurement for the ACR clock fails during this time. After this transient period, a fresh MTIE measurement is performed.

Similarly, when the GPS clock recovers, for the same difference in characteristics, ACR fails to recover clock and MTIE fails for a transient period.

This is an expected behavior.

- When large-sized packets are received along with the CEM packets by the devices in the core network or PSN traffic, CEM packets may incur delay with variance in delay. As ACR is susceptible to delay and variance in delay, MTIE measurement may fail. This behavior is documented in *ITU-T G.8261 section 10*.

  This is an expected behavior.

- For a provisioned ACR clock that is in Acquired state, if the ACR clock configuration under the recovered-clock global configuration mode is removed and then reconfigured, the status of the ACR clock may initially be ACQUIRED and not FREERUN and then move to Acquiring. This happens because the ACR clock is not fully unprovisioned until the CEM circuit and the controller clock source recovered configuration are removed. Hence, the clock starts from the old state and then re-attempts to recover the clock.

  This is an expected behavior.

Use the **show recovered-clock** command to verify the ACR of T1 interfaces for SAToP:

```
Router#show recovered-clock
Recovered clock status for subslot 0/1
---------------------------------------
Clock Type Mode Port CEM Status Frequency Offset(ppb)
1 T1/E1 ADAPTIVE 3 1 ACQUIRED 100
```

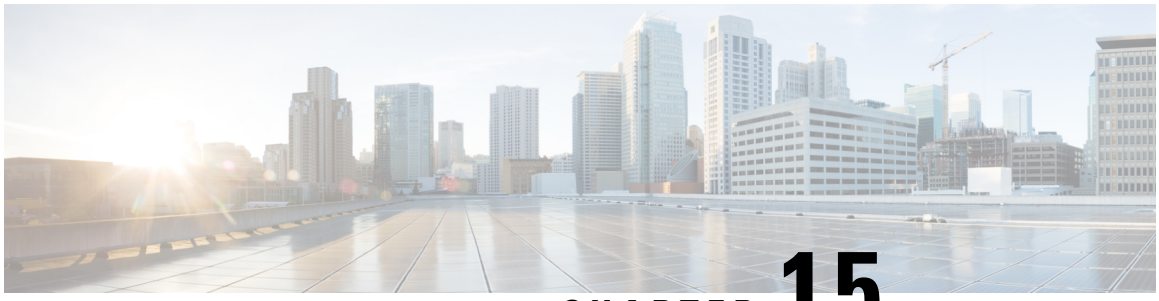
Use the **show running-config** command to verify the recovery of adaptive clock of T1 interfaces:

```
Router#show running-config
controller T1 0/1/2
clock source recovered 1
cem-group 1 unframed
interface CEM0/1/3
cem 1
no ip address
xconnect 2.2.2.2 10
encapsulation mpls
```

Associated Commands

Commands	Links
cem-group	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2440628600
clock source	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp3848511150
clock recovered adaptive cem	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp8894393830

Commands	Links
controller t1	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp1472647421
recovered-clock	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html



CHAPTER 15

Configuring and Monitoring Alarm

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

This chapter includes the following sections:

Monitoring Alarms

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

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

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

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

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

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

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

Network Administrator Checks Console or Syslog for Alarm Messages

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

Enabling the Logging Alarm Command

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

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

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

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

Examples of Alarm Messages

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

SPA REMOVED

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

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

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

SPA RE-INSERTED

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

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

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

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

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

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

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

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

ALARMS for Router

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

SPA Removed

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

SPA Re-Inserted

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

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

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

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

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

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

```
Router# show platform diag
Chassis type: ASR903
Slot: 1, A900-RSP2A-128
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time   : 00:03:41 (00:56:24 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Sub-slot: 0/0, A900-IMA2Z
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time  : 00:04:46 (00:55:19 ago)
Sub-slot: 0/1, A900-IMA8T
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time  : 00:04:46 (00:55:19 ago)
Sub-slot: 0/2, A900-IMA8S
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time  : 00:04:46 (00:55:19 ago)
Sub-slot: 0/3, A900-IMA4OS
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:18 ago)
  Logical insert detect time  : 00:04:46 (00:55:18 ago)
Sub-slot: 0/4, A900-IMA8S1Z
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:18 ago)
  Logical insert detect time  : 00:04:46 (00:55:18 ago)
Sub-slot: 0/5, A900-IMASER14A/S
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:46 (00:55:19 ago)
  Logical insert detect time  : 00:04:46 (00:55:19 ago)
Slot: R0, A900-RSP2A-128
  Running state               : ok, standby
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:24:37 (00:35:28 ago)
  Software declared up time   : 00:31:28 (00:28:36 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Slot: R1, A900-RSP2A-128
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time   : 00:02:33 (00:57:31 ago)
```

```
  Became HA Active time       : 00:34:41 (00:25:23 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Slot: F0,
  Running state               : ok, standby
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:24:37 (00:35:28 ago)
  Software declared up time   : 00:31:45 (00:28:20 ago)
  Hardware ready signal time  : 00:31:39 (00:28:25 ago)
  Packet ready signal time    : 00:33:25 (00:26:40 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Slot: F1,
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:02:33 (00:57:31 ago)
  Software declared up time   : 00:03:23 (00:56:42 ago)
  Hardware ready signal time  : 00:03:14 (00:56:51 ago)
  Packet ready signal time    : 00:04:19 (00:55:46 ago)
  Became HA Active time       : 00:33:25 (00:26:40 ago)
  CPLD version                : 15092360
  Firmware version            : 15.4(3r)S2
Slot: P0, Unknown
  State                       : N/A
  Physical insert detect time : 00:00:00 (never ago)
Slot: P1, A900-PWR550-A
  State                       : ok
  Physical insert detect time : 00:03:17 (00:56:48 ago)
Slot: P2, A903-FAN-E
  State                       : ok
  Physical insert detect time : 00:03:21 (00:56:44 ago)
```

Reviewing and Analyzing Alarm Messages

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

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

Configuring External Alarm Trigger

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

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

Approaches for Monitoring Hardware Alarms

Onsite Network Administrator Responds to Audible or Visual Alarms

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

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

Clearing Audible and Visual Alarms

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

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

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

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

How to Configure External Alarms

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **alarm-contact** *contact-number* **description** *string*
4. **alarm-contact** {*contact-number* | **all** {**severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}}
5. **exit**
6. **show facility-alarm status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**alarm-contact** *contact-number* **description** *string* **Example:** `Router(config)#alarm-contact 2 description door sensor`	(Optional) Configures a description for the alarm contact number. • The contact-number can be from 1 to 4. • The description string can be up to 80 alphanumeric characters in length and is included in any generated system messages
Step 4	**alarm-contact** {*contact-number* | **all** {**severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}} **Example:** `Router(config)#alarm-contact 2 severity major`	Configures the trigger and severity for an alarm contact number or for all contact numbers. • Enter a contact number (1 to 4) or specify that you are configuring **all** alarms. • For **severity**, enter **critical**, **major**, or **minor**. If you do not configure a severity, the default is **minor**. • For **trigger**, enter **open** or **closed**. If you do not configure a trigger, the alarm is triggered when the circuit is **closed**.
Step 5	**exit** **Example:** `Router#exit`	Exits the configuration mode.
Step 6	**show facility-alarm status** **Example:** `Router#show facility-alarm status`	Displays configured alarms status.

Example

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

Source                    Time                   Severity      Description [Index]
------                    ------                 --------      -------------------
subslot 0/0               Sep 21 2016 15:19:55   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/1               Sep 21 2016 15:19:12   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/2               Sep 21 2016 15:16:59   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/3               Sep 21 2016 15:18:10   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/5               Sep 21 2016 15:16:11   CRITICAL      Active Card Removed OIR
```

```
Alarm [0]
subslot 0/6                Sep 21 2016 15:15:45   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/7                Sep 21 2016 15:14:22   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/8                Sep 21 2016 15:10:33   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/9                Sep 21 2016 12:00:43   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/10               Sep 21 2016 15:11:49   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/13               Sep 21 2016 14:56:35   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/14               Sep 21 2016 14:56:29   CRITICAL      Active Card Removed OIR
Alarm [0]
subslot 0/15               Sep 21 2016 14:56:33   CRITICAL      Active Card Removed OIR
Alarm [0]
Fan Tray Bay 0             Sep 21 2016 11:50:39   CRITICAL      Fan Tray Module Missing [0]
Router(config)#
```

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

Alarm Filtering Support

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

Information About Alarm Filtering Support

Overview of Alarm Filtering Support

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

CISCO-ENTITY-ALARM-MIB

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

ceAlarmGroup

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

Following are the objects in ceAlarmGroup:

- ceAlarmCriticalCount
- ceAlarmMajorCount

- ceAlarmMinorCount
- ceAlarmCutoff
- ceAlarmFilterProfile
- ceAlarmSeverity
- ceAlarmList

ceAlarmFilterProfileTable

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

ceAlarmFilterProfile

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

ceAlarmHistTable:

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

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

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

ceAlarmDescrTable:

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

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

ceAlarmTable:

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

Prerequisites for Alarm Filtering Support

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

Restrictions for Alarm Filtering Support

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

How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications

Configuring Alarm Filtering for Syslog Messages

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

```
enable
configure terminal
logging alarm 2
show facility-alarm status
```

Configuring Alarm Filtering for SNMP Notifications

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

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

Configuration Examples for Alarm Filtering Support

Configuring Alarm Filtering for Syslog Messages: Example

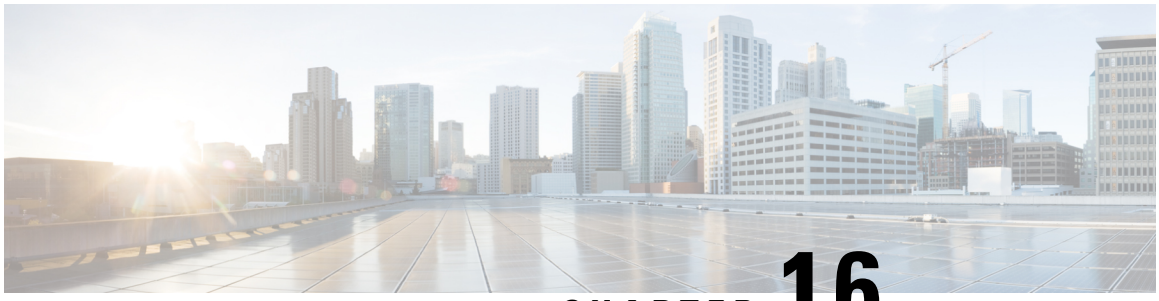
The following example shows how to configure an alarm filter for syslog messages:

Configuring Alarm Filtering for SNMP Notifications: Example

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

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

```
xcvr container 0/5/7       Jun 07 2016 13:37:43   INFO          Transceiver Missing [0]
```



CHAPTER 16

Quality of Service

The following sections describe support for Quality of Service features on the Cisco ASR 920 Series Router.

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 920 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.

Global QoS Limitations

The following limitations apply to multiple QoS features for the Cisco ASR 920 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 920 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 920 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-920 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

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 920 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 920 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 rage 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 supported with the access-list permit and ip access-list extended commands, whereas for IPv6 QoS ACL neq configuration is not supported.
- 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 920 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 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 920 Series Router:

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 920 Series Router:

- The Cisco ASR 920 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 Cisco ASR 920 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 920 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 920 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 920 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 920 Series Router does not support policing on egress interfaces.

Queuing

The Cisco ASR 920 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 920 Series Router does not support queuing on ingress interfaces.

Egress Queuing Limitations

The Cisco ASR 920 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 Cisco ASR 920 Series Router supports scheduling on egress interfaces. Scheduling is not supported on ingress interfaces.

Ingress Scheduling Limitations

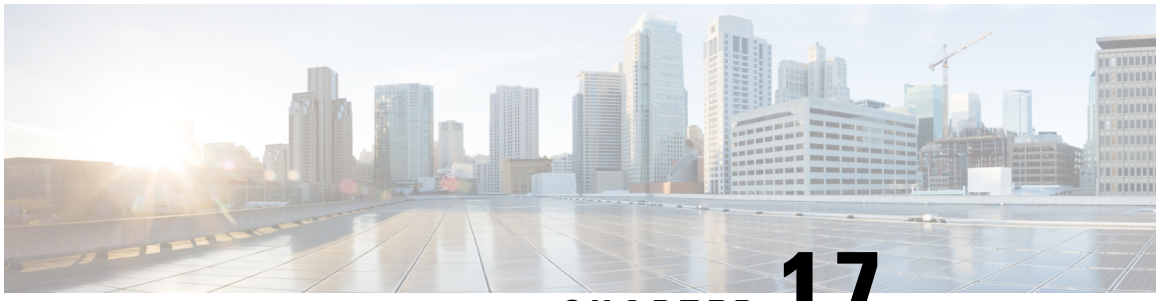
The Cisco ASR 920 Series Router does not support scheduling on ingress interfaces.

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.



CHAPTER 17

Tracing and Trace Management

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 920 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 920 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 920 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 920 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, on page 170 section 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.

The table below shows all of the trace levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

Table 12: 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 920 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 920 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 920 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:

```
Router# show platform software trace level forwarding-manager rp active
Module Name                      Trace Level
----------------------------------------------
acl                              Notice
binos                            Notice
binos/brand                      Notice
bipc                             Notice
bsignal                          Notice
btrace                           Notice
cce                              Notice
cdllib                           Notice
cef                              Notice
chasfs                           Notice
chasutil                         Notice
erspan                           Notice
ess                              Notice
ether-channel                    Notice
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
fman_rp                          Notice
fpm                              Notice
fw                               Notice
icmp                             Notice
interfaces                       Notice
iosd                             Notice
ipc                              Notice
```

```
ipclog                          Notice
iphc                            Notice
ipsec                           Notice
mgmte-acl                       Notice
mlp                             Notice
mqipc                           Notice
nat                             Notice
nbar                            Notice
netflow                         Notice
om                              Notice
peer                            Notice
qos                             Notice
route-map                       Notice
sbc                             Notice
services                        Notice
sw_wdog                         Notice
tdl_acl_config_type             Notice
tdl_acl_db_type                 Notice
tdl_cdlcore_message             Notice
tdl_cef_config_common_type      Notice
tdl_cef_config_type             Notice
tdl_dpidb_config_type           Notice
tdl_fman_rp_comm_type           Notice
tdl_fman_rp_message             Notice
tdl_fw_config_type              Notice
tdl_hapi_tdl_type               Notice
tdl_icmp_type                   Notice
tdl_ip_options_type             Notice
tdl_ipc_ack_type                Notice
tdl_ipsec_db_type               Notice
tdl_mcp_comm_type               Notice
tdl_mlp_config_type             Notice
tdl_mlp_db_type                 Notice
tdl_om_type                     Notice
tdl_ui_message                  Notice
tdl_ui_type                     Notice
tdl_urpf_config_type            Notice
tdllib                          Notice
trans_avl                       Notice
uihandler                       Notice
uipeer                          Notice
uistatus                        Notice
urpf                            Notice
vista                           Notice
wccp                            Notice
```

Setting a Tracing Level

To set a tracing level for any module on the Cisco ASR 920 Series Router, or for all modules within a process on the Cisco ASR 920 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

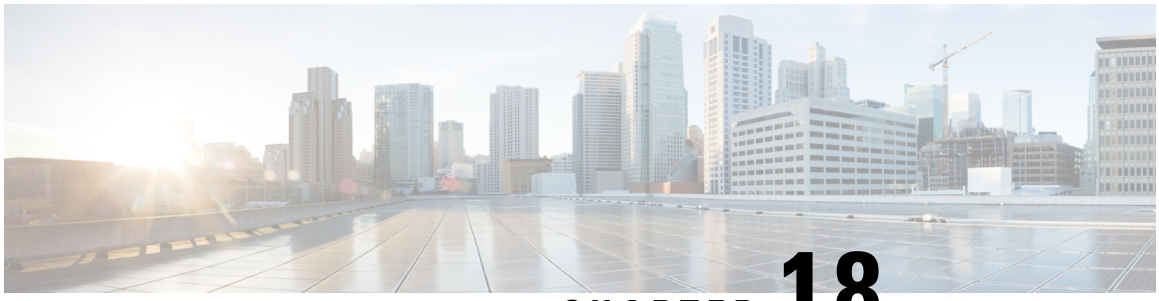
See the **set platform software trace** command reference for additional information about the options for this command.

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
```



CHAPTER 18

BCP Support on MLPPP

This feature module describes how to configure Bridge Control Protocol (BCP) Support over Multilink PPP (MLPPP).

Note This feature is only applicable for Cisco ASR 900 RSP2 Module.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information for BCP Support on MLPPP section.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for BCP Support on MLPPP

- Cisco IOS XE Everest 16.5.1 or a later release that supports the BCP Support on MLPPP feature must be installed previously on the Cisco ASR 900.

Restrictions for BCP Support on MLPPP

- IPv6 is not supported.
- Routing is not supported, hence, BDI is also not supported on BCP over MLPPP.

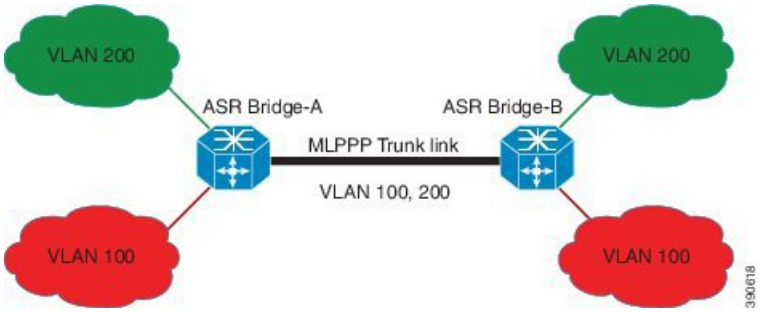
- Spanning Tree Protocol (STP) and Resilient Ethernet Protocol (REP) are not supported.
- Jumbo frames are not supported.
- Supports 16 T1/E1 and OC3 IM only. A maximum number of 16 (0-15) links per MLPPP bundle are supported, where traffic rate is not beyond MLPPP bandwidth. For E1 link, 16 E1 serial interfaces can be in one MLPPP bundle. For T1, 16 T1 links can be in one MLPPP bundle.
- The following encapsulations are not supported: **QinQ**, **dot1ad**, and **dot1ad-dot1q** .
- You cannot configure **default** or **untagged** encapsulations on two different multilinks. When **default** is configured on a multilink, you can configure another EFP as **untagged** on the same multilink. For **untagged**, the same multilink cannot have another EFP configured as **untagged**.
- Two different multilinks cannot bridge the same encapsulated VLAN.
- The same bridge domain cannot be configured twice on the same interface.
- Connectivity Fault Management (CFM), Y.1731, and Layer 2 protocol forward tagged are not supported.
- Set qos-group is not supported in the output policy of physical Gigabit interface and EVC of the multilink interface. Set qos-group on ASR 903 will not mark the packet. The scope of the set qos-group is limited to the router.
- QoS policy is not supported on multilink at the interface level. However, it is supported on different EVCs of the multilink interfaces.
- Qos-group classification will work only on the egress interface or EFP interface.
- The MLPPP interface bundle supports only a maximum of 64 EVCs.
- A miximum of 64 VLANs are supported across all the MLPPPs.
- Layer 3 traffic with default encapsulation is not supported.
- Multicast and IGMP is not supported.
- For ingress classification to work, it should be classified based on “match cos inner <>” or “match vlan inner <>”.
- Layer 2 QoS behavior is supported only on tagged/priority tagged packets. It is not supported for untagged packets.
- Only 1r2C policer is supported at the egress.
- With BCP on MLPPP, the COS bits in the paylod are not preserved end to end.

Information About BCP Support on MLPPP

The BCP, as described in RFC 3518, is responsible for configuring, enabling and disabling the bridge protocol modules on both ends of the point-to-point link. The BCP feature enables forwarding of Ethernet frames over serial networks, and provides a high-speed extension of enterprise LAN backbone traffic through a metropolitan area.

When BCP is supported on MLPPP, it enables transport of Ethernet Layer 2 frames through MLPPP. In the following diagram, Bridge-A is connected to Bridge-B using MLPPP. The MLPPP bundle acts as a trunk link connecting Bridge-A and Bridge-B, transporting multiple VLANs. Using this feature, the hosts in VLAN 100, who are connected to Bridge-A, can talk to the hosts in VLAN 200, who are connected to Bridge-B.

Figure 4: BCP over MLPPP



Supported Profiles and Protocols

- Ethernet II frames
- 802.1Q tagged frames
- IPv4 packets
- Frame sizes from 64 to 1522 octets

Quality of Service

The Ethernet Layer 2 traffic is classified on the egress at the EVC of the Multilink interface based on IP DSCP or VLAN CoS bits. Based on this classification, egress policing (bandwidth percent or priority percent) is achieved. You can also re-mark the QoS field. The following table lists the options available for re-marking.

Table 13: Re-Marking Options

IP DSCP	VLAN CoS or PCP Bits
Set IP DSCP (re-mark IP DSCP)	Set IP DSCP
Set VLAN CoS or Priority Code Point (PCP) Bits	Set VLAN CoS Bits (re-mark VLAN CoS or PCP Bits)
Bandwidth Percent or Priority Percent	Bandwidth Percent or Priority Percent

How to Configure BCP Support on MLPPP

Configuring Multiple EFPs Bridged Through the Same Link

To bridge multiple EFPs through the same multilink, you should create two EFPs and add them to the multilink.

To configure an EFP and a multilink, complete the following tasks:

Configuring an EFP

To configure an EFP, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *number* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **rewrite ingress tag pop 1 symmetric**
7. **bridge-domain** *bridge-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 50`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies that encapsulation modification occurs on packets at ingress.
Step 7	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 100`	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.

Adding an EFP to a Multilink

To add an EFP to a multilink, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *number* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **rewrite ingress tag pop 1 symmetric**
7. **bridge-domain** *bridge-id*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Multilink 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 60`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies that encapsulation modification occurs on packets at ingress.
Step 7	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 100`	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.
Step 8	**exit** **Example:** `Router(config-if-srv)# exit`	Exits service instance configuration mode and enters the interface configuration mode. **Note** Repeat Step 4 to Step 7 to add another EFP to the Multilink.

Configuring Multiple Encapsulated VLANs Bridged Through Different Multilinks

You should create two encapsulated VLANs and add them to two multilinks for this configuration to work.

To configure multiple encapsulated VLANs bridged through different multilinks, complete the following tasks:

Adding an Encapsulated VLAN to Multilinks

To add an encapsulated VLAN to separate multilinks, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *number* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **rewrite ingress tag pop 1 symmetric**
7. **bridge-domain** *bridge-id*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Multilink 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 10 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 60`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 6	**rewrite ingress tag pop 1 symmetric** **Example:**	Specifies that encapsulation modification occurs on packets at ingress.

	Command or Action	Purpose
	`Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	
Step 7	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 100`	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.
Step 8	**exit** **Example:** `Router(config-if-srv)# exit`	Exits service instance configuration mode and enters the interface configuration mode. **Note** Repeat steps 3 to 7 to create another multilink and add the VLAN information.

Configuring QoS for BCP Support on MLPPP

The egress policy at the EVC of the multilink interface matches the IP DSCP value and VLAN CoS bits. Based on this classification it re-marks these values and performs egress policing (Priority percent or Bandwidth percent), shaping, priority shaper, BRR/BRP.

To configure QoS for BCP Support on MLPPP, complete the following tasks:

Note Define a QoS policy, and apply it to the MLPPP interface, and configure a matching policy on the EFP interface.

Defining a QoS Policy

To define a QoS policy, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map match-any** *class-map-name*
4. **match ip dscp** *dscp-list*
5. **class-map match-any** *class-map-name*
6. **match qos-group** *qos-group-value*
7. **policy-map** *policy-map-name*
8. **class** *class-name*
9. **priority percent** *percentage*
10. **set ip dscp** *ip-dscp-value*
11. **class** *class-name*
12. **bandwidth percent** *percentage*
13. **set qos-group** *group-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map match-any** *class-map-name* **Example:** `Router(config)# class-map match-any dscpaf11`	Creates a class map to be used for matching packets to a specified class and enters QoS class-map configuration mode. • *class-map-name*—Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map.
Step 4	**match ip dscp** *dscp-list* **Example:** `Router(config-cmap)# match ip dscp af11`	Matches IP DSCP packeting using Assured Forwarding (AF) by entering the binary representation of the DSCP value.
Step 5	**class-map match-any** *class-map-name* **Example:** `Router(config-cmap)# class-map match-any qos-group3`	Creates a class map to be used for matching packets to a specified class.
Step 6	**match qos-group** *qos-group-value* **Example:** `Router(config-cmap)# match qos-group 3`	Identifies a specific quality of service (QoS) group value as a match criterion. • *qos-group-value*—The exact value used to identify a QoS group value. The valid range is from 0 to 7.
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config-cmap)# policy-map bcpmlpppqos`	Creates a policy map that can be attached to one or more interfaces. • *poliicy-map-name*—Name of the policy map.
Step 8	**class** *class-name* **Example:** `Router(config-pmap)# class dscpaf11`	Specifies the name of the class whose policy you want to create or change. Alternatively, is used to specify the default class (commonly known as the class-default class) before you configure its policy. • *class-name*—Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map. .
Step 9	**priority percent** *percentage* **Example:**	Provides priority to a class of traffic belonging to a policy map.

	Command or Action	Purpose
	`Router(config-pmap-c)# priority percent 20`	• *percentage*—Total available bandwidth to be set aside for the priority class. The valid range is from 1 to 100.
Step 10	**set ip dscp** *ip-dscp-value* **Example:** `Router(config-pmap-c)# set ip dscp ef`	Marks a packet by setting the IP DSCP value in the type of service (ToS) byte. • *ip-dscp-value*—IP DSCP value; The valid values are from 0 to 63.
Step 11	**class** *class-name* **Example:** `Router(config-pmap-c)# class qos-group3`	Specifies the name of the class whose policy you want to create or change. Alternatively, is used to specify the default class (commonly known as the class-default class) before you configure its policy.
Step 12	**bandwidth percent** *percentage* **Example:** `Router(config-pmap-c)# bandwidth percent 20`	Specifies the bandwidth allocated for a class belonging to a policy map. • *percentage*—Specifies the percentage of guaranteed bandwidth based on an absolute percent of available bandwidth to be set aside for the priority class or on a relative percent of available bandwidth. The valid range is from 1 to 100.
Step 13	**set qos-group** *group-id* **Example:** `Router(config-pmap-c)# set qos-group 4`	Sets a QoS group identifier (ID) that can be used later to classify packets. • *group-id*—group-id—Group ID number. The valid range is from 0 to 99.

Applying a QoS Policy on an MLPPP Interface

To apply a QoS policy on an MLPPP interface, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *number* **ethernet**
5. **service-policy output** *policy-map-name*
6. **encapsulation dot1q** *vlan-id*
7. **rewrite ingress tag pop 1 symmetric**
8. **bridge-domain** *bridge-id*

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Multilink 5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**service instance** *number* **ethernet** **Example:** `Router(config-if)# service instance 20 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • *number*—EFP identifier; an integer from 1 to 4000.
Step 5	**service-policy output** *policy-map-name* **Example:** `Router(config-if)# service-policy output bcpmlpppqos`	Attaches a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC. • *policy-map-name*—The name of a service policy map (created using the **policy-map** command) to be attached.
Step 6	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 50`	Configures encapsulation type for the service instance. • *vlan-id*—Virtual LAN identifier. The valid range is from 1 to 4094.
Step 7	**rewrite ingress tag pop 1 symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies that encapsulation modification occurs on packets at ingress.
Step 8	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 100`	Configures the bridge domain ID. • *bridge-id*—Bridge domain number. The valid range is from 1 to 4094.

Verifying BCP Support on MLPPP

To display the Multilink PPP bundle information on various interfaces on a router, use the **show** command, as described in the following example:

```
Router# show ppp multilink interface multilink 1

Multilink1
  Bundle name: ASR1
  Remote Endpoint Discriminator: [1] ASR1
  Local Endpoint Discriminator: [1] ASR2
  Bundle up for 17:06:50, total bandwidth 20480, load 6/255
  2 receive classes, 2 transmit classes
  Receive buffer limit 123040 bytes per class, frag timeout 1000 ms
  Bundle is Distributed
  Receive Class 0:
```

```
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0xB9026C received sequence
  Receive Class 1:
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x5D2E8F received sequence
  Transmit Class 0:
    0x5CBA5 sent sequence
  Transmit Class 1:
    0x146FA1 sent sequence
 Distributed MLP. Multilink in Hardware.
 Distributed Fragmentation is on. Fragment size: 256.
 Bundle status is: active
  Member links: 10 active, 0 inactive (max 255, min not set)
    Se0/6:0, since 01:36:49, 7680 weight, 256 frag size
    Se0/2:0, since 01:26:26, 7680 weight, 256 frag size
    Se0/5:0, since 01:25:18, 7680 weight, 256 frag size
    Se0/9:0, since 01:25:17, 7680 weight, 256 frag size
    Se0/1:0, since 01:24:25, 7680 weight, 256 frag size
    Se0/4:0, since 01:24:20, 7680 weight, 256 frag size
    Se0/0:0, since 01:24:18, 7680 weight, 256 frag size
    Se0/7:0, since 01:24:17, 7680 weight, 256 frag size
    Se0/8:0, since 01:23:09, 7680 weight, 256 frag size
    Se0/3:0, since 01:23:08, 7680 weight, 256 frag size
```

Configuration Examples for BCP Support on MLPPP

Example: Configuring an EFP

The following are the examples of two ways in which you can configure an EFP.

Method 1

```
enable
configure terminal
interface GigabitEthernet 0/0
service instance 10  ethernet
encapsulation dot1q 50
rewrite ingress tag pop 1 symmetric
bridge-domain 100
```

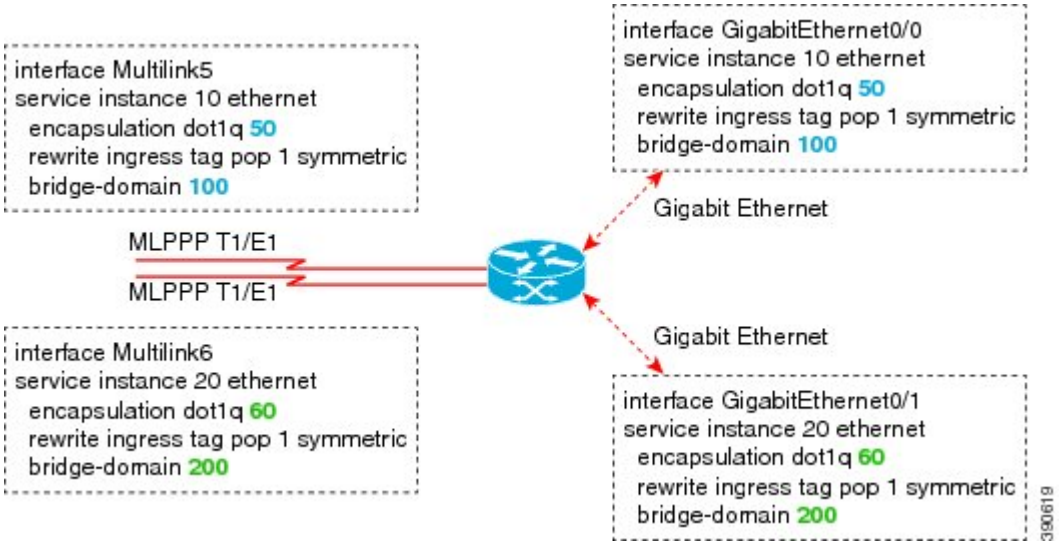
Method 2

```
enable
configure terminal
interface GigabitEthernet 0/0
service instance 10  ethernet
encapsulation dot1q 50
rewrite ingress tag pop 1 symmetric
exit
configure terminal
bridge-domain 100
member Multilink1 service-instance 100
```

Example: Multilink with a Single EFP

The following is a sample configuration of a multilink with a single EFP.

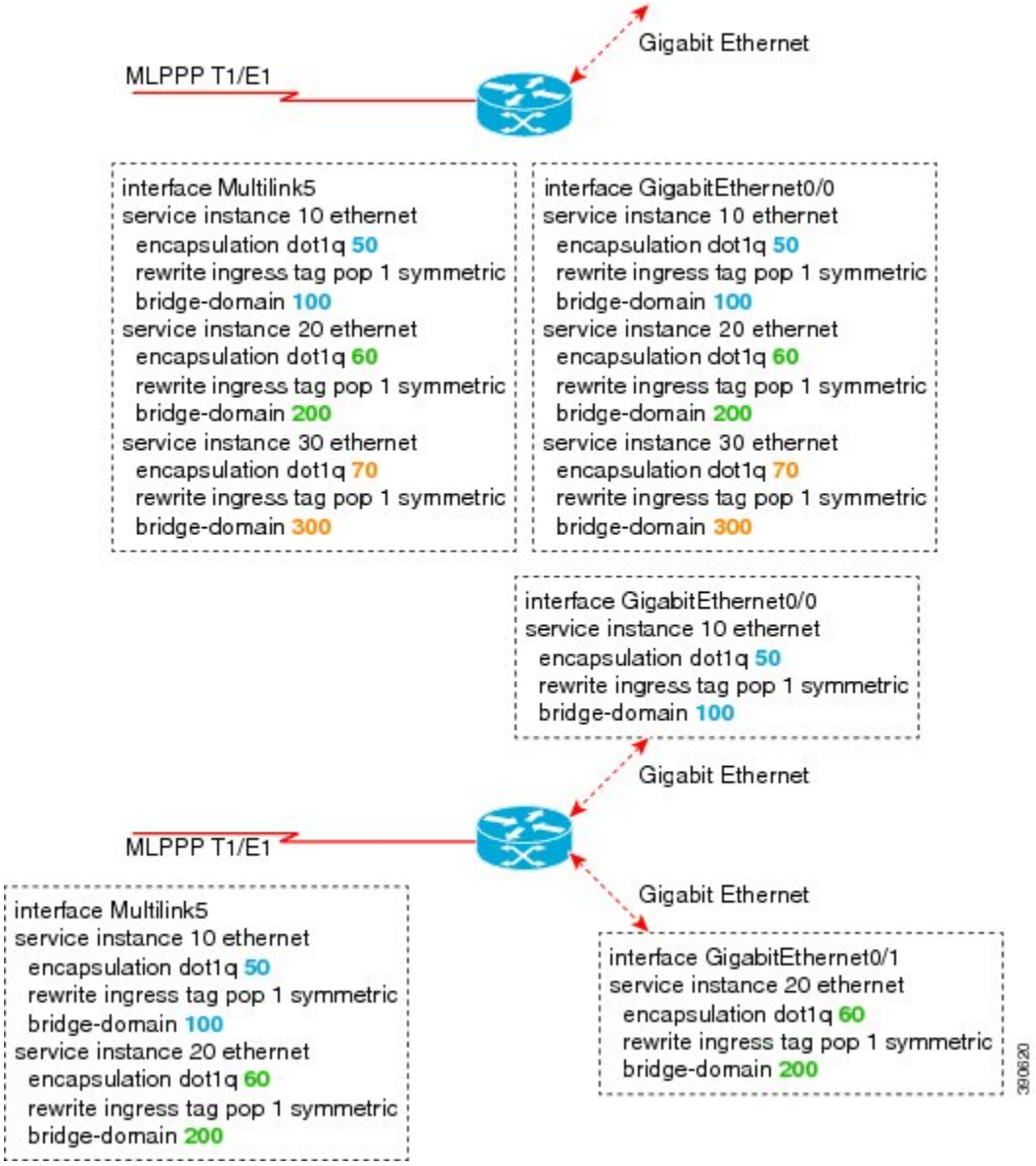
Figure 5: Multilink with a Single EFP



Example: Multilink with Multiple EFPs

The following is a sample configuration of a multilink with multiple EFPs.

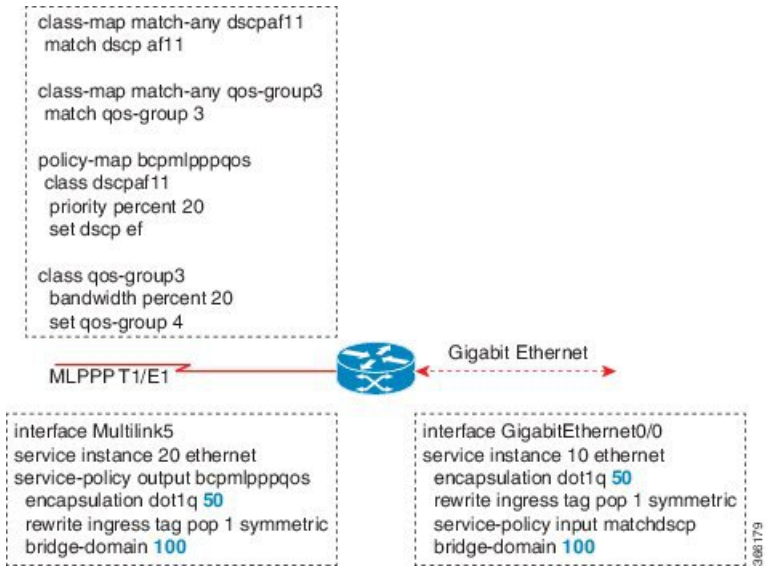
Figure 6: Multilink with Multiple EFPs



Example: Multilink with QoS

The following is a sample configuration of Multilink with QoS:

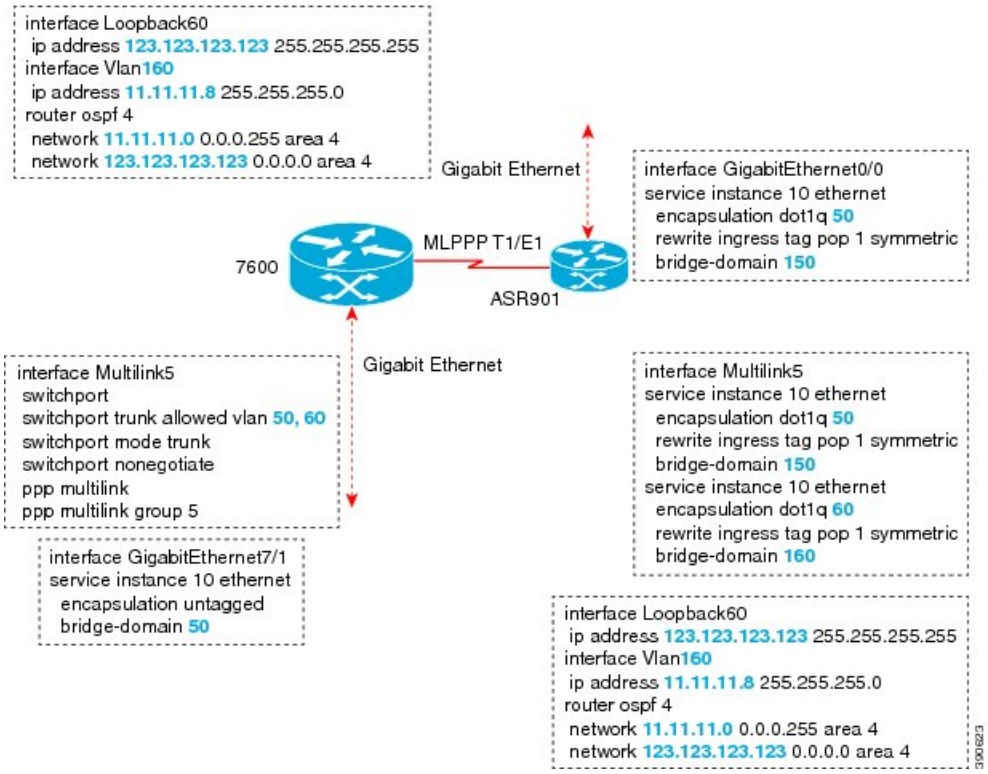
Figure 7: Multilink with QoS



Example: Multilink Between Cisco ASR 903 Series Routers and Cisco C7600 Series Routers

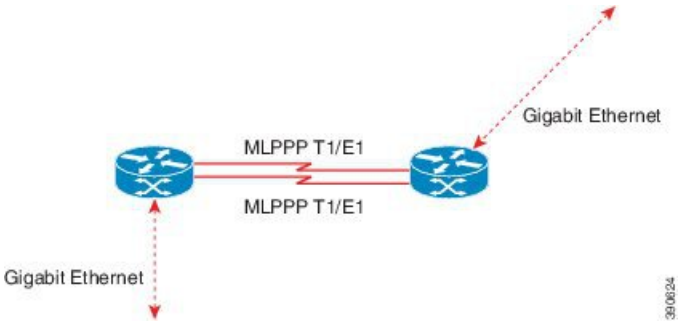
The following is a sample configuration of multilink between a Cisco ASR 903 Series Routers and Cisco C7600 Series Routers:

Figure 8: Multilink Between Cisco ASR 903 Series Routers and Cisco C7600 Series Routers



Example: Multilink with Maximum 10 Links

The following is a sample configuration of multilink with maximum 10 links.



The following sample configurations show how to configure multilink with maximum 10 links.

Policy Map 1

```
class-map match-any qos-group1
match qos-group 1
class-map match-any qos-group2
match qos-group 2
class-map match-any qos-group3
```

```
match qos-group 3
class-map match-any qos-group4
match qos-group 4
class-map match-any qos-group5
match qos-group 5
class-map match-any qos-group6
match qos-group 6
class-map match-any qos-group7
match qos-group 7

policy-map bcpmlpppqos
class qos-group1
priority percent 20
set qos-group 2
class qos-group2
bandwidth percent 20
set qos-group 3
class qos-group3
bandwidth percent 10
set qos-group 4
class qos-group4
bandwidth percent 5
set qos-group 5
class qos-group5
bandwidth percent 30
set qos-group 6
class qos-group7
bandwidth percent 15
set qos-group 1
```

Policy Map 2

```
class-map match-any dscpaf11
match ip dscp af11
class-map match-any dscpaf12
match ip dscp af12
class-map match-any dscpaf21
match ip dscp af21
class-map match-any dscpaf31
match ip dscp af31
class-map match-any dscpcs1
match ip dscp cs1
class-map match-any dscpef
match ip dscp ef
class-map match-any dscpdefault
match ip dscp default

policy-map bcpmlpppdscp
class dscpaf11
priority percent 20
set ip dscp af12
class dscpaf12
bandwidth percent 20
set ip dscp af13
class dscpaf21
bandwidth percent 10
set ip dscp af22
class dscpaf31
bandwidth percent 5
set ip dscp af32
class dscpcs1
bandwidth percent 30
```

```
set ip dscp cs2
class dscpef
bandwidth percent 10
set ip dscp cs7
class dscpdefault
bandwidth percent 5
set ip dscp cs5
```

MLPPP-GIG - 1

```
interface Multilink1
service instance 1 ethernet
service-policy output bcpmlpppqos
  encapsulation  untagged
    bridge-domain 3000

interface Multilink2
service instance 1 ethernet
service-policy output bcpmlpppqos
  encapsulation   dot1q  50
    bridge-domain 2000
service instance 2 ethernet
  encapsulation  dot1q  60
    bridge-domain 2001

interface gigabitethernet 0/5
service instance 1 ethernet
  encapsulation   dot1q  50
    bridge-domain 2000
service instance 2 ethernet
  encapsulation  dot1q  60
    bridge-domain 2001
service instance 3 ethernet
  encapsulation  untagged
    bridge-domain 3000
```

ADD-MLPPP-GIG - 1

```
interface Multilink1
service instance 2 ethernet
service-policy output bcpmlpppqos
  encapsulation   dot1q  70
    bridge-domain 3001

interface gigabitethernet 0/5
service instance 4 ethernet
  encapsulation   dot1q  70
    bridge-domain 3001
```

MLPPP-GIG-2

```
interface Multilink1
service instance 1 ethernet
service-policy output bcpmlpppdscp
  encapsulation  untagged
    bridge-domain 3000
```

```
interface Multilink2
service instance 2 ethernet
service-policy output bcpmlpppdscp
  encapsulation  dot1q  any
    bridge-domain 3001

interface gigabitethernet 0/5
service instance 1 ethernet
  encapsulation  untagged
    bridge-domain 3000
service instance 2 ethernet
  encapsulation  dot1q any
    bridge-domain 3001
```

MLPPP-GIG-3

```
interface Multilink1
service instance 1 ethernet
service-policy output bcpmlpppdscp
  encapsulation  default
    bridge-domain 3000

interface gigabitethernet 0/5
service instance 1 ethernet
  encapsulation  default
    bridge-domain 3000
```

Sample Configuration of MLPPP Bundled 10 Member Links

```
interface Multilink1
 no ip address
 load-interval 30
 ppp pfc local request
 ppp pfc remote apply
 ppp acfc local request
 ppp acfc remote apply
 ppp multilink
 ppp multilink interleave
 ppp multilink group 1
 ppp multilink fragment size 256
 ppp multilink multiclass
 service instance 102 ethernet
 service-policy output bcpmlpppqos
  encapsulation dot1q 102
  rewrite ingress tag pop 1 symmetric
  bridge-domain 102
 !

interface Serial0/0:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/1:0
 no ip address
 encapsulation ppp
 ppp multilink
```

```
 ppp multilink group 1
interface Serial0/2:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/3:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/4:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/5:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/6:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/7:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/8:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
interface Serial0/9:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Additional References

The following sections provide references related to BCP Support on MLPPP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 3518	*Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP)*

Technical Assistance

Table 14: Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for BCP Support on MLPPP

Feature Name	Releases	Feature Information
BCP Support on MLPPP	Cisco IOS XE Everest 16.5.1	This feature was introduced on the Cisco ASR 903 Series Routers.