Cisco ASR 920 Series Aggregation Services Router Configuration Guide, Cisco IOS XE Release 3S

First Published: 2014-07-29

Last Modified: 2018-09-10

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 and ASR-920-8S4Z-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-920-8S4Z-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-920-8S4Z-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	Presen
Time of Day port	Present	Present	Not Present	Not Present	Not Present	Presen
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.
- Starting with Cisco IOS XE Everest 16.9.1, ASR 920-12SZ-IM, Cisco ASR-920-12SZ-A, and Cisco ASR-920-12SZ-D routers only load No Payload Encryption (NPE) images. If a non-NPE image is loaded, the routers stop responding.

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-920-8S4Z-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 2-7 are Gigabit Ethernet SFP ports.
- Interfaces 8-11 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
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 and ASR-920-8S4Z-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
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.

<table>
<tr><th>Command</th><th>Comment</th></tr>
<tr><td><pre>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)#</pre></td><td>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.</td></tr>
<tr><td><pre>Router(config-if)# ip ?
Interface IP configuration subcommands:
access-group Specify access control for
packets
accounting Enable IP accounting on this
interface
address Set the IP address of an interface
authentication authentication subcommands
bandwidth-percent Set EIGRP bandwidth limit
broadcast-address Set the broadcast address
of an 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</pre></td><td>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.</td></tr>
</table>

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 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 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
2  55497216 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

- Use the power switch to turn off the router and then turn it on again.
- 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.
- Type **confreg 0x2142** at the ROMMON.

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

  The router reboots, but ignores the saved configuration.

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

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

```
(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

Note The Cisco ASR 920 Series Router (ASR-920-20SZ-M, 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 TFTP server, 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 TFTP server must be turned green.
- DHCP server should be configured to ensure reachability to 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, ASR-920-10SZ-PD, ASR-920-8S4Z-PD, ASR-920-12SZ-D and ASR-920-12SZ-A) have a ZTP button on the front panel.

The Cisco ASR 920 Series Routers (ASR-920-20SZ-M, 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
    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 TFTP server. 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 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) and default router address to the router.
3. If the TFTP option (150) is present, the router requests a bootstrap configuration that can be stored in any of the following files: PID-<mac-address>, network-confg, router-confg, ciscortr.cfg, or cisconet.cfg.

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
!
{ncs router-specifc configuration content}
!
end
```

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, ASR-920-10SZ-PD, ASR-920-8S4Z-PD ASR-920-12SZ-D and ASR-920-12SZ-A):

Process	PWR LED	STAT LED
Press ZTP button	Green	Blinking Amber
Loading image	Blinking Green/Red	OFF
Image loaded	Green	Green
ZTP process running	Green	Blinking Amber
ZTP process success and config-file download completes	Green	Green
ZTP process failure or aborted	Green	Red

On Cisco ASR 920 Series Routers (ASR-920-20SZ-M, 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 ZTP Configuration

To verify if the ZTP configuration is successful, use the following command:

- **show running-config**

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, ASR-920-8S4Z-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, ASR-920-12SZ-A/Cisco ASR-920-12SZ-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, ASR-920-10SZ-PD, and ASR-920-8S4Z-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:
    a. the reachability
    b. 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.
    a. Unconfigure the current policy using the following command.

        no event manager policy Mandatory.dualrate_eem_policy.tcl type system

    b. 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 and Telnet 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 *Cisco 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 in any other Cisco platforms. For information on traditional Telnet, see the **line** command in the Cisco IOS Terminal Services Command Reference guide.

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. 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 even when the IOS XE process has failed.

Persistent Telnet

In traditional Cisco routers, accessing the router using Telnet 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 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 you use Telnet to access diagnostic mode, the Telnet 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.

Procedure

	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.
		• **wait**—Creates a banner message seen by users waiting for the IOS vty to become available.

	Command or Action	Purpose
		• *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.

Procedure

	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	**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.

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.

	Command or Action	Purpose
		• **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:

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
```

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

- Persistent SSH is not supported on Cisco ASR 920 IOS XE release.
- The Telnet settings made in the transport map overrides any other Telnet 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 sessions can disconnect the active sessions. Removing a transport map from an interface, however, does not disconnect any active Telnet sessions.
- Configuring the diagnostic and wait banners is optional but recommended. The banners are especially useful as indicators to users of the status of their Telnet or SSH attempts.

CHAPTER 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 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 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 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 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 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 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, ASR 920-10SZ-PD, or ASR-920-8S4Z-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

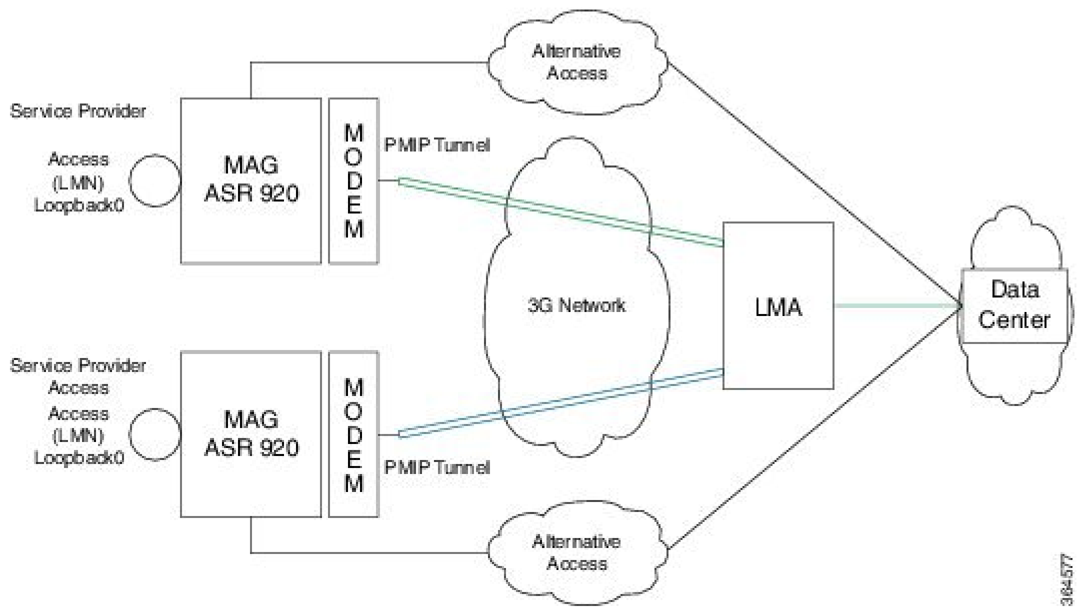
For Cisco IOS-XE Release 3.15.0S:

- 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

Procedure

	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.
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.

	Command or Action	Purpose
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. **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

Procedure

	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.
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.

	Command or Action	Purpose
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.

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

Router(config)# license feature upoe
```

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

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.

How to Configure the PoE

Procedure

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.

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.

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

Procedure

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

Procedure

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:

Procedure

	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:

Procedure

	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.

	Command or Action	Purpose
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.

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.

Procedure

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

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

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.

Procedure

	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.

	Command or Action	Purpose
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:

Procedure

	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:

Procedure

	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.

	Command or Action	Purpose
		• 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.
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	Description
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.
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.
- When FPGA upgrade is triggered during reload or SDM template change, the last reset reason in show version shows as power on.

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 images and packages:

- DRAM Memory—4 GB
- Software Image—asr920-universalk9_npe.bin—420 MB (ASR 920-24SZ-IM)
- Software Image—asr920-universalk9_npe.bin—430 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-920-8S4Z-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, ASR-920-8S4Z-PD, and ASR-920-12SZ-IM).

Note Always use bootflash instead of flash on all the system operations.

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 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.
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.

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 router: platform trace runtime slot 0 bay 0 process iomd module all-modules level info

The 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:

Procedure

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*. To purchase a license, contact Cisco.

Upgrading the ROMMON on router

The 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:

Procedure

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 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 not applicable to Cisco ASR-920-12SZ-IM Router for TDM IMs.

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.

- Verify that the correct IM is inserted in the IM slot.
- 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 94, for active interfaces to be shut down.
- Wait for a minute.
- Default all interfaces to be removed from the router.
- 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.

- Verify that the correct IM is in OK state in the router.
- 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.
- Shut down all pluggable IM interfaces in the router.
- Wait for a minute.
- Default all pluggable IM interfaces in the router.
- 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.

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; 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:

Procedure

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 111.

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.

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 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
```

Configuring Hot Standby Router Protocol

Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts without relying on the availability of any single router. You can deploy HSRP in a group of routers to select an active router and a standby router. (An *active* router is the router of choice for routing packets; a *standby* router is a router that takes over the routing duties when an active router fails, or when preset conditions are met).

HSRP is enabled on an interface by entering the **standby** [*group-number*] **ip** [*ip-address* [**secondary**]] command. The **standby** command is also used to configure various HSRP elements. This document does not discuss more complex HSRP configurations. For additional information on configuring HSRP, see to the HSRP section of the Cisco IP Configuration Guide publication that corresponds to your Cisco IOS XE software release. In the following HSRP configuration, standby group 2 on Gigabit Ethernet port 0/1/0 is configured at a priority of 110 and is also configured to have a preemptive delay should a switchover to this port occur:

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

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

The maximum number of HSRP or VRRP groups allowed are:

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

Note TCAM space utilization changes when HSRP groups are configured on the router. If HSRP groups are configured the TCAM space is utilized. Each HSRP group takes 1 TCAM entry. The “Out of TCAM” message may be displayed if total number of TCAM space used by HSRP groups and prefixes on the router exceeds scale limit.

Note HSRP state flaps with sub-second “Hello” or “Dead” timers.

Restrictions

HSRPv2 is not supported.

Verifying HSRP

To verify the HSRP information, use the show standby command in EXEC mode:

```
Router# show standby
Ethernet0 - Group 0
Local state is Active, priority 100, may preempt
Hellotime 3 holdtime 10
Next hello sent in 0:00:00
Hot standby IP address is 198.92.72.29 configured
Active router is local
```

```
Standby router is 198.92.72.21 expires in 0:00:07
Standby virtual mac address is 0000.0c07.ac00
Tracking interface states for 2 interfaces, 2 up:
UpSerial0
UpSerial1
```

Modifying the Interface MTU Size

Note The 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.

Note If the MTU interface configuration exceeds the maximum number of supported bytes, then the input errors are incremented. For packets with maximum size, the counter does not support increment by using CLI as the ASIC is unable to handle it. This is applicable on Cisco ASR 920-10SZ-PD (OD), ASR-920-8S4Z-PD, ASR-920-12SZ-IM, ASR-920U-12SZ-IM, ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M routers.

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 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.

Limitation

The **giants** and **input errors** field counts are not incremented for both 1G and 10G ports on Cisco ASR 920 platforms.

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* 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 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 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 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.
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 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 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 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.

Procedure

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:

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

Exits global-configuration (config) mode and enters privilege-exec mode.

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

Configuring Optical Interface Modules

This chapter describes the most common configurations for optical interface modules on the ASR 920 Series Routers.

Limitations and Restrictions

- SDH framing mode is supported; SONET framing is supported beginning in Cisco IOS XE Release 3.8.
- On the OC-3 controller, framing mode is applicable on the interface module and per port. When framing mode is set to SONET, all the 4 ports on the interface module are enabled for SONET mode. Similarly, when framing mode is set to SDH mode, all 4 ports on the interface module are enabled for SDH mode.
- The OC-3 controller supports Asynchronous mode at the V5 byte level for Plesiochronous Digital Hierarchy (PDH). This value cannot be modified. If a mismatch occurs between the V5 byte, and the peer (remote router), loss of frames may be observed at the PDH level.
- HDLC, PPP, and MLPPP encapsulation are supported. In POS mode, HDLC and PPP are supported.
- ATM Layer 2 AAL0 and AAL5 encapsulation types are supported.
- E1 unframed encapsulation is not supported except using SAToP pseudowire interfaces.

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

Managing Interface Naming

The following sections describe how to manage interface naming on the ASR 920 Series Routers.

Identifying Slots and Subslot

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

- slot—Specifies the chassis slot number where the interface module is installed; the slot number is always 0 for interface modules on the .ASR 920 Series Router.
- subslot—Specifies the subslot where the interface module is installed.
- port—Specifies the SONET port number.

For example, if the optical interface module is installed in slot 0 of the chassis, the controller configuration address is specified as **controller sonet 0/1/0**.

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

- channel-group—Specifies the logical channel group assigned to the time slots within the T1 link.

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.

To set the card type for the OC-3/OC-12 interface module, complete these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 **card type** {**OC3** | **OC12**} *slot bay*

Example:

```
Router(config)# card type OC12 0 1
```

Sets the mode for the interface module:

- OC3—Specifies one OC-3 /STM-1 port.
- OC12—Specifies one OC-12/STM-4 port.
- *slot bay* —Specifies the location of the interface module.

Step 3 **exit**

Example:

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

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

Configuring the Controller

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

Note When the mode is changed, the interface module reloads.

Command	Purpose
controller sonet *slot*/*subslot*/*port* `Router(config)# controller sonet 0/1/3`	Selects the controller to configure and enters controller configuration mode, where: • *slot*/*subslot*/*port* —Specifies the location of the interface.

Configuring SDH

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

Configuring SDH Mode

SDH T1 Mode

To configure SDH T1 mode, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**framing sdh** **Example:** `Router(config-controller)# framing sdh`	Specifies SDH as the frame type.
Step 2	**aug mapping** {**au-4**} **Example:** `Router(config-controller)# aug mapping au-4`	Configures AUG mapping for SDH framing.
Step 3	**clock source** {**internal** | **line**} **Example:** `Router(config-controller)# clock source line`	Sets the clock source, where: • 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.

	Command or Action	Purpose
Step 4	**au-4** *au-4#* **tug-3** *tug-3#* **Example:** `Router(config-controller)# au-4 1 tug-3 3`	Configures AU-4, and tributary unit groups, type 3 (TUG-3) for AU-4 and enters specific configuration mode. • *au-4#*—Range is from 1 to 4 for OC-12 mode and 1 for OC-3 mode • *tug-3#*—Range is from 1 to 3.
Step 5	In SDH framing in AU-4 mode: **Example:** **`mode {c-11 | c-12 | t3 | e3}`** **Example:** `Router(config-ctrlr-tug3)# mode {c-11 | c-12 | t3 | e3}`	(Optional) Configures mode of operation for AU-3 or AU-4 mode, where: C-11 and C-12 are container level-n (SDH) channelized T3s. They are types of T3 channels that are subdivided into 28 T1 channels. • **c-11**—Specifies an AU-3/AU-4 TUG-3 divided into seven TUG-2s. Each TUG-2 is then divided into four TU11s, each carrying a C-11 T1. • **c-12**—Specifies an AU-3/AU-4 TUG-3 divided into seven TUG-2. Each TUG-2 is then divided into three TU12s, each carrying a C-12 E1. • **t3**—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) T3. • **e3**—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) E3. **Note** Only c-11 and c-12 are currently supported.
Step 6	**SAToP CEM Group** **Example:** **`tug-2 1 e1 1 cem-group 1 unframed`** **Example:** `Router(config-ctrlr-tug3)# tug-2 1 e1 1 cem-group 1 unframed` **Example:** **CESoPSN CEM Group** **`tug-2 1 e1 1 cem-group 1 timeslots 1-31`** **Example:**	Creates a CEM group, IMA group, or channel-group for the AU-3 or AU-4. Valid values are: • e1— 1–3 • **tug-3—1-3** • **tug-2**—1–7 • **unframed**—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.

	Command or Action	Purpose

	`Router(config-ctrlr-tug3)# tug-2 1 e1 1 cem-group 1 timeslots 1-31`
	Example:
	IMA Group
	tug-2 1 e1 1 ima-group 1
	Example:
	`Router(config-ctrlr-tug3)# tug-2 1 e1 1 ima-group 1`
	Example:
	Channel Group
	tug-2 1 e1 1 [[channel-group *channel-group-number]* [**timeslots** *list-of-timeslots]]*
	Example:
	`Router(config-ctrlr-tug3)#` **tug-2** *1* **e1** *1* **channel-group** 1 **timeslots** *1-31]*	

Step 7	exit **Example:** `Router(config-controller)#` **exit**	Exits controller configuration mode.
Step 8	**controller t1** *interface-path-id* **Example:** `Router(config-controller)#` **controller t1 0/1/1/0/0/0**	Enters controller configuration mode for an individual T1 or E1.
Step 9	Creates a CEM group, IMA group, or channel-group on the T1 or E1 controller.	**SAToP CEM Group** `Router(config-ctrlr)#` **t1 cem-group** 1 **unframed** **CESoPSN CEM Group** `Router(config-ctrlr)#` **t1 cem-group** 1 **timeslots 1-24** **Clear-Channel ATM** `Router(config-ctrlr-tug3)#` **e1** *1* **atm** **IMA Group**

	Command or Action	Purpose

		`Router(config-ctrlr-tug3)# e1 1 ima-group 1`
		Channel Group
		`Router(config-ctrlr)# t1 2 channel-group 4 [[channel-group channel-group-number] [timeslots list-of-timeslots]]`

What to do next

Example

The example configures SDH E1 mode:

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-4
Router(config-controller)# clock source internal
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 1 e1 1 channel-group 1 timeslots 1-31
```

SDH T1 Mode

To configure SDH T1 mode, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**framing sdh** **Example:** `Router(config-controller)# framing sdh`	Specifies SDH as the frame type.
Step 2	**aug mapping** {**au-3**} **Example:** `Router(config-controller)# aug mapping au-3`	Configures AUG mapping for SDH framing. Supports au-3 and au-4 aug mapping. The default setting is **au-3.**
Step 3	**clock source** {**internal** | **line**} **Example:** `Router(config-controller)# clock source line`	Sets the clock source, where: • internal—Specifies that the internal clock source is used. • l

	Command or Action	Purpose
		ine—Specifies that the network clock source is used. This is the default for T1 and E1.
Step 4	**au-3** *au-3#* **Example:** `Router(config-controller)#` **`au-3`** *`au-3#`*	Configures AU-3, and enters specific configuration mode. • *au-3#* —Range is from 1 to 12 for OC-12 mode. For OC-3 mode, the value is 1–3.
Step 5	In SDH framing in AU-3 mode: **Example:** **`mode {c-11 | c-12 | t3 | e3}`** **Example:** `Router(config-ctrlr-au3)#` **`mode`** `{`**`c-11 | c-12 | t3 | e3}`**	(Optional) Configures mode of operation for AU-3 or AU-4 mode, where: C-11 and C-12 are container level-n (SDH) channelized T3s. They are types of T3 channels that are subdivided into 28 T1 channels. • **c-11**—Specifies an AU-3/AU-4 TUG-3 divided into seven TUG-2s. Each TUG-2 is then divided into four TU11s, each carrying a C-11 T1. • **c-12**—Specifies an AU-3/AU-4 TUG-3 divided into seven TUG-2. Each TUG-2 is then divided into three TU12s, each carrying a C-12 E1. • **t3**—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) T3. • **e3**—Specifies an AU-3/AU-4 TUG-3 carrying an unchannelized (clear channel) E3. **Note** Only c-11 and c-12 are currently supported.
Step 6	**SAToP CEM Group** **Example:** **`tug-2`** `1` **`t1`** `1` **`cem-group`** `1` **`unframed`** **Example:** `Router(config-ctrlr-au3)#` **`tug-2`** *`1`* **`t1`** `1` **`cem-group`** `1` **`unframed`** **Example:** **CESoPSN CEM Group** **Example:**	Creates a CEM group, IMA group, or channel-group for the AU-3 or AU-4. Valid values are: • **t1**—Range is from 1 to 12 for OC-12 mode. For OC-3 mode, the value is 1–3. • **tug-2**—1–7 • **unframed**—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.

	Command or Action	Purpose

	tug-2 1 e1 1 cem-group 1 timeslots 1-31
	Example:
	`Router(config-ctrlr-au3)# tug-2 1 t1 1 cem-group 1 timeslots 1-31`
	Example:
	IMA Group
	tug-2 1 t1 1 ima-group 1
	Example:
	`Router(config-ctrlr-au3)# tug-2 1 t1 1 ima-group 1`
	Example:
	Channel Group
	tug-2 1 e1 1 [[**channel-group** *channel-group-number*] [**timeslots** *list-of-timeslots*]]
	Example:
	`Router(config-ctrlr-tug3)# tug-2 1 t1 1 channel-group 0 timeslots 1-31`	

Step 7	exit **Example:** `Router(config-controller)# exit`	Exits controller configuration mode.
Step 8	**controller t1** *interface-path-id* **Example:** `Router(config-controller)# controller t1 0/1/1/0/0/0`	Enters controller configuration mode for an individual T1 or E1.

Step 9	Creates a CEM group, IMA group, or channel-group on the T1 or E1 controller.	**SAToP CEM Group**
		`Router(config-ctrlr)# t1 cem-group 1 unframed`
		CESoPSN CEM Group
		`Router(config-ctrlr)# t1 cem-group 1 timeslots 1-24`

	Command or Action	Purpose

		Clear-Channel ATM
		`Router(config-ctrlr-tug3)# e1 1 atm`
		IMA Group
		`Router(config-ctrlr-tug3)# e1 1 ima-group 1`
		Channel Group
		`Router(config-ctrlr)# t1 2 channel-group 4 [[channel-group channel-group-number] [timeslots list-of-timeslots]]`

What to do next

The example configures SDH T1 mode:

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 1 t1 1 channel-group 1 timeslots 1-31
```

For information about configuring optional features, see Optional Configurations, on page 146.

Configuring SDH in POS Mode

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

Procedure

	Command or Action	Purpose
Step 1	**controller sonet** *slot/subslot/port* **Example:** **Example:** `Router(config)# controller sonet 0/1/0`	Selects the controller to be configured.
Step 2	**framing {sonet | sdh}** **Example:** `Router(config)# framing sdh`	Specifies SDH as the framing mode. **Note** The interface module reloads if the framing is changed.

	Command or Action	Purpose
Step 3	**aug mapping** {**au-3** | **au-4**} **Example:** `Router(config-controller)# aug mapping au-4`	Specifies AUG mapping. **Note** POS mode is only supported with AU-4 mode.
Step 4	**au-4** *au-4-number* **pos** **Example:** `Router(config-controller)# au-4 1 pos`	Selects the AU-4 to be configured in POS mode with SDH framing. The command creates a POS interface, such as POS0/1/0:1. In OC-3 mode, the value is 1; in OC-12 mode, valid values are 1-4.
Step 5	**end** **Example:** `Router(config-controller)# end`	Exits configuration mode.

Configuring SONET Mode

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

Configuring SONET Mode

To configure an interface module to use SONET mode:

Procedure

	Command or Action	Purpose
Step 1	**controller sonet** *slot*/*subslot*/*port* **Example:** `Router(config)# controller sonet 0/1/0`	Selects the controller to be configured.
Step 2	**framing {sonet | sdh}** **Example:** `Router(config-controller)# framing sonet`	Specifies SONET as the framing mode.
Step 3	**clock source** {**line** | **internal**} **Example:** `Router(config-if)# clock source line`	Specifies the clock source for the POS link, where: • **line**—The link uses the recovered clock from the line. This is the default setting.

	Command or Action	Purpose
		• **internal**—The link uses the internal clock source.
Step 4	**sts-1 {1 - 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12}** **Example:** `Router(config-controller)# sts-1 1 - 3`	Specifies the SONET Synchronous Transport Signal (STS) level and enters STS-1 configuration mode. The starting-number and ending-number arguments indicate the starting and ending STS value of the interface. For OC-3 interfaces, this value is 1. **Note** The **1-12** value is supported only in OC-12 mode.
Step 5	**vtg** *vtg-number* **t1** *t1-line-number* **channel-group** *channel-group-no* **timeslots** *list-of-timeslots* **Example:** `Router(config-if)# vtg 1 t1 1 channel-group 0 timesolts 1-24`	Configures the T1 on the VTG, where • *vtg-number*—Specifies the VTG number. The framing is1-7 • **t1** *t1-line-number*—1-4 • **channel-group** *channel-group-no*—0-24 • **timeslots** *list-of-timeslots*—1-24
Step 6	**end** **Example:** `Router(config-if)# end`	Exits configuration mode.

What to do next

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

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sonet
Router(config-controller)# clock source line
Router(config-controller)# sts-1 1 - 3
Router(config-ctrlr-sts1)# vtg 1 t1 1 channel-group 0 timeslot 1-24
Router(config-controller)# end
```

For information on optional SONET configurations, see Optional Configurations, on page 146. For information on optional ATM, IMA, POS and Serial interface configuration, see Optional Configurations, on page 146.

Configuring SONET Mode

Example

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

```
Router(config-controller)# au-4 1 pos
Router(config-controller)# end
```

For information about configuring optional features, see Optional Packet over SONET Configurations, on page 148

Configuring SONET POS Mode

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

Procedure

	Command or Action	Purpose
Step 1	**controller sonet** *slot/subslot/port* **Example:** `Router(config)# controller sonet 0/1/0`	Selects the controller to be configured.
Step 2	**framing {sonet | sdh}** **Example:** `Router(config-controller)# framing sonet`	Specifies SONET as the framing mode.
Step 3	**clock source** {**line** | **internal**} **Example:** `Router(config-controller)# clock source line`	Specifies the clock source for the POS link, where: • **line**—The link uses the recovered clock from the line. This is the default setting. • **internal**—The link uses the internal clock source.
Step 4	**sts-1 {1- 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12} pos** **Example:** `Router(config-controller)# sts-1 1 - 3 pos`	Specifies POS mode; starting-number and ending-number arguments indicate the starting and ending STS value of the POS interface. For OC-3 interfaces, this value is 1. **Note** The **1-12** value is supported only in OC-12 mode.
Step 5	**exit** **Example:** `Router(config-controller# exit`	Exits controller configuration mode.
Step 6	Do one of the following: • **interface POS** *slot/subslot/port* •	Use any of the following commands to access the POS interface.

	Command or Action	Purpose

	• **interface POS** *slot/subslot/port.POS-interface*
	•
	• **interface POS** *slot/subslot/port:POS-interface*
	Example:
	`interface 0/1/1`
	Example:
	`interface 0/1/1.1`
	Example:
	`interface 0/1/1:1`	

Step 7	**encapsulation** *encapsulation-type* {**hdlc** | **ppp**} **Example:** `Router(config-if)# encapsulation hdlc`	Configures encapsulation; you can configure the following options: • **hdlc**—Serial HDLC. This is the default for synchronous serial interfaces. • **ppp**—Point-to-Point Protocol (for serial interface).
Step 8	**end** **Example:** `Router(config-if)# end`	Exits configuration mode.

What to do next

Example

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sonet
Router(config-controller)# clock source line
Router(config-controller)# sts-1 1 - 3 pos
Router(config-controller)# exit
Router(config)# interface 0/1/1
Router(config-if)# encapsulation hdlc
Router(config-if)# end
```

For information on optional SONET configurations, see Configuring SONET POS Mode, on page 137.

Configuring a CEM group

Configuring CEM Group in SONET Mode

To configure a T1 CEM group in SONET mode:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**controller sonet** *slot/bay/port* **Example:** `Router(config)# controller sonet 0/1/1`	Selects the controller to configure and enters controller configuration mode, where: • *slot/bay/port*—Specifies the location of the interface. **Note** The slot number is always 1 and the bay number is always 0.
Step 4	**framing {sonet | sdh}** **Example:** `Router(config)# framing sonet`	Specifies SONET as the framing mode.
Step 5	**sts-1 {1 - 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12}** **Example:** `Router(config-controller)# sts-1 1 - 3`	Specifies the SONET Synchronous Transport Signal (STS) level and enters STS-1 configuration mode. The starting-number and ending-number arguments indicate the starting and ending STS value of the interface. For OC-3 interfaces, this value is 1. **Note** The **1-12** value is supported only in OC-12 mode.
Step 6	**mode {t3 | vt-15}** **Example:** `Router(config-ctrlr-sts1-3)# mode t3`	Specifies the mode of operation of an STS-1 path, where: **Note** Note VT-15 is the only supported mode. • **t3**—DS3 clear channel mode. STS-1carries an unchannelized (clear channel) T3. • **vt-15**—A STS-1 is divided into seven Virtual Tributary Groups (VTG). Each

	Command or Action	Purpose
		VTG is then divided into four VT1.5's, each carrying a T1.

Step 7	**SATOP CEM**
	Example:
	`cem-group` *`channel-number`* `unframed`
	Example:
	`Router(config-ctrlr-sts1-3)# cem-group 0 unframed`
	Example:
	CeSOP CEM
	`vtg` *`vtg_number`* **`t1`** *`t1_line_number`* **`cem-group`** *`channel-number`* **`timeslots`** *`list-of-timesolts`*
	Example:
	`Router(config-ctrlr-sts1-3)# vtg 1 t1 1 cem-group 1 timeslots 1-10`
		Configures the T1 on the VTG, where:
		• *vtg_number*—Specifies the VTG number. For SONET framing, values are 1 to 7.
		• *t1_line_number*—Specifies the T1 line number. Valid range is 1 to 4.
		• *channel-number*—Specifies the channel number. Valid range is 0 to 2015.
		• *list-of-timeslots*—Specifies the list of timeslots. Valid range is from 1 to 24.

Step 8	**end**	Exits controller configuration mode and returns to privileged EXEC mode.

What to do next

Example

The example shows a CEM interface configuration:

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sonet
Router(config-controller)# sts-1 1
Router(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 1 timeslots 1-10
Router(config-ctrlr-sts1)# exit
```

Configuring CEM Group in SDH Mode

To configure CEM group in SDH mode:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**controller sonet** *slot/bay/port* **Example:** `Router(config)# controller sonet 0/1/0`	Selects the controller to configure and enters controller configuration mode, where: • *slot/bay/port*—Specifies the location of the interface. **Note** The slot number is always 1 and the bay number is always 0.
Step 4	**framing {sonet | sdh}** **Example:** `Router(config-controller)# framing sdh`	Specifies SDH as the framing mode.
Step 5	**au-4** *au-4#* **tug-3** *tug-3#* **Example:** `Router(config-controller)# au-4 1 tug-3 1`	Configures AU-4, and tributary unit groups, type 3 (TUG-3) for AU-4 and enters specific configuration mode. In SDH framing mode, each TUG-3, and AU-4 can be configured with one of these commands. Depending on currently configured AUG mapping setting, this command further specifies TUG-3, or AU-4 muxing. The CLI command parser enters into config-ctrlr-tug3 (SDH mode) or config-ctrlr-au3 (SDH mode), which makes only relevant commands visible. • au-4#—Range is from 1 to 4. For OC-3 mode, the value is 1. **Note** DS3 configuration is supported only on AuU-4. • tug-3#—Range is from 1 to 3. **Note** T1 can only be configured in au-3 mode, E1 can only be configured in the au-4 mode.
Step 6	**mode {t3 | e3}** **Example:** `Router(config-ctrlr-tug3)# mode e3`	Specifies the mode of operation. • **t3**—Specifies an unchannelized (clear channel) T3. • **e3**—Specifies a AU-3 or C3 that carries a unchannelized (DS3 clear channel) E3. **Note** Only e3 mode is supported for SDH framing.
Step 7	**cem-group group-number** {**unframed**} **Example:**	Creates a CEM group.

	Command or Action	Purpose
	`Router(config-ctrlr-tug3)# cem-group 4 unframed`	• **unframed**—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.
Step 8	**end** **Example:** `Router(config-ctrlr-tug3)# end`	Exits controller configuration mode and returns to privileged EXEC mode.

What to do next

Example

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

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

Note DS3 clear channel is supported only on CEM.

Configuring DS3 Clear Channel in SONET Mode

To configure DS3 clear channel in SONET mode:

Procedure

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

	Command or Action	Purpose
Step 3	**controller sonet** *slot/bay/port* **Example:** `Router(config)# controller sonet 0/1/1`	Selects the controller to configure and enters controller configuration mode, where: • *slot/bay/port*—Specifies the location of the interface. **Note** The slot number is always 1 and the bay number is always 0.
Step 4	**framing {sonet | sdh}** **Example:** `Router(config)# framing sonet`	Specifies SONET as the framing mode.
Step 5	**clock source** {**line** | **internal**} **Example:** `Router(config-if)# clock source internal`	Specifies the clock source for the POS link, where: • **line**—The link uses the recovered clock from the line. This is the default setting. • **internal**—The link uses the internal clock source.
Step 6	**sts-1 {1 - 12 | 1 - 3 | 4 - 6 | 7 - 9 | 10 - 12}** **Example:** `Router(config-controller)# sts-1 1`	Specifies the SONET Synchronous Transport Signal (STS) level and enters STS-1 configuration mode. The starting-number and ending-number arguments indicate the starting and ending STS value of the interface. For OC-3 interfaces, this value is 1. The 1-12 value is supported only in OC-12 mode.
Step 7	**mode {t3 | vt-15}** **Example:** `Router(config-ctrlr-sts1)# mode t3`	Specifies the mode of operation of an STS-1 path, where: • **t3**—DS3 clear channel mode. STS-1 carries an unchannelized (clear channel) T3. • **vt-15**—A STS-1 is divided into seven Virtual Tributary Groups (VTG). Each VTG is then divided into four VT1.5's, each carrying a T1.
Step 8	cem-group *channel-number* {unframed} **Example:** `Router(config-ctrlr-sts1)# cem-group 4 unframed`	Creates a CEM group. • **unframed**—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.

	Command or Action	Purpose
Step 9	**end**	Exits controller configuration mode and returns to privileged EXEC mode.

What to do next

Example

The below example shows the configuration for a DS3 interface:

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

Configuration Example

```
controller SONET 0/1/0
framing sonet
clock source internal
!
sts-1 1
mode t3
cem-group 0 unframed
!
sts-1 2
mode t3
cem-group 1 unframed
!
sts-1 3
mode t3
cem-group 2 unframed
interface CEM0/1/0
no ip address
cem 0
xconnect 2.2.2.2 501 encapsulation mpls
!
cem 1
xconnect 2.2.2.2 502 encapsulation mpls
!
cem 2
xconnect 2.2.2.2 503 encapsulation mpls
!
```

Configuring DS3 Clear Channel in SDH Mode

To configure DS3 clear channel in SDH mode:

Procedure

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

	Command or Action	Purpose
		• Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**controller sonet** *slot/bay/port* **Example:** `Router(config)# controller sdh 0/1/0`	Selects the controller to configure and enters controller configuration mode, where: • *slot/bay/port*—Specifies the location of the interface. **Note** The slot number is always 1 and the bay number is always 0.
Step 4	**framing {sonet | sdh}** **Example:** `Router(config-controller)# framing sdh`	Specifies SDH as the framing mode.
Step 5	**clock source** {**line** | **internal**} **Example:** `Router(config-controller)# clock source line`	Specifies the clock source for the POS link, where: • **line**—The link uses the recovered clock from the line. This is the default setting. • **internal**—The link uses the internal clock source.
Step 6	**aug mapping au-4** **Example:** `Router(config-controller)# aug mapping au-4`	Configures AUG mapping for SDH framing. If the AUG mapping is configured to be AU-4, then the following muxing, alignment, and mapping will be used: TUG-3 <--> VC-4 <--> AU-4 <--> AUG.
Step 7	**au-4** *au-4#* **tug-3** *tug-3#* **Example:** `Router(config-controller)# au-4 1 tug-3 1`	Configures AU-4, and tributary unit groups, type 3 (TUG-3) for AU-4 and enters specific configuration mode. In SDH framing mode TUG-3, and AU-4 can be configured with one of these commands. Depending on currently configured AUG mapping setting, this command further specifies TUG-3, or AU-4 muxing. The CLI command parser enters into config-ctrlr-tug3 (SDH mode) or config-ctrlr-au3 (SDH mode), which makes only relevant commands visible. • au-4#—Range is from 1 to 4. For OC-3 mode, the value is 1. • tug-3#—Range is from 1 to 3. **Note** E1 can only be configured in the AU-4 mode.

	Command or Action	Purpose
Step 8	**mode e3** **Example:** `Router(config-ctrlr-au4)# mode e3`	Specifies the mode of operation. • **e3**—Specifies a C3 that carries a unchannelized (DS3 clear channel) E3.
Step 9	**cem-group** *channel-number* {**unframed**} **Example:** `Router(config-ctrlr-au4)# cem-group 4 unframed`	Creates a CEM group. • **unframed**—Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.
Step 10	**end**	Exits controller configuration mode and returns to privileged EXEC mode.

What to do next

Example

```
Router# configure terminal
Router(config)# controller sonet 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# clock source line
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 1
Router(config-ctrlr-au4)# mode e3
Router(config-ctrlr-au4)# cem-group 4 unframed
Router(config-ctrlr-au4)# end
```

Optional Configurations

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

Configuring the National Bit

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

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

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

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

Command	Purpose
Router(config)# **controller {t1 | e1}** *slot/subslot/port*	Selects the controller to configure. • t1—Specifies the T1 controller. • e1—Specifies the E1 controller. • slot/subslot/port—Specifies the location of the controller.
Router(config-controller)# *national reserve {0 | 1} {0 | 1} {0 | 1} {0 | 1} {0 | 1} {0 | 1}*	Sets the national bit (the first bit): • 0—Sets the international bit in the G.704 frame to 0. This is the default. • 1—Sets the international bit in the G.704 frame to 1. **Note** When CRC4 framing is configured, the first bit is the national bit. When no-CRC4 framing is configured, the first bit becomes the international bit and should be set to 1 if crossing international borders and 0 if not crossing international borders. Sets the five national bits: • 0—Set to 0 when not crossing international borders. • 1—Set to 1 when crossing international bordrs.

Verifying the National Bit

Use the show controllers command to verify the national bits:

```
router# show controllers E1
E1 0/1/0 is up.
Applique type is Channelized E1 - balanced
No alarms detected.
alarm-trigger is not set
Framing is CRC4, Line Code is HDB3, Clock Source is Line.
International Bit: 1, National Bits: 11111
Data in current interval (234 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 5 15 minute intervals):
0 Line Code Violations, 0 Path Code Violations,
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Configuring the CRC Size for T1

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The 1-Port Channelized OC-3/STM-1 SPA and 1-Port Channelized OC-12/STM-4 SPA uses a 16-bit cyclic redundancy check (CRC) by default, but also supports a 32-bit CRC. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

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

Procedure

	Command or Action	Purpose
Step 1	**interface serial** *slot*/*subslot*/*port*:*channel-group* **Example:** `Router(config)# interface serial 0/1/1.1/1/1/1:0`	Selects the interface to configure and enters interface configuration mode. • *slot*/*subslot*/*port*:*channel-group* —Specifies the location of the interface.
Step 2	**crc {16 | 32}** **Example:** `Router(config-if)# crc 16`	Selects the CRC size in bits, where: • 16—16-bit CRC. This is the default. • 32—32-bit CRC.

Optional Packet over SONET Configurations

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

Encapsulation

encapsulation *encapsulation-type* `Router(config-if)# encapsulation hdlc`	Configures encapsulation; you can configure the following options: • HDLC • PPP

MTU Value

mtu bytes `Router(config-if)# mtu 4000`	Configures the maximum packet size for an interface in bytes. The default packet size is 4470 bytes.

CRC Value

crc *size-in-bits* `Router(config-if)# crc 32`	CRC size in bits. Valid values are 16 and 32. The default is 16.

Keepalive Value

keepalive [*period* [*retries*]] `Router(config-if)#` **`keepalive 9 4`**	Specifies the frequency at which the Cisco IOS software sends messages to the other end of the line to ensure that a network interface is alive, where: • *period*—Specifies the time interval in seconds for sending keepalive packets. The default is 10 seconds. • *retries*—Specifies the number of times that the device continues to send keepalive packets without response before bringing the interface down. The default is 3 retries.

Bandwidth

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

bandwidth {*kbps* | **inherit** [*kbps*]}	To set and communicate the current bandwidth value for an interface to higher-level protocols, use the **bandwidth** command in interface configuration mode.Valid values are from 1 to 10000000. You can apply the following keywords: • **inherit** —Specifies how a subinterface inherits the bandwidth of its main interface. • **receive**—Specifies the receive-side bandwidth.

Scrambling

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

pos scramble-atm	Enables scrambling on the interface.

C2 Flag

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

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

J1 Flag

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

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

You can use the following commands to verify your configuration:

- **show interfaces pos**

Configuring Multilink Point-to-Point Protocol

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

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

MLPPP Configuration Guidelines

When configuring MLPPP, consider the following guidelines:

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

Creating a Multilink Bundle

To create a multilink bundle, use the following commands:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink 1`	Creates a multilink interface and enters multilink interface mode, where: • group-number—The group number for the multilink bundle.
Step 3	**ip address** *address mask* **Example:**	Sets the IP address for the multilink group, where: • address—The IP address.

	Command or Action	Purpose
	`Router(config-if)# ip address 192.168.1.1 255.255.255.0`	• mask—The subnet mask.

Assigning an Interface to a Multilink Bundle

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface serial** *slot/subslot/port* **Example:** `Router(config)# interface serial 0/1/1.1/1/1/1:0`	Selects the interface to configure and enters interface configuration mode, where: • *slot/subslot/port* —Specifies the location of the controller.
Step 3	*encapsulation ppp* **Example:** `Router(config-if)# encapsulation ppp`	Enables PPP encapsulation.
Step 4	**ppp multilink** *group group-number* **Example:** `Router(config-if)# ppp multilink group 1`	Assigns the interface to a multilink bundle, where: • group-number—The multilink group number for the T1 or E1 bundle.
Step 5	**end**	

What to do next

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

```
Router# configure terminal
Router(config)# controller SONET 0/1/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 1
Router(config-controller)# tug-2 1 e1 1 channel-group 0 timeslots 1-31
```

```
Router# configure terminal
Router(config)# interface multilink 1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ppp multilink endpoint string string1
Router(config)# interface serial 0/1/1.1/1/1/1:0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink group 1
```

Configuring Fragmentation Size and Delay on an MLPPP Bundle

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink 1`	Creates a multilink interface and enters multilink interface mode, where: • *group-number* —The group number for the multilink bundle. Range 1-2147483647
Step 3	**ppp multilink fragment size** *fragment-size* **Example:** `Router(config-if)# ppp multilink fragment size 512`	Sets the fragmentation size in bytes. Fragmentation is disabled by default. Valid values are 42 to 65535 bytes.
Step 4	**ppp multilink fragment-delay** *delay* **Example:** `Router(config-if)# ppp multilink fragment-delay 20`	Sets the configured delay on the multilink bundle that satisfies the fragmentation size, where: • *delay* —Delay in milliseconds.

What to do next

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

```
Router#
show ppp multilink
Multilink1, bundle name is test2
Bundle up for 00:00:13
Bundle is Distributed
0 lost fragments,
0 reordered, 0 unassigned
0 discarded, 0 lost received, 206/255 load
```

```
0x0 received sequence,
0x0 sent sequence Member
links: 2 active, 0 inactive (max not set, min not set)
Se0/1/0/1:0, since 00:00:13, no frags rcvd
Se0/1/0/2:0, since 00:00:10, no frags rcvd
Distributed fragmentation on.
Fragment size 512.  Multilink in Hardware.
```

Changing the Default Endpoint Discriminator

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

Command	Purpose
`Router(config-if)# ppp multilink endpoint {hostname | ip IP-address | mac LAN-interface | none | phone telephone-number | string char-string }`	Overrides or changes the default endpoint discriminator the system uses when negotiating the use of MLP with the peer.

Disabling Fragmentation on an MLPPP Bundle

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface multilink** *group-number* **Example:** `Router(config)# interface multilink 1`	*Specifies the multilink interface and enters multilink interface mode, where:* • *group-number—The group number for the multilink bundle. Range 1-2147483647*
Step 3	**ppp multilink fragment disable** **Example:** `Router(config-if)# ppp multilink fragment disable`	Disables PPP multilink fragmentation.

Configuring BERT

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

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

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

Configuring Automatic Protection Switching

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

Verifying Interface Configuration

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

Verifying Per-Port Interface Status

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

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

Troubleshooting

You can use the following commands to verify your configuration:

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

- **show running configuration**—Shows detail on each CEM group.
- **show xconnect all**—Displays the state of the pseudowire and local and peer access circuits.
- **show interfaces pos—Displays all the current interface processors and their interfaces.**

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

- SLOS
- SLOF
- B1-TCA
- B2-TCA

When SLOS is reported, all the other alarms are masked.

```
Router(config-controller)# show controller sonet 0/1/2
SONET 0/1/2 is down.
  Hardware is A900-IMA4OS

Applique type is Channelized Sonet/SDH
Clock Source is Line, AUG mapping is AU4.
.
.
.
Multiplex Section:
  AIS = 6          RDI = 0          REI = 0          BIP(B2) = 0
Active Defects: None
Detected Alarms: SLOS SLOF LAIS B1-TCA B2-TCA ......<shows all alarms reported>
Asserted/Active Alarms: SLOS B1-TCA B2-TCA..........<shows hierarchy>
Alarm reporting enabled for: SLOS SLOF SF B1-TCA B2-TCA
BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6
```

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

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

Command or Action	Purpose
`Router#` **`show aps`**	Displays information about the automatic protection switching feature.
`Router#` **`show controller sonet`** *`slot/ port-adapter/ port`*	Displays information about the hardware.
`Router#` **`show interfaces`**	Displays information about the interface.

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

Framing and Encapsulation Configuration Example

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

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

National Bit Configuration Example

The following example sets the Natijonal Bits for the controller:

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

CRC Configuration Example

The following example sets the CRC size for the interface:

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

Facility Data Link Configuration Example

The following example configures Facility Data Link:

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

MLPPP Configuration Example

The following example creates a PPP Multilink bundle:

```
! Enter global configuration mode
!
Router# configure terminal
!
! Create a multilink bundle and assign a group number to the bundle
!
Router(config)# interface multilink 1
!
! Specify an IP address for the multilink group
!
Router(config-if)# ip address 123.456.789.111 255.255.255.0
!
! Enable Multilink PPP
!
Router(config-if)# ppp multilink
```

```
!
! Leave interface multilink configuration mode
!
Router(config-if)# exit
!
! Specify the interface to assign to the multilink bundle
!
Router(config)# interface serial 0/1/0:1
!
! Enable PPP encapsulation on the interface
!
Router(config-if)# encapsulation PPP
!
! Assign the interface to a multilink bundle
!
Router(config-if)# multilink-group 1
!
! Enable Multilink PPP
!
Router(config-if)# ppp multilink
!
! Exit interface configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
Router#
```

MFR Configuration Example

The following example configures Multilink Frame Relay (MFR):

```
! Create a MFR interface and enter interface configuration mode
!
Router(config)# interface mfr 49
!
! Assign the bundle identification (BID) name 'test' to a multilink bundle.
!
Router(config-if)# frame-relay multilink bid test
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Specify the serial interface to assign to a multilink bundle
!
Router(config)# interface serial 0/1/3:0
!
! Creates a multilink Frame Relay bundle link and associates the link with a multilink
bundle
!
Router(config-if)#
encapsulation frame-relay mfr 49
!
! Assigns a bundle link identification (LID) name with a multilink bundle link
!
Router(config-if)#
frame-relay multilink lid test
!
! Configures the interval at which the interface will send out hello messages
```

```
!
Router(config-if)# frame-relay multilink hello 15
!
! Configures the number of seconds the interface will wait for a hello message acknowledgement
 before resending the hello message
!
Router(config-if)# frame-relay multilink ack 6
!
! Configures the maximum number of times the interface will resend a hello message while
waiting for an acknowledgement
!
Router(config-if)# frame-relay multilink retry 5
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
```

Router(config)# exit

Configuration Examples

This section includes the following configuration examples:

Example of Cyclic Redundancy Check Configuration

The following example configures CRC on a T1 interface:

```
! Specify the interface to configure and enter interface configuration mode.
!
Router(config)# interface serial 0/1/0.1
!
! Specify the CRC type.
!
Router(config-if)# crc 32
```

Example of Facility Data Link Configuration

The following example configures FDL on a T1 interface:

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

Example of Invert Data on T1/E1 Interface

The following example inverts the data on the serial interface:

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

Additional Resources

For more information about configuring ATM, see

- Asynchronous Transfer Mode Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 920 Series)

For additional information on configuring optical interfaces, see

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

CHAPTER 14

Clocking and Timing

This chapter explains how to configure timing ports on the Cisco ASR 920 Series Router.

Clocking and Timing Restrictions

The following clocking and timing restrictions apply to the Cisco ASR 920 Series Router:

- Do not configure GNSS in high accuracy operating mode, when Cisco ASR-920-12SZ-A or Cisco ASR-920-12SZ-D router is configured as Precision Time Protocol (PTP) server.
- You can configure only a single clocking input source within each group of eight ports (0–7 and 8–15) on the T1/E1 interface module using the **network-clock input-source** command.
- Multicast timing is not supported.
- Precision Time Protocol (PTP) is supported only on loopback interfaces, layer 2 interfaces, and BDI interfaces. It is not supported on Layer 3 interfaces.
- Out-of-band clocking and the **recovered-clock** command are not supported.
- Synchronous Ethernet clock sources are not supported with PTP. Conversely, PTP clock sources are not supported with synchronous Ethernet except when configured as hybrid clock. However, you can use hybrid clocking to allow the router to obtain frequency using Synchronous Ethernet, and phase using PTP.
- Time of Day (ToD) and 1 Pulse per Second (1PPS) input is not supported when the router is in boundary clock mode.
- On Cisco ASR 920 Series Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, and ASR-920-4SZ-D), 1 PPS is only available through ToD port. To provide both ToD and 1 PPS signal on the same port you must use a special Y-cable.

Note The Cisco ASR-920-24SZ-M and ASR-920-24TZ-M do not have a ToD port, BITS port or a 1pps SMB port.

- Cisco ASR 920 Series Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-24SZ-M, ASR-920-24TZ-M), supports only BITS port and not 10 M input.

Note Fixed Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M Aggregation Services Routers cannot take any external input and cannot give out any external output.

- Multiple ToD clock sources are not supported.
- PTP redundancy is supported only on unicast negotiation mode; you can configure up to three server clocks in redundancy mode.
- In order to configure time of day input, you must configure both an input 10 Mhz and an input 1 PPS source.
- PTP over IPv6 is not supported.
- When PTP is configured on Cisco ASR-920-24SZ-IM Router, changing the configuration mode from LAN to WAN or WAN to LAN is not supported for following IMs:
  - 2x10G
  - 8x1G_1x10G_SFP
  - 8x1G_1x10G_CU
- PTP functionality is restricted by license type.

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

Table 12: PTP Functions Supported by Different Licenses

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

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

- End-to-end Transparent Clock is not supported for PTP over Ethernet.
- G.8265.1 telecom profiles are not supported with PTP over Ethernet.
- The Cisco ASR 920 Series Router do not support a mix of IPv4 and Ethernet clock ports when acting as a transparent clock or boundary clock.

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

- To use the **network-clock synchronization ssm option** command, ensure that the router configuration does not include the following:
  - Input clock source
  - Network clock quality level
  - Network clock source quality source (synchronous Ethernet interfaces)
- The **network-clock synchronization ssm option** command must be compatible with the **network-clock eec** command in the configuration.
- To use the **network-clock synchronization ssm option** command, ensure that there is not a network clocking configuration applied to synchronous Ethernet interfaces, BITS interfaces, and timing port interfaces.
- We recommended that you do not configure multiple input sources with the same priority as this impacts the TSM (Switching message delay).
- You can configure a maximum of 4 clock sources on interface modules, with a maximum of 2 per interface module. This limitation applies to both synchronous Ethernet and TDM interfaces.
- The **network-clock input-interface ptp domain** command is not supported.
- To shift from non hybrid clock configuration to hybrid clock configuration, you must first unconfigure PTP, unconfigure netsync, reconfigure netsync and configure hybrid PTP.

Clocking and Timing Overview

The Cisco ASR 920 Series Router have the following timing ports:

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

You can use the timing ports on the Cisco ASR 920 Series Router to perform the following tasks:

- Provide or receive 1 PPS messages
- Provide or receive time of day (ToD) messages
- Provide output clocking at 10 Mhz, 2.048 Mhz, and 1.544 Mhz (Cisco ASR-920-24SZ-IM Router)

- Receive input clocking at 10 Mhz, 2.048 Mhz, and 1.544 Mhz (Cisco ASR-920-24SZ-IM Router)

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

Understanding PTP

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

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

Table 13: Nodes within a PTP Network

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

Telecom Profiles

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

Effective Cisco IOS-XE Release 3.18, the G.8275.1 telecom profile is also supported on the Cisco ASR920 Series Routers (Cisco ASR-920-12CZ-A/D, ASR-920-4SZ-A/D, Cisco ASR 920-10SZ-PD and Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M). For more information, see G.8275.1 Telecom Profile, on page 213.

PTP Redundancy

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

- Interact with multiple server ports such as grandmaster clocks and boundary clock nodes.
- Open PTP sessions.
- Select the best server clock from the existing list of server clocks (referred to as the PTP server port or server clock source).
- Switch to the next best server clock available in case the first server clock fails, or its connectivity is lost.

Note BMCA can also be triggered if clock class of the newly-added server clock is better. This is true for both, normal PTP as well as PTP with hybrid.

Note The Cisco ASR 920 Series Router supports unicast-based timing as specified in the 1588-2008 standard.

For instructions on how to configure PTP redundancy, see Configuring PTP Redundancy, on page 191.

PTP Redundancy Using Hop-By-Hop Topology Design

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

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

However, with this topology the following issues may occur:

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

No On-Path Support Topology

The topology (see the figure below) describes a ring with no on-path support. S1 to S5 are the boundary clocks that use the same server clocks. GM1 and GM2 are the grandmaster clocks. In this design, the following issues are observed:

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

Figure 3: Deployment in a Ring - No On-Path Support with IPv4

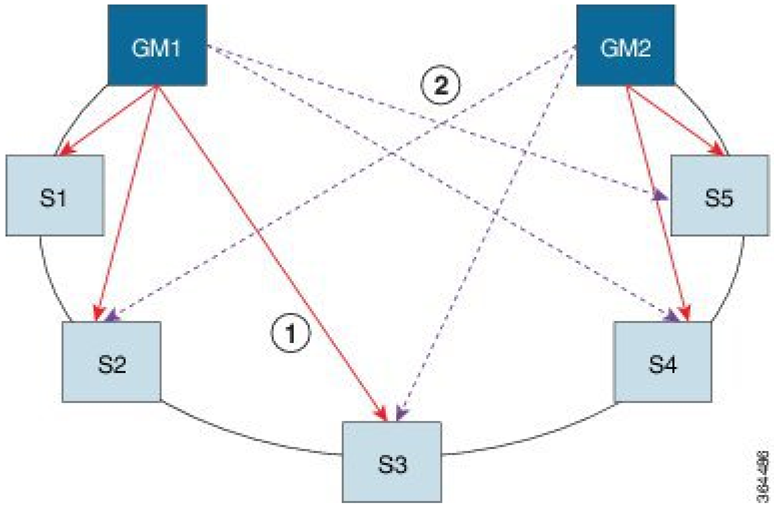


Table 14: PTP Ring Topology—No On-Path Support

Clock Nodes	Behavior in the PTP Ring
GM1	Grandmaster Clock
GM2	Grandmaster Clock
S1	Server clocks: M1 (1st), M2 (2nd)
S2	Server clocks: M1 (1st), M2 (2nd)
S3	Server clocks: M1 (1st), M2 (2nd)
S4	Server clocks: M2 (1st), M1 (2nd)
S5	Server clocks: M2 (1st), M1 (2nd)

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

Hop-By-Hop Topology in a PTP Ring

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

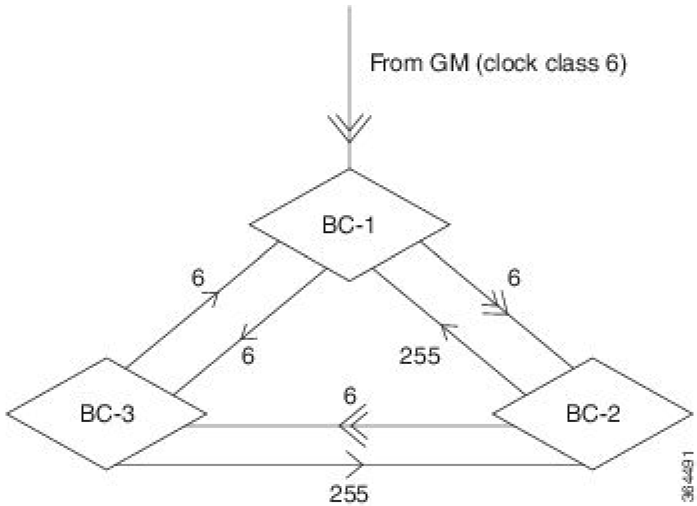
Prerequisites

- PTP boundary clock configuration is required on all clock nodes in the ring, except the server clock nodes (GM), which provide the clock timing to ring. In the above example nodes S1—S5 must be configured as BC.
- The server clock (GM1 and GM2 in the above figure) nodes in the ring can be either a OC server clock or BC server clock.

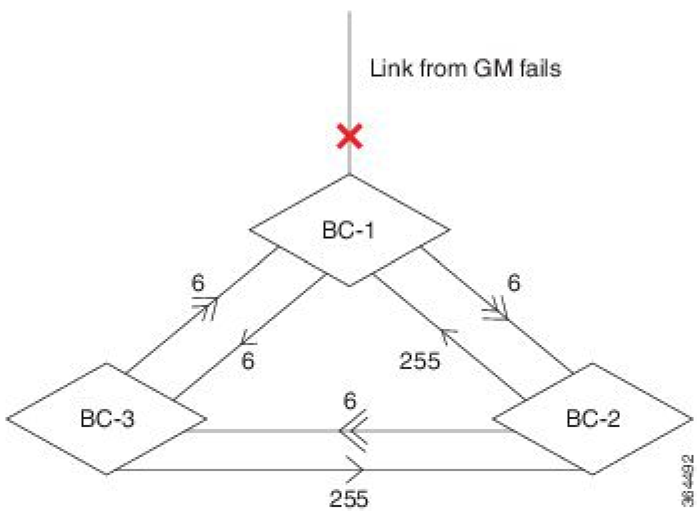
- Instead of each BC using same the GM as a PTP server clock, each BC selects its adjacent nodes as PTP server clocks. These PTP BC-server clocks are traceable to the GM in the network.
- Boundary clock nodes must be configured with the **single-hop** keyword in the PTP configuration to ensure that a PTP node can communicate with it's adjacent nodes only.

Restrictions

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



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



- In a BC configuration, the same loopback interface should never be used for both server port and client port configuration.
- **Single-hop** keyword is not supported for PTP over MPLS with explicit null configuration. The Single-hop keyword is not supported when PTP packets are sent out with a MPLS tag.

On-Path Support Topology Scenario

Consider the topology as shown in the figure:

Figure 4: PTP Ring Topology—On-Path Support

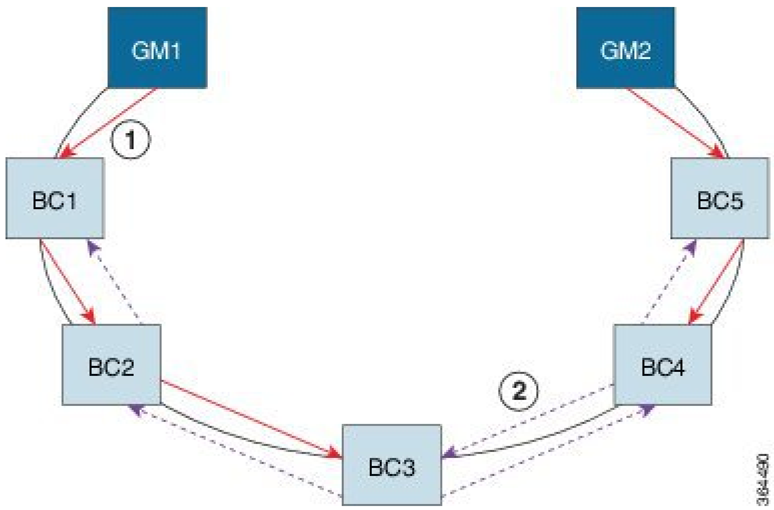


Table 15: PTP Ring Topology—On-Path Support

Clock Node	Behavior in the PTP Ring
GM1	Grandmaster Clock
GM2	Grandmaster Clock
BC1	Server clocks: M1 (1st), BC2 (2nd) Client clocks: BC2
BC2	Server clocks: BC1(1st), BC3 (2nd) Client clocks: BC1, BC3
BC3	Server clocks: BC2 (1st), BC4 (2nd) Client clocks: BC2, BC4
BC4	Server clocks: BC5 (1st), BC3 (2nd) Client clocks: BC3, BC5
BC5	Server clocks: M2(1st), BC4 (2nd) Client clocks: BC4

Now consider there is a failure between BC1 and BC2 (see the figure below). In this case, the BC2 cannot communicate with GM1. Node BC2 receives the clock from BC3, which in turn receives the clock from GM2.

Figure 5: Deployment in a Ring—On-Path Support (Failure)

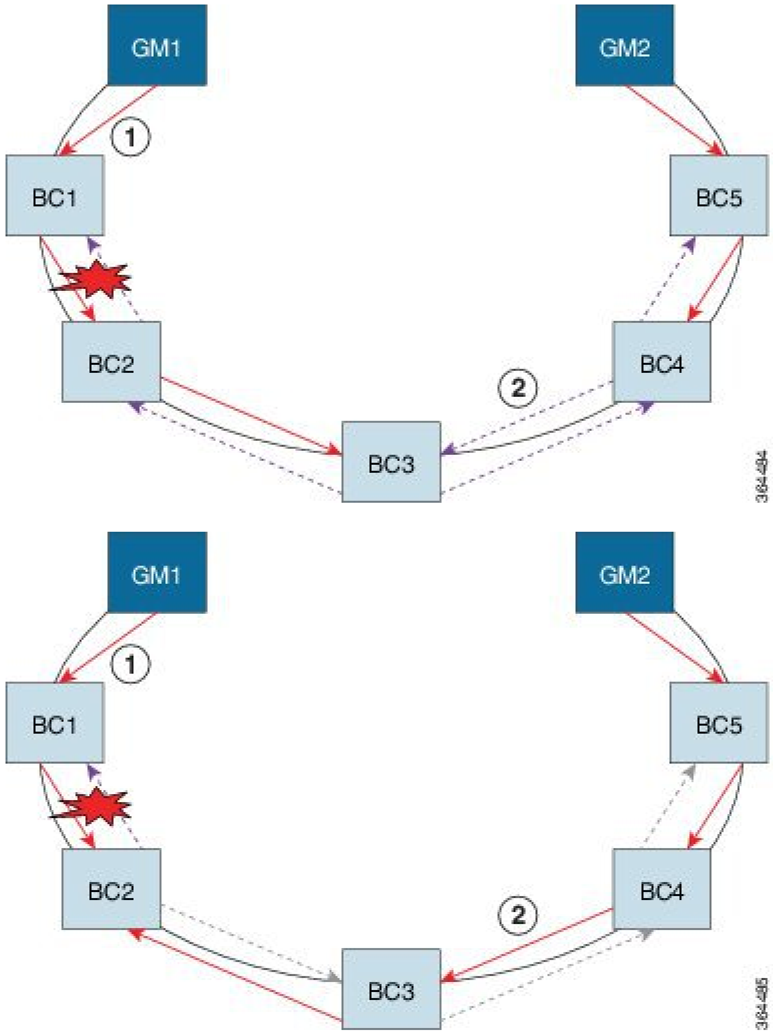


Table 16: PTP Ring Topology—On-Path Support (Failure)

Clock Node	Behavior in the PTP Ring[9]
GM1	Grandmaster Clock
GM2	Grandmaster Clock
BC1	Server clocks: M1 (1st), BC2 (2nd) Client clocks: BC2
BC2	Server clocks: BC1(1st), BC3 (2nd) Client clocks: BC1, BC3
BC3	Server clocks: BC2 (1st), BC4 (2nd) Client clocks: BC2, BC4

Clock Node	Behavior in the PTP Ring[9]
BC4	Server clocks: BC5 (1st), BC3 (2nd) Client clocks: BC3, BC5
BC5	Server clocks: M2(1st), BC4 (2nd) Client clocks: BC4

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

Configuration Example

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

```
ptp clock boundary domain 0
           clock-port client-port slave
               transport ipv4 unicast interface Lo0 negotiation single-hop
               clock source 1.1.1.1
               clock source 2.2.2.2 1
           clock-port server-port master
               transport ipv4 unicast interface Lo1 negotiation single-hop
.
.
```

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

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

BMCA

Effective Cisco IOS-XE Release 3.15.0S, BMCA is supported on the Cisco ASR 920 Series Routers.

BMCA is used to select the server clock on each link, and ultimately, select the grandmaster clock for the entire Precision Time Protocol (PTP) domain. BMCA runs locally on each port of the ordinary and boundary clocks, and selects the best clock.

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

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

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

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

For information on configuring the BMCA, see Configuring Clocking and Timing, on page 174.

Hybrid BMCA

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

Configuration Example: Hybrid BMCA on Ordinary Clock

```
ptp clock ordinary domain 0 hybrid
clock-port client-port slave
transport ipv4 unicast interface Lo0 negotiation
clock source 133.133.133.133
clock source 144.144.144.144 1
clock source 155.155.155.155 2

Network-clock input-source 10 interface gigabitEthernet 0/4
```

Configuration Example: Hybrid BMCA on Boundary Clock

```
ptp clock boundary domain 0 hybrid
clock-port client-port slave
transport ipv4 unicast interface Lo0 negotiation
clock source 133.133.133.133
clock source 144.144.144.144 1
clock source 155.155.155.155 2
clock-port server-port master
transport ipv4 unicast interface Lo1 negotiation

Network-clock input-source 10 interface gigabitEthernet 0/4
```

Hybrid Clocking

The Cisco ASR 920 Series Router support a hybrid clocking mode that uses clock frequency obtained from the synchronous Ethernet port while using the phase (ToD or 1 PPS) obtained using PTP. The combination of using physical source for frequency and PTP for time and phase improves the performance as opposed to using only PTP.

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

For more information on how to configure hybrid clocking, see Configuring a Transparent Clock, on page 183.

Transparent Clocking

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

There are two kinds of transparent clocks:

- End-to-end transparent clock—Measures the residence time of a PTP message and accumulates the times in the correction field of the PTP message or an associated follow-up message.

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

Note The Cisco ASR 920 Series Router does not currently support peer-to-peer transparent clock mode.

For information on how to configure the Cisco ASR 920 Series Router as a transparent clock, see Configuring a Transparent Clock, on page 183.

Time of Day (TOD)

You can use the time of day (ToD) and 1PPS ports on the Cisco ASR 920 Series Router to exchange ToD clocking. In server mode, the router can receive time of day (ToD) clocking from an external GPS unit; the router requires a ToD, 1PPS, and 10MHZ connection to the GPS unit.

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

For instructions on how to configure ToD on the Cisco ASR 920 Series Router, see the Configuring a Server Ordinary Clock, on page 174 and Configuring a Slave Ordinary Clock, on page 179.

Synchronizing the System Clock to Time of Day

You can set the router's system time to synchronize with the time of day retrieved from an external GPS device. For information on how to configure this feature, see Synchronizing the System Time to a Time-of-Day Source, on page 196.

Timing Port Specifications

The following sections provide specifications for the timing ports on the Cisco ASR 920 Series Router.

BITS Framing Support

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

Table 17: Framing Modes for a BITS Port on a Cisco ASR 920 Series Router

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

The BITS port behaves similarly to the T1/E1 ports on the T1/E1 interface module.

Understanding Synchronous Ethernet ESMC and SSM

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

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

When configured to use synchronous Ethernet, the Cisco ASR 920 Series Router synchronizes to the best available clock source. If no better clock sources are available, the router remains synchronized to the current clock source.

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

For more information about Ethernet ESMC and SSM, seeConfiguring Synchronous Ethernet ESMC and SSM, on page 197.

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

Note PTP clock sources are not supported with synchronous Ethernet.

Clock Selection Modes

The Cisco ASR 920 Series Router supports two clock selection modes, which are described in the following sections.

QL-Enabled Mode

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

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

QL-Disabled Mode

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

- Clock availability
- Priority

> **Note** You can use override the default clock selection using the commands described in the Specifying a Clock Source, on page 201 and Disabling a Clock Source, on page 203 sections.

Managing Clock Selection

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

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

For more information about how to use these features, see Specifying a Clock Source, on page 201 and Disabling a Clock Source, on page 203 sections.

Configuring Clocking and Timing

The following sections describe how to configure clocking and timing features on the Cisco ASR 920 Series Router:

Configuring a Server Ordinary Clock

Follow these steps to configure the Cisco ASR 920 Series Router to act as a server ordinary clock.

Procedure

	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 configuration mode.
Step 3	**platform ptp 1pps GPS** **Example:** `Router(config)#platform ptp 1pps GPS`	Enables 1pps SMA port.

	Command or Action	Purpose
Step 4	**ptp clock ordinary domain** *domain-number* **Example:** `Router(config)# ptp clock ordinary domain 0`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
Step 5	**priority1** *priorityvalue* **Example:** `Router(config-ptp-clk)# priority1 priorityvalue`	Sets the preference level for a clock. Client devices use the priority1 value when selecting a server clock: a lower priority1 value indicates a preferred clock. The priority1 value is considered above all other clock attributes. Valid values are from 0-255. The default value is 128.
Step 6	**priority2** *priorityvalue* **Example:** `Router(config-ptp-clk)# priority2 priorityvalue`	Sets a secondary preference level for a clock. Subordinaate devices use the priority2 value when selecting a server clock: a lower priority2 value indicates a preferred clock. The priority2 value is considered only when the router is unable to use priority1 and other clock attributes to select a clock. Valid values are from 0-255. The default value is 128.
Step 7	**utc-offset** *value* **leap-second "date time" offset** {-1 | 1} **Example:** `Router(config-ptp-clk)# utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1`	(Optional) Starting with Cisco IOS-XE Release 3.18SP, the new utc-offset CLI is used to set the UTC offset value. Valid values are from 0-255. The default value is 36. (Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure the current UTC offset, leap second event date and Offset value (+1 or -1). Leap second configuration will work only when the frequency source is locked and ToD was up before. • *"date time"*— Leap second effective date in dd-mm-yyyy hh:mm:ss format.
Step 8	input [1pps] {R0 | R1} **Example:** `Router(config-ptp-clk)# input 1pps R0`	Enables Precision Time Protocol input 1PPS using a 1PPS input port. Use R0 or R1 to specify the active RSP slot.
Step 9	**tod** {**R0** | **R1**} {**ubx** | **nmea** | **cisco** | **ntp**} **Example:**	Configures the time of day message format used by the ToD interface.

	Command or Action	Purpose
	`Router(config-ptp-clk)# tod R0 ntp`	**Note** It is mandatory that when electrical ToD is used, the **utc-offset** command is configured *before* configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the server and client clocks. **Note** The ToD port acts as an input port in case of Server clock and as an output port in case of Client clock.
Step 10	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-clk)# clock-port server-port master`	Defines a new clock port and sets the port to PTP server or client mode; in server mode, the port exchanges timing packets with PTP client devices. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.
Step 11	Do one of the following: • **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]* • **transport ethernet unicast** [**negotiation**] **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation`	Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport. The **negotiation** keyword configures the router to discover a PTP server clock from all available PTP clock sources. **Note** PTP redundancy is supported only on unicast negotiation mode.
Step 12	exit	Exits clock-port configuration.
Step 13	**network-clock synchronization automatic** **Example:** `Router(config)# network-clock synchronization automatic`	Enables automatic selection of a clock source. **Note** This command is mandatory to configure the **leap second** command. **Note** This command must be configured before any input source.
Step 14	**network-clock synchronization mode ql-enabled**	Enables automatic selection of a clock source based on quality level (QL).

	Command or Action	Purpose
	Example: `Router(config)#` **`network-clock synchronization mode ql-enabled`**	**Note** This command is disabled by default.
Step 15	Use one of the following options: • network-clock input-source <priority> controller {SONET | wanphy} • network-clock input-source <priority> external {R0 | R1} [10m | 2m] • network-clock input-source <priority> external {R0 | R1} [2048k | e1 {cas {120ohms | 75ohms | crc4}}] • network-clock input-source <priority> external {R0 | R1} [2048k | e1 {crc4 | fas] {120ohms | 75ohms} {linecode {ami | hdb3}} • network-clock input-source <priority> external {R0 | R1} [t1 {d4 | esf | sf} {linecode {ami | b8zs}}] • network-clock input-source <priority> interface <type/slot/port> **Example:** `Router(config)# network-clock input-source 1 external R0 10m`	• (Optional) To nominate SDH or SONET controller as network clock input source. • (Optional) To nominate 10Mhz port as network clock input source. • (Optional) To nominate BITS port as network clock input source in e1 mode. • (Optional) To nominate BITS port as network clock input source in e1 mode. • (Optional) To nominate BITS port as network clock input source in t1 mode. • (Optional) To nominate Ethernet interface as network clock input source.
Step 16	**clock destination** *source-address* | *mac-address* {**bridge-domain** *bridge-domain-id}* | **interface** *interface-name*} **Example:** `Router(config-ptp-port)# clock-source 8.8.8.1`	Specifies the IP address or MAC address of a clock destination when the router is in PTP server mode.
Step 17	**sync interval** *interval* **Example:** `Router(config-ptp-port)# sync interval -4`	Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values, as follows: • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second

	Command or Action	Purpose
		• -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second. • -7—1 packet every 1/128 seconds, or 128 packets per second.
Step 18	**announce interval** *interval* **Example:** `Router(config-ptp-port)# announce interval 2`	Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows: • 3—1 packet every 8 seconds • 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second
Step 19	**end** **Example:** `Router(config-ptp-port)# end`	Exit configuration mode.

Example

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

```
ptp clock ordinary domain 24

local-priority 1

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

Configuring a Slave Ordinary Clock

Follow these steps to configure the Cisco ASR 920 Series Router to act as a slave ordinary clock.

Procedure

	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`	Enter configuration mode.
Step 3	**ptp clock ordinary domain** *domain-number* [**hybrid**] **Example:** `Router(config)# ptp clock ordinary domain 0`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in Master or Slave mode.
Step 4	**output [1pps] {R0 | R1}** [**offset** *offset-value*] [**pulse-width** *value*] **Example:** `Router(config-ptp-clk)# output 1pps R0 offset 200 pulse-width 20 µsec`	Enables Precision Time Protocol input 1PPS using a 1PPS input port. Use R0 or R1 to specify the active RSP slot. **Note** Effective Cisco IOS XE Everest 16.6.1, on the Cisco ASR-920-12SZ-IM router, the 1pps pulse bandwith can be changed from the default value of 500 milliseconds to up to 20 microsecond.
Step 5	**tod** {**R0 | R1}** {**ubx** | **nmea** | **cisco** | **ntp**} **Example:** `Router(config-ptp-clk)# tod R0 ntp`	Configures the time of day message format used by the ToD interface. **Note** The ToD port acts as an input port in case of Master clock and as an output port in case of Slave clock.
Step 6	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-clk)# clock-port Slave slave`	Sets the clock port to PTP master or slave mode; in slave mode, the port exchanges timing packets with a PTP master clock. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best

	Command or Action	Purpose
		master clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.
Step 7	Do one of the following: • **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]* • • **transport ethernet unicast** [**negotiation**] **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation`	Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport. The **negotiation** keyword configures the router to discover a PTP master clock from all available PTP clock sources. **Note** PTP redundancy is supported only on unicast negotiation mode.
Step 8	**clock source** *source-address* | *mac-address* {**bridge-domain** *bridge-domain-id*} | **interface** *interface-name*} [*priority*] **Example:** `Router(config-ptp-port)# clock-source 8.8.8.1`	Specifies the IP or MAC address of a PTP master clock. • *priority*—Sets the preference level for a PTP clock. • *delay asymmetry value*—Performs the PTP asymmetry readjustment on a PTP node to compensate for the delay in the network.
Step 9	**announce timeout** *value* **Example:** `Router(config-ptp-port)# announce timeout 8`	Specifies the number of PTP announcement intervals before the session times out. Valid values are 1-10.
Step 10	**delay-req interval** *interval* **Example:** `Router(config-ptp-port)# delay-req interval 1`	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state. The intervals are set using log base 2 values, as follows: • 3—1 packet every 8 seconds • 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second

	Command or Action	Purpose
		• -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second. • -7—1 packet every 1/128 seconds, or 128 packets per second.
Step 11	**end** **Example:** `Router(config-ptp-port)# end`	Exit configuration mode.

Configuring a Boundary Clock

Follow these steps to configure the Cisco ASR 920 Series Router to act as a boundary clock.

Procedure

	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`	Enter configuration mode.
Step 3	**ptp clock ordinary domain** *domain-number* **Example:** `Router(config)# ptp clock ordinary domain 0`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.

	Command or Action	Purpose
Step 4	time-properties persist **value** **Example:** `Router(config-ptp-clk)#` **`time-properties persist 600`**	(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure time properties holdover time. Valid values are from 0 to 10000 seconds. When a server clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged. In case leap second midnight occurs when holdover timer is running, utc-offset value is updated based on leap59 or leap61 flags. This value is used as long as there are no PTP packets being received from the selected server clock. In case the selected server clock is sending announce packets, the time-properties advertised by server is used.
Step 5	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-clk)# clock-port client-port slave`	Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.
Step 6	**transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***]* **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation`	Specifies the transport mechanism for clocking traffic. The **negotiation** keyword configures the router to discover a PTP server clock from all available PTP clock sources. **Note** PTP redundancy is supported only on unicast negotiation mode.
Step 7	**clock-source** *source-address [priority]* **Example:** `Router(config-ptp-port)# clock source 133.133.133.133`	Specifies the address of a PTP server clock. You can specify a priority value as follows: • No priority value—Assigns a priority value of 0. • 1—Assigns a priority value of 1.

	Command or Action	Purpose
		• 2—Assigns a priority value of 2, the highest priority.
Step 8	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-port)# clock-port server-port master`	Sets the clock port to PTP server or client mode; in server mode, the port exchanges timing packets with PTP client devices. **Note** The server clock-port does not establish a clocking session until the client clock-port is phase aligned. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.
Step 9	**transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***]* **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation`	Specifies the transport mechanism for clocking traffic. The **negotiation** keyword configures the router to discover a PTP server clock from all available PTP clock sources. **Note** PTP redundancy is supported only on unicast negotiation mode.
Step 10	**end** **Example:** `Router(config-ptp-port)# end`	Exit configuration mode.

Configuring a Transparent Clock

Follow these steps to configure the Cisco ASR 920 Series Router as an end-to-end transparent clock.

Note The Cisco ASR 920 Series Router does not support peer-to-peer transparent clock mode.

Note The transparent clock ignores the domain number.

Procedure

	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`	Enter configuration mode.
Step 3	**ptp clock e2e-transparent domain** *domain-number* **Example:** `Router(config)# ptp clock e2e-transparent domain 0`	Configures the router as an end-to-end transparent clock. • e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at subordinate clock.
Step 4	**exit** **Example:** `Router(config)# exit`	Exit configuration mode.

Configuring a Hybrid Boundary Clock

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

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

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**ptp clock** {**ordinary** | **boundary**} **domain** *domain-number* **hybrid** **Example:** `Router(config)# ptp clock ordinary domain 0 hybrid`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in server or client mode. • boundary—Terminates PTP session from Grandmaster and acts as PTP server to clients downstream.
Step 4	time-properties persist **value** **Example:** `Router(config-ptp-clk)#` **`time-properties persist 600`**	(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure time properties holdover time. Valid values are from 0 to 10000 seconds. The default value is 300 seconds. When a server clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged. In case leap second midnight occurs when holdover timer is running, utc-offset value is updated based on leap59 or leap61 flags. This value is used as long as there are no PTP packets being received from the selected server clock. In case the selected server clock is sending announce packets, the time-properties advertised by server is used.
Step 5	**utc-offset** *value* **leap-second “date time” offset** {-1 | 1} **Example:** `Router(config-ptp-clk)#` **`utc-offset 45 leap-second “01-01-2017 00:00:00” offset 1`**	(Optional) Starting with Cisco IOS-XE Release 3.18SP, the new utc-offset CLI is used to set the UTC offset value. Valid values are from 0-255. The default value is 36. (Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure the current UTC offset, leap second event date and Offset value (+1 or -1). Leap second configuration will work only when the frequency source is locked and ToD was up before. • *“date time”*— Leap second effective date in dd-mm-yyyy hh:mm:ss format.

	Command or Action	Purpose
Step 6	**min-clock-class** *value* **Example:** `Router(config-ptp-clk)#` **`min-clock-class 157`**	Sets the threshold clock-class value. This allows the PTP algorithm to use the time stamps from an upstream server clock, only if the clock-class sent by the server clock is less than or equal to the configured threshold clock-class. Valid values are from 0-255. **Note** Min-clock-class value is supported only for PTP with single server source configuration.
Step 7	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-clk)# clock-port client-port slave`	Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock. **Note** Hybrid mode is only supported with client clock-ports; server mode is not supported. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.

Step 8	**transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***] [***single-hop**]
	Example:
	`Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation`
	Example:
	`Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop`
		Specifies the transport mechanism for clocking traffic.
		• **negotiation**—**(Optional)** configures the router to discover a PTP server clock from all available PTP clock sources.
		Note PTP redundancy is supported only on unicast negotiation mode.
		Note **single-hop—(Optional) Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.**

Step 9	**clock-source** *source-address [priority]* **Example:** `Router(config-ptp-port)# clock source 133.133.133.133`	Specifies the address of a PTP server clock. You can specify a priority value as follows: • No priority value—Assigns a priority value of 0. • 1—Assigns a priority value of 1.

	Command or Action	Purpose
		• 2—Assigns a priority value of 2, the highest priority.
Step 10	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-port)# clock-port server-port master`	Sets the clock port to PTP server or client mode; in server mode, the port exchanges timing packets with PTP client devices. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.

Step 11	**transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***] [***single-hop]**
	Example:
	`Router(config-ptp-port)# transport ipv4 unicast interface Lo1 negotiation`
	Example:
	`Router(config-ptp-port)# transport ipv4 unicast interface Lo1 negotiation single-hop`
		Specifies the transport mechanism for clocking traffic.
		• **negotiation**—**(Optional)** configures the router to discover a PTP server clock from all available PTP clock sources.
		Note PTP redundancy is supported only on unicast negotiation mode.
		• **single-hop—(Optional) Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.**

Step 12	**exit**	Exits clock-port configuration.
Step 13	**network-clock synchronization automatic** **Example:** `Router(config)# network-clock synchronization automatic`	Enables automatic selection of a clock source. **Note** This command is mandatory to configure the **leap second** command. **Note** This command must be configured before any input source.
Step 14	**network-clock synchronization mode ql-enabled** **Example:** `Router(config)# network-clock synchronization mode ql-enabled`	Enables automatic selection of a clock source based on quality level (QL). **Note** This command is disabled by default.

	Command or Action	Purpose
Step 15	Use one of the following options: • network-clock input-source <priority> controller {SONET | wanphy} • network-clock input-source <priority> external {R0 | R1} [10m | 2m] • network-clock input-source <priority> external {R0 | R1} [2048k | e1 {cas {120ohms | 75ohms | crc4}}] • network-clock input-source <priority> external {R0 | R1} [2048k | e1 {crc4 | fas] {120ohms | 75ohms} {linecode {ami | hdb3}} • network-clock input-source <priority> external {R0 | R1} [t1 {d4 | esf | sf} {linecode {ami | b8zs}}] • network-clock input-source <priority> interface <type/slot/port> **Example:** `Router(config)# network-clock input-source 1 external R0 10m`	• (Optional) To nominate SDH or SONET controller as network clock input source. • (Optional) To nominate 10Mhz port as network clock input source. • (Optional) To nominate BITS port as network clock input source in e1 mode. • (Optional) To nominate BITS port as network clock input source in e1 mode. • (Optional) To nominate BITS port as network clock input source in t1 mode. • (Optional) To nominate Ethernet interface as network clock input source.
Step 16	network-clock synchronization input-threshold *ql value* **Example:** `Router(config)#` **`network-clock synchronization input-threshold ql value`**	(Optional) Starting with Cisco IOS-XE Release 3.18SP, this new CLI is used to set the threshold QL value for the input frequency source. The input frequency source, which is better than or equal to the configured threshold QL value, will be selected to recover the frequency. Otherwise, internal clock is selected.
Step 17	**network-clock hold-off** {**0** | *milliseconds*} **Example:** `Router(config)# network-clock hold-off 0`	(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action. **Note** You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.
Step 18	**end** **Example:** `Router(config)# end`	Exit configuration mode.

Configuring a Hybrid Ordinary Clock

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

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

Procedure

	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`	Enter configuration mode.
Step 3	**ptp clock** {**ordinary** | **boundary**} **domain** *domain-number* **hybrid** **Example:** `Router(config)# ptp clock ordinary domain 0 hybrid`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in server or client mode. • boundary—Terminates PTP session from Grandmaster and acts as PTP server to clients downstream.
Step 4	**output [1pps] {R0 | R1}** [**offset** *offset-value*] [**pulse-width** *value*] **Example:** `Router(config-ptp-clk)# output 1pps R0 offset 200 pulse-width 20 µsec`	Enables Precision Time Protocol input 1PPS using a 1PPS input port. Use R0 or R1 to specify the active RSP slot. **Note** Effective Cisco IOS XE Everest 16.6.1, on the Cisco ASR-920-12SZ-IM router, the 1pps pulse bandwith can be changed from the default value of 500 milliseconds to up to 20 microsecond.
Step 5	**tod** {**R0** | **R1}** {**ubx** | **nmea** | **cisco** | **ntp**} **Example:**	Configures the time of day message format used by the ToD interface.

	Command or Action	Purpose
	`Router(config-ptp-clk)# tod R0 ntp`	**Note** The ToD port acts as an input port in case of server clock and as an output port in case of client clock.
Step 6	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-clk)# clock-port client-port slave`	Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock. **Note** Hybrid mode is only supported with client clock-ports; server mode is not supported. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.
Step 7	**transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]* **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation`	Specifies the transport mechanism for clocking traffic. The **negotiation** keyword configures the router to discover a PTP server clock from all available PTP clock sources. **Note** PTP redundancy is supported only on unicast negotiation mode.
Step 8	**clock-source** *source-address [priority]* **Example:** `Router(config-ptp-port)# clock source 133.133.133.133`	Specifies the address of a PTP server clock. You can specify a priority value as follows: • No priority value—Assigns a priority value of 0. • 1—Assigns a priority value of 1. • 2—Assigns a priority value of 2, the highest priority.
Step 9	**exit** **Example:** `Router(config-ptp-port)# exit`	Exit clock-port configuration.
Step 10	Use one of the following options: • network-clock input-source <priority> controller {SONET | wanphy} • network-clock input-source <priority> external {R0 | R1} [10m | 2m]	• (Optional) To nominate SDH or SONET controller as network clock input source. • (Optional) To nominate 10Mhz port as network clock input source.

	Command or Action	Purpose
	• network-clock input-source <priority> external {R0 | R1} [2048k | e1 {cas {120ohms | 75ohms | crc4}}] • network-clock input-source <priority> external {R0 | R1} [2048k | e1 {crc4 | fas] {120ohms | 75ohms} {linecode {ami | hdb3}} • network-clock input-source <priority> external {R0 | R1} [t1 {d4 | esf | sf} {linecode {ami | b8zs}}] • network-clock input-source <priority> interface <type/slot/port> **Example:** `Router(config)# network-clock input-source 1 external R0 10m`	• (Optional) To nominate BITS port as network clock input source in e1 mode. • (Optional) To nominate BITS port as network clock input source in e1 mode. • (Optional) To nominate BITS port as network clock input source in t1 mode. • (Optional) To nominate Ethernet interface as network clock input source.
Step 11	**network-clock synchronization mode ql-enabled** **Example:** `Router(config-ptp-clk)# network-clock synchronization mode ql-enabled`	Enables automatic selection of a clock source based on quality level (QL). **Note** This command is disabled by default.
Step 12	**network-clock hold-off** {**0** | *milliseconds*} **Example:** `Router(config-ptp-clk)# network-clock hold-off 0`	(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action. **Note** You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.
Step 13	**end** **Example:** `Router(config-ptp-clk)# end`	Exit configuration mode.

Configuring PTP Redundancy

The following sections describe how to configure PTP redundancy on the Cisco ASR 920 Series Router:

Configuring PTP Redundancy in Client Clock Mode

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

Procedure

	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`	Enter configuration mode.
Step 3	**ptp clock** {**ordinary** | **boundary**} **domain** *domain-number* [**hybrid**] **Example:** `Router(config)# ptp clock ordinary domain 0`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in server or client mode. • boundary—Terminates PTP session from Grandmaster and acts as PTP server to clients downstream.
Step 4	**ptp clock e2e-transparent domain** *domain-number* **Example:** `Router(config)# ptp clock e2e-transparent domain 0`	Configures the PTP clock. • e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at client.
Step 5	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-clk)# clock-port client-port slave`	Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.
Step 6	**transport ipv4 unicast interface** *interface-type interface-number [***negotiation***] [***single-hop]** **Example:** `Router(config-ptp-port)# transport ipv4`	Specifies the transport mechanism for clocking traffic. • **negotiation**—(Optional) Configures the router to discover a PTP server clock from all available PTP clock sources.

	Command or Action	Purpose

	`unicast interface Loopback 0 negotiation`
	Example:
	`Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop`
		Note PTP redundancy is supported only on unicast negotiation mode.
		• **single-hop**—(Optional) **It ensures that the PTP node communicates only with the adjacent nodes.**

Step 7	**clock-source** *source-address [priority]* **Example:** `Router(config-ptp-port)# clock source 133.133.133.133 1`	Specifies the address of a PTP server clock. You can specify a priority value as follows: • No priority value—Assigns a priority value of 0. • 1—Assigns a priority value of 1. • 2—Assigns a priority value of 2, the highest priority.
Step 8	**clock-source** *source-address [priority]* **Example:** `Router(config-ptp-port)# clock source 133.133.133.134 2`	Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.
Step 9	**clock-source** *source-address [priority]* **Example:** `Router(config-ptp-port)# clock source 133.133.133.135`	Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to 3 server clocks.
Step 10	**end** **Example:** `Router(config-ptp-port)# end`	Exit configuration mode.

Configuring PTP Redundancy in Boundary Clock Mode

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

Procedure

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

	Command or Action	Purpose
Step 3	**ptp clock** {**ordinary** | **boundary**} **domain** *domain-number* [**hybrid**] **Example:** `Router(config)# ptp clock ordinary domain 0`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in server or client mode. • boundary—Terminates PTP session from Grandmaster and acts as PTP server to clients downstream.
Step 4	**ptp clock e2e-transparent domain** *domain-number* **Example:** `Router(config)# ptp clock e2e-transparent domain 0`	Configures the PTP clock. • e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at client.
Step 5	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-clk)# clock-port client-port slave`	Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.

Step 6	**transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]* *[***single-hop]**
	Example:
	`Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation`
	Example:
	`Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop`
		Specifies the transport mechanism for clocking traffic.
		• **negotiation**—(Optional) Configures the router to discover a PTP server clock from all available PTP clock sources.
		Note PTP redundancy is supported only on unicast negotiation mode.
		• **single-hop—**(Optional) **Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.**

Step 7	**clock-source** *source-address [priority]* **Example:**	Specifies the address of a PTP server clock. You can specify a priority value as follows:

	Command or Action	Purpose
	`Router(config-ptp-port)# clock source 133.133.133.133 1`	• No priority value—Assigns a priority value of 0. • 1—Assigns a priority value of 1. • 2—Assigns a priority value of 2, the highest priority.
Step 8	**clock-source** *source-address [priority]* **Example:** `Router(config-ptp-port)# clock source 133.133.133.134 2`	Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to 3 server clocks.
Step 9	**clock-source** *source-address [priority]* **Example:** `Router(config-ptp-port)# clock source 133.133.133.135`	Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to 3 server clocks.
Step 10	**clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}] **Example:** `Router(config-ptp-port)# clock-port server-port master`	Specifies the address of a PTP server clock. The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. **Note** Using a telecom profile requires that the clock have a domain number of 4–23.
Step 11	**transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]* *[***single-hop]** **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation single-hop`	Specifies the transport mechanism for clocking traffic. • **negotiation**—(Optional) Configures the router to discover a PTP server clock from all available PTP clock sources. **Note** PTP redundancy is supported only on unicast negotiation mode. • **single-hop—**(Optional) **Must be configured if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes**
Step 12	**end** **Example:** `Router(config-ptp-port)# end`	Exit configuration mode.

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

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

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

Note System time to a ToD source (Server Mode) can be configured only when PTP server is configured. See Configuring a Server Ordinary Clock, on page 174. Select any one of the four available ToD format; cisco, nmea, ntp or ubx.10m must be configured as network clock input source.

Follow these steps to configure the system clock to a ToD source in server mode.

Procedure

	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`	Enter configuration mode.
Step 3	**tod-clock input-source** *priority* {**gps** {**R0** | **R1**} | **ptp domain** *domain*} **Example:** `Router(config)# TOD-clock 2 gps R0/R1`	In server mode, specify a GPS port connected to a ToD source.
Step 4	**exit** **Example:** `Router(config)# exit`	Exit configuration mode.

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

Note System time to a ToD source (Client Mode) can be configured only when PTP client is configured. See Configuring a Slave Ordinary Clock, on page 179.

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

Procedure

	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`	Enter configuration mode.
Step 3	**tod-clock input-source** *priority* {**gps** {**R0** | **R1**} | **ptp domain** *domain*} **Example:** `Router(config)# TOD-clock 10 ptp domain 0`	In client mode, specify a PTP domain as a ToD input source.
Step 4	Router(config)# **end**	Exit configuration mode.

Synchronous Ethernet ESMC and SSM

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

Configuring Synchronous Ethernet ESMC and SSM

Follow these steps to configure ESMC and SSM on the Cisco ASR 920 Series Router:

Procedure

	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	**network-clock synchronization automatic** **Example:**	Enables the network clock selection algorithm. This command disables the Cisco-specific

	Command or Action	Purpose
	`Router(config)# network-clock synchronization automatic`	network clock process and turns on the G.781-based automatic clock selection process. **Note** This command must be configured before any input source.
Step 4	**network-clock eec** {**1** | **2**} **Example:** `Router(config)# network-clock eec 1`	Specifies the Ethernet Equipment Clock (EEC) type. Valid values are • 1—ITU-T G.8262 option 1 (2048) • 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544)
Step 5	**network-clock synchronization ssm option** {**1** | **2** {**GEN1** | **GEN2**}} **Example:** `Router(config)# network-clock synchronization ssm option 2 GEN2`	Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command: • Option 1 refers to G.781 synchronization option 1, which is designed for Europe. This is the default value. • Option 2 refers to G.781 synchronization option 2, which is designed for the United States. • GEN1 specifies option 2 Generation 1 synchronization. • GEN2 specifies option 2 Generation 2 synchronization.
Step 6	Use one of the following options: • network-clock input-source <priority> controller {SONET | wanphy} • network-clock input-source <priority> external {R0 | R1} [10m | 2m] • network-clock input-source <priority> external {R0 | R1} [2048k | e1 {cas {120ohms | 75ohms | crc4}}] • network-clock input-source <priority> external {R0 | R1} [2048k | e1 {crc4 | fas] {120ohms | 75ohms} {linecode {ami | hdb3}} • network-clock input-source <priority> external {R0 | R1} [t1 {d4 | esf | sf} {linecode {ami | b8zs}}] • network-clock input-source <priority> interface <type/slot/port> • network-clock input-source <priority> ptp domain <domain-number> **Example:**	• (Optional) To nominate SDH or SONET controller as network clock input source. • (Optional) To nominate 10Mhz port as network clock input source. • (Optional) To nominate BITS port as network clock input source in e1 mode. • (Optional) To nominate BITS port as network clock input source in e1 mode. • (Optional) To nominate BITS port as network clock input source in t1 mode. • (Optional) To nominate Ethernet interface as network clock input source. • (Optional) To nominate PTP as network clock input source.

	Command or Action	Purpose
	`Router(config)# network-clock input-source 1 external R0 10m`	
Step 7	**network-clock synchronization mode ql-enabled** **Example:** `Router(config)# network-clock synchronization mode ql-enabled`	Enables automatic selection of a clock source based on quality level (QL). **Note** This command is disabled by default.
Step 8	**network-clock hold-off** {**0** | *milliseconds*} **Example:** `Router(config)# network-clock hold-off 0`	(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action. **Note** You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.
Step 9	**network-clock wait-to-restore** *seconds* **Example:** `Router(config)# network-clock wait-to-restore 70`	(Optional) Configures a global wait-to-restore timer for synchronous Ethernet clock sources. The timer specifies how long the router waits before including a restored clock source in the clock selection process. Valid values are 0 to 86400 seconds. The default value is 300 seconds. **Note** You can also specify a wait-to-restore value for an individual interface using the **network-clock wait-to-restore** command in interface mode.
Step 10	**network-clock revertive** **Example:** `Router(config)# network-clock revertive`	(Optional) Sets the router in revertive switching mode when recovering from a failure. To disable revertive mode, use the **no** form of this command.
Step 11	**esmc process** **Example:** `Router(config)# esmc process`	Enables the ESMC process globally.
Step 12	**network-clock external** *slot/card/port* **hold-off** {**0** | *milliseconds*} **Example:** `Router(config)# network-clock external 0/1/0 hold-off 0`	Overrides the hold-off timer value for the external interface.

	Command or Action	Purpose
Step 13	**network-clock quality-level** {**tx** | **rx**} *value* {**controller** [**E1**| **BITS**] *slot/card/port* | external [**2m** | **10m** | **2048k** | **t1** | **e1**] } **Example:** `Router(config)# network-clock quality-level rx qL-pRC external R0 e1 cas crc4`	Specifies a quality level for a line or external clock source. The available quality values depend on the G.781 synchronization settings specified by the **network-clock synchronization ssm option** command: • Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU. • Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS. • Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.

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

Step 15	**synchronous mode** **Example:** `Router(config-if)# synchronous mode`	Configures the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface.
Step 16	network-clock source quality-level *value* {**tx** | **rx**} **Example:** `Router(config-if)# network-clock source quality-level QL-PrC tx`	Applies quality level on sync E interface. The available quality values depend on the G.781 synchronization settings specified by the **network-clock synchronization ssm option** command: • Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU. • Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS. • Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.

	Command or Action	Purpose
Step 17	**esmc mode** [**ql-disabled** | **tx** | **rx**] *value* **Example:** `Router(config-if)# esmc mode rx QL-STU`	Enables the ESMC process at the interface level. The **no** form of the command disables the ESMC process.
Step 18	**network-clock hold-off** {*0* | *milliseconds*} **Example:** `Router(config-if)# network-clock hold-off 0`	(Optional) Configures an interface-specific hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action. You can configure the hold-off time to either 0 or any value between 50 to 10000 ms. The default value is 300 ms.
Step 19	**network-clock wait-to-restore** *seconds* **Example:** `Router(config-if)# network-clock wait-to-restore 70`	(Optional) Configures the wait-to-restore timer for an individual synchronous Ethernet interface.
Step 20	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

What to do next

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

Specifying a Clock Source

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

Selecting a Specific Clock Source

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

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

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

Forcing a Clock Source Selection

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

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

> **Note** Forcing a clock source selection overrides a clock selection using the **network-clock switch manual command.**

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

Disabling Clock Source Specification Commands

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

Command	Purpose
network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]} `Router#` **`network-clock clear switch t0`**	Disable a clock source selection.

Disabling a Clock Source

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

Locking Out a Clock Source

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

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

Restoring a Clock Source

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

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

Verifying the Configuration

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

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

- **show network-clock synchronization detail**—Displays the details of network clock synchronization parameters at the global and interface levels.
- **show ptp clock dataset**
- **show ptp port dataset**
- **show ptp clock running**
- **show platform software ptpd statistics**
- **show platform ptp all**
- **show platform ptp tod all**

Troubleshooting

The below table list the debug commands that are available for troubleshooting the SyncE configuration on the Cisco ASR 920 Series Router:

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

Table 18: SyncE Debug Commands

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

The below table provides the information about troubleshooting your configuration

Table 19: Troubleshooting Scenarios

Problem	Solution
Clock selection	• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command. • Ensure that the nonrevertive configurations are in place. • Reproduce the issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm commands. Contact Cisco Technical Support if the issue persists.

Problem	Solution
Incorrect QL values	• Ensure that there is no framing mismatch with the SSM option. • Reproduce the issue using the debug network-clock errors and debug network-clock event commands.
Alarms	• Reproduce the issue using the debug platform network-clock command enabled in the RSP. Alternatively, enable the debug network-clock event and debug network-clock errors commands.
Incorrect clock limit set or queue limit disabled mode	• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command. • Use the **show network-clock synchronization** command to confirm if the system is in revertive mode or nonrevertive mode and verify the non-revertive configurations. • Reproduce the current issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm RSP commands.
Incorrect QL values when you use the **show network-clock synchronization detail** command.	• Use the **network clock synchronization SSM** (*option 1* |*option 2*) command to confirm that there is no framing mismatch. Use the **show run interface** command to validate the framing for a specific interface. For the SSM option 1, framing should be SDH or E1, and for SSM option 2, it should be T1. • Reproduce the issue using the debug network-clock errors and debug network-clock event RSP commands.

Configuration Examples

This section contains sample configurations for clocking features on the Cisco ASR 920 Series Router.

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

Ordinary Clock—Client

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

Ordinary Clock —Client Mode (Ethernet)

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

Ordinary Clock—Server

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

Ordinary Clock—Server (Ethernet)

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

Unicast Configuration—Client Mode

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

Unicast Configuration—Client Mode (Ethernet)

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

Unicast Configuration—Server Mode

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

Unicast Configuration—Server Mode (Ethernet)

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

Unicast Negotiation—Client

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

Unicast Negotiation—Client (Ethernet)

```
ptp clock ordinary domain 0
```

```
  clock-port subordinate-port slave
    transport ethernet unicast negotiation
      clock source 1234.5678.90ab bridge-domain 5 5
  clock-port subordinate-port1 slave
    transport ethernet unicast negotiation
      clock source 1234.9876.90ab interface gigabitethernet 0/0/4 2
```

Unicast Negotiation—Server

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

Unicast Negotiation—Server (Ethernet)

```
ptp clock ordinary domain 0
clock-port server-port master
transport ethernet unicast negotiation
```

Boundary Clock

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

Transparent Clock

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

Hybrid Clock—Boundary

```
network-clock synchronization automatic
ptp clock boundary domain 0 hybrid
 clock-port subordinate-port slave
  transport ipv4 unicast interface Loopback0 negotiation
  clock source 133.133.133.133
 clock-port server-port master
  transport ipv4 unicast interface Loopback1 negotiation
Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

Hybrid Clock—Client

```
network-clock synchronization automatic
ptp clock ordinary domain 0 hybrid
 clock-port subordinate-port slave
  transport ipv4 unicast interface Loopback 0 negotiation
  clock source 133.133.133.133

Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

PTP Redundancy—Client

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

PTP Redundancy—Boundary

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

Hop-By-Hop PTP Redundancy—Client

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

Hop-By-Hop PTP Redundancy—Boundary

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

Time of Day Source—Server

```
TOD-clock 10 gps R0/R1
```

Time of Day Source—Client

```
TOD-clock 10 ptp R0/R1
```

Clock Selection Parameters

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

ToD/1PPS Configuration—Server

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

ToD/1PPS Configuration—Client

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

Show Commands

```
Router# show ptp clock dataset ?
  current          currentDS dataset
  default          defaultDS dataset
  parent           parentDS dataset
  time-properties  timePropertiesDS dataset
Router# show ptp port dataset ?
 foreign-master  foreignMasterDS dataset
 port            portDS dataset
Router# show ptp clock running domain 0
                      PTP Ordinary Clock [Domain 0]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         ACQUIRING      1              98405          296399         Track one
                               PORT SUMMARY
   PTP Master
Name               Tx Mode      Role         Transport    State        Sessions     Port
Addr
SLAVE              unicast      slave              Lo0          Slave              1
     8.8.8.8
                             SESSION INFORMATION
SLAVE [Lo0] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs
 8.8.8.8            296399     98405      0          0
Router#
Router# show platform software ptpd stat stream 0
LOCK STATUS : PHASE LOCKED
SYNC Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 0, Acting Interval 0
  Tx packets : 0,  Rx Packets : 169681
  Last Seq Number : 0,  Error Packets : 1272
Delay Req Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 0, Acting Interval : 0
  Tx packets : 84595, Rx Packets : 0
  Last Seq Number : 19059, Error Packets : 0
!output omitted for brevity
Current Data Set
  Offset from master :  0.4230440
  Mean Path Delay :  0.0
  Steps Removed 1
General Stats about this stream
```

```
  Packet rate : 0, Packet Delta (ns) : 0
  Clock Stream handle : 0, Index : 0
  Oper State : 6, Sub oper State : 7
  Log mean sync Interval : -5, log mean delay req int : -4
Router# show platform ptp all
Slave info  : [Loopback0][0x38A4766C]
--------------------------------
clock role          : SLAVE
Slave Port hdl      : 486539266
Tx Mode             : Unicast-Negotiation
Slave IP            : 4.4.4.4
Max Clk Srcs        : 1
Boundary Clock      : FALSE
Lock status         : HOLDOVER
Refcnt              : 1
Configured-Flags    : 0x7F - Clock Port Stream
Config-Ready-Flags  : Port Stream
-----------
PTP Engine Handle   : 0
Master IP           : 8.8.8.8
Local Priority      : 0
Set Master IP       : 8.8.8.8
Router# show platform ptp tod all
--------------------------------
ToD/1PPS Info for 0/0
--------------------------------
ToD CONFIGURED        : YES
ToD FORMAT            : NMEA
ToD DELAY             : 0
1PPS MODE             : OUTPUT
OFFSET                : 0
PULSE WIDTH           : 0
ToD CLOCK             : Mon Jan 1  00:00:00 UTC 1900
Router# show ptp clock running domain 0
                      PTP Boundary Clock [Domain 0]
State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
PHASE_ALIGNED  2              32355          159516         Hot standby
PORT SUMMARY

  PTP Master
Name              Tx Mode      Role         Transport State        Sessions Port Addr

Subordinate             unicast      slave        Ethernet                            1
        9.9.9.1
Primary                 unicast      master       Ethernet  -                 2
  -
                             SESSION INFORMATION

Subordinate [Ethernet] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs

 9.9.9.1            159083     31054      0          0

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

Input Synchronous Ethernet Clocking

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

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

CHAPTER 15

G.8275.1 Telecom Profile

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

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

Effective Cisco IOS-XE Release 3.18S, Cisco ASR 920 Series Aggregation Services Routers support the G.8275.1 telecom profile. This profile targets accurate time and phase distribution and requires boundary clocks at every node in the network.

Effective Cisco IOS-XE Release 3.18SP, Cisco ASR 920 Series Aggregation Services Routers support the G.8273.2 telecom recommendation.

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

Why G.8275.1?

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

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

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

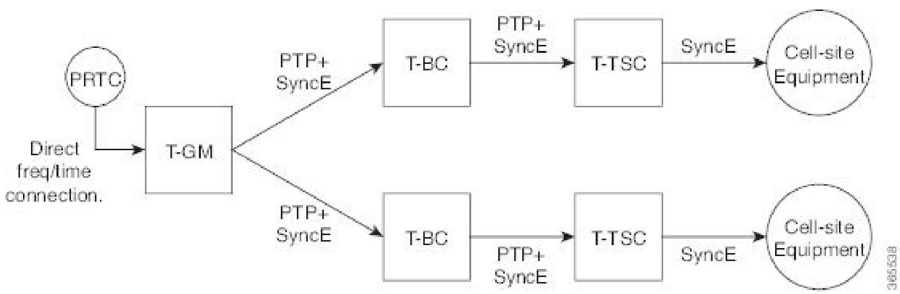
More About G.8275.1

The G.8275.1 must meet the following requirements:

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

The following figure describes a sample G.8275.1 topology.

Figure 6: A Sample G.8275.1 Topology



PTP Domain

A PTP domain is a logical grouping of clocks that communicate with each other using the PTP protocol.

A single computer network can have multiple PTP domains operating separately, for example, one set of clocks synchronized to one time scale and another set of clocks synchronized to another time scale. PTP can run over either Ethernet or IP, so a domain can correspond to a local area network or it can extend across a wide area network.

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

PTP Messages and Transport

The following PTP transport parameters are defined:

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

The source MAC address is the interface MAC address.

- For receiving PTP packets, both multicast MAC addresses (01-80-C2-00-00-0E and 01-1B-19-00-00-00) are supported.
- The packet rate for Announce messages is 8 packets-per-second. For Sync, Delay-Req, and Delay-Resp messages, the rate is 16 packets-per-second.

• Signaling and management messages are not used.

PTP Modes

Two-Way Operation

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

One-Step and Two-Step Clock Mode

Both one-step and two-step clock modes are supported in the G.8275.1 profile.

A subordinate port must be capable of receiving and processing messages from both one-step clocks and two-step clocks, without any particular configuration. However, the primary clock supports only one-step mode.

PTP Clocks

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

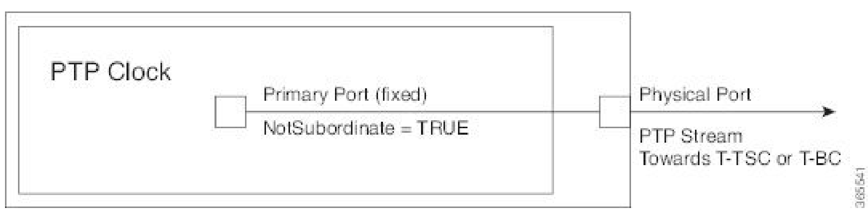
Ordinary Clock (OC)

1. OC that can only be a grandmaster clock (T-GM). In this case, one or more PTP ports will be used as server ports.

   The T-GM uses the frequency, 1PPS, and ToD input from an upstream grandmaster clock.

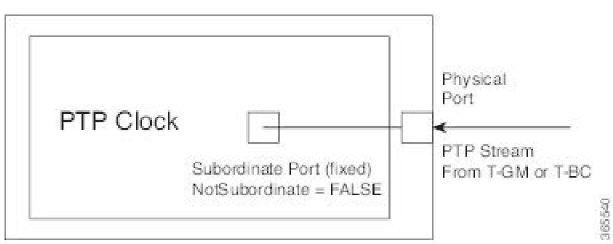
   Note The T-GM server port is a fixed server port.

Figure 7: Ordinary Clock As T-GM



2. OC that can only be a subordinate/client clock (T-TSC). In this case, only one PTP port is used for T-TSC, which in turn will have only one PTP server clock associated with it.

Figure 8: Ordinary Clock As Subordinate/Client Clock (T-TSC)

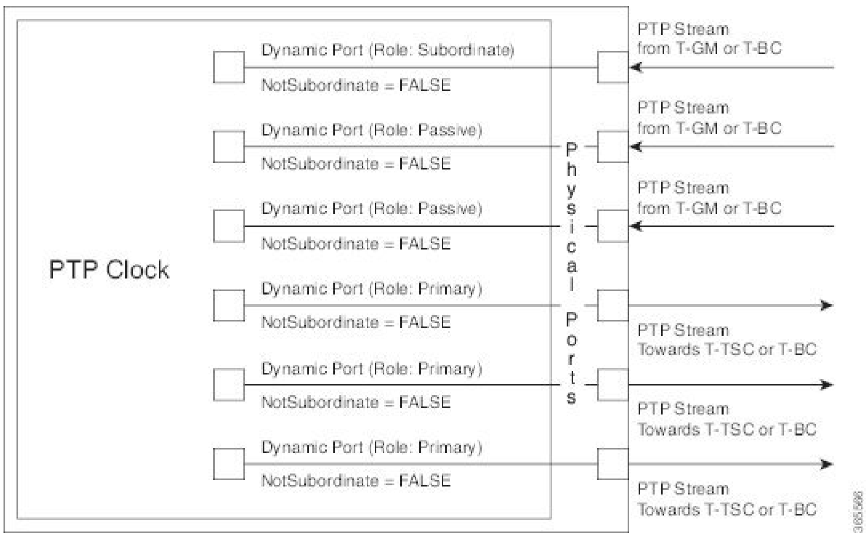


Boundary Clock (T-BC)

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

If the BMCA selects a port on the T-BC to be a server port, all other ports are moved into the server role or a passive state.

Figure 9: Boundary Clock



PTP Ports

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

A server port provides the clock to its downstream peers.

A client port receives clock from an upstream peer.

A dynamic port can work either as a server or a client clock based on the BMCA decision.

In Cisco's implementation of the G.8275.1:

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

Virtual Port Support on T-BC

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

Alternate Best Primary Clock Algorithm

> **Note** The BMCA is referred to as the Best Primary Clock Algorithm in this document.

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

Benefits

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

Prerequisites for Using the G.8275.1 Profile

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

Restrictions for Using the G.8275.1 Profile

- PTP Transparent clocks are not permitted in this profile.
- Changing PTP profile under an existing clock configuration is not allowed. Different ports under the same clock cannot have different profiles. You must remove clock configuration before changing the PTP profile. Only removing all the ports under a clock is not sufficient.
- One PTP port is associated with only one physical port in this profile.
- There is no support for BDI and VLAN.
- Signaling and management messages are not used.
- PTP message rates are not configurable.
- Non-hybrid T-TSC and T-BC clock configurations are not supported.

Configuring the G.8275.1 Profile

> **Note** To know more about the commands referenced in this module, see the Cisco IOS Interface and Hardware Component Command Reference or the Cisco IOS Master Command List.

Configuring Physical Frequency Source

For more information, see the Configuring Synchronous Ethernet ESMC and SSM, on page 197 section in the Clocking and Timing chapter of this book.

Creating a Server-Only Ordinary Clock

```
ptp clock ordinary domain 24
local-priority 1
priority2 128
clock-port server-port-1 master profile g8275.1 local-priority 1
transport ethernet multicast interface Gig 0/0/1
clock-port server-port-2 master profile g8275.1
transport ethernet multicast interface Gig 0/0/2
clock-port server-port-3 master profile g8275.1
transport ethernet multicast interface Gig 0/0/3
clock-port server-port-4 master profile g8275.1
transport ethernet multicast interface  Gig 0/0/4
```

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

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

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

Associated Commands

- ptp clock
- local-priority
- priority2

Creating an Ordinary Subordinate

```
ptp clock ordinary domain 24 hybrid
clock-port subordinate-port slave profile g8275.1
transport ethernet multicast interface Gig 0/0/0
```

Creating Dynamic Ports

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

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

Configuring Virtual Ports

Restrictions

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

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

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

Associated Commands

input

Verifying the Local Priority of the PTP Clock

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

```
  Clock Quality:
    Class: 224
    Accuracy: Unknown
    Offset (log variance): 4252
```

Verifying the Port Parameters

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

Verifying the Foreign Master Information

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

Current Master: SLA

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

Verifying Current PTP Time

```
Router# show platform software ptpd tod
PTPd ToD information:

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

Verifying the Virtual Port Status

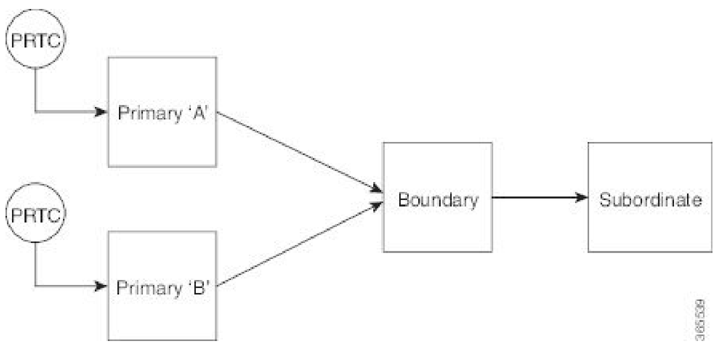
```
Router# show ptp port virtual domain 24
VIRTUAL PORT [vp]
```

```
  Status: down
  Clock Identity: 0x74:A2:E6:FF:FE:5D:CE:3F
  Port Number: 1
  Clock Quality:
    Class: 6
    Accuracy: 0x21
    Offset (log variance): 0x4E5D
  Steps Removed: 0
  Priority1: 128
  Priority2: 128
  Local Priority: 128
  Not-slave: False
```

G.8275.1 Deployment Scenario

The following example illustrates a possible configuration for a G.8275.1 network with two server clocks, a boundary clock and a client. Let's assume that server A is the server clock and B is the backup server clock.

Figure 10: Topology for a Configuration Example



The configuration on server clock A is:

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

The configuration on server clock B is:

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

The configuration on the boundary clock is:

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

The configuration on the client clock is:

```
ptp clock ordinary domain 24 hybrid
```

```
clock-port client-port slave profile g8275.1
  transport Ethernet multicast interface Gig 0/0/0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Interface and Hardware Component commands	Cisco IOS Interface and Hardware Component Command Reference
Clocking and Timing	Clocking and Timing

Standards

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

MIBs

MIB	MIBs Link
—	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.

Feature Information for G.8275.1

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

Note Table 20: Feature Information for G.8275.1 , on page 223 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 20: Feature Information for G.8275.1

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

CHAPTER 16

Configuring the Global Navigation Satellite System

Effective Cisco IOS-XE Release 3.17, the Cisco ASR-920-12SZ-IM router uses a satellite receiver, also called the global navigation satellite system (GNSS), as a new timing interface.

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

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

Overview of the GNSS Module

The GNSS module is present on the front panel of the Cisco ASR-920-12SZ-IM router. The GNSS LED on the front panel indicates the status of the module. The following table explains the different LED status.

LED Status	Description
Off	GNSS is not configured.
Green	GNSS Normal State. Self-survey is complete.
Red	Power up. GNSS is not tracking any satellite.
Amber	Auto holdover.

LED Status	Description
Blinking green	Learning state–normal. Self-survey is not completed.

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

Note The Cisco ASR-920-12SZ-IM router can also receive 1PPS, 10 MHz, and ToD signals from an external clocking and timing source. However, the timing signals from the GNSS module (when enabled) take precedence over those of the external source.

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

Operation of the GNSS Module

The GNSS module has the following stages of acquiring and providing timing signals to the Cisco ASR-920-12SZ-IM router:

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

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

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

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

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

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

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

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

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

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

When the GNSS self-survey is restarted using the default **gnss slot R0/R1** command in config mode, the 10MHz, 1PPS, and ToD signals are not changed and remain up.

Licensing of the GNSS Module

The GNSS is a fixed module on the Cisco ASR-920-12SZ-IM router and requires a license to enable the functionality.

After installing the license, you must enable it by using the **license feature gnss** command.

Note The GNSS module will shut down, if it is in use and the license is disabled.

Prerequisites for GNSS

To use GNSS:

- 1PPS, 10 MHz, and ToD must be configured for netsync and PTP. For more information see the Configuring Clocking and Timing chapter in the *Cisco ASR 920 Series Aggregation Services Router Configuration Guide* .
- License must be enabled on the Cisco ASR-920-12SZ-IM router.
- The antenna must have a clear view of the sky. For proper timing, minimum of four satellites should be locked. For information, see the *Cisco ASR-920-12SZ-IM Aggregation Services Router Hardware Installation Guide* .

Restrictions for GNSS

- The GNSS module is not supported through SNMP; all configurations are performed through commands.
- On HA system, the traps from the standby system are logged to the console as the SNMP infra does not get enabled on standby RSP module.
- GNSS objects or performance counters are updated every 5 seconds locally and acknowledge the MIB object request accordingly.
- GNSS traps generation is delayed for 300 seconds for the first time after system startes to avoid any drop of GNSS traps.

How to Configure the GNSS

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

- Enabling the GNSS License (Required)
- Enabling the GNSS on the Cisco Router (Required)
- Configuring the Satellite Constellation for GNSS (Required)
- Configuring Pulse Polarity and Cable Delay (Required)
- Configuring Cable Delay (Required)
- Disabling Anti-Jam Configuration (Optional)

Enabling the GNSS License

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

Enabling the GNSS on the Cisco Router

```
enable
configure terminal
gnss slot r0
no shutdown
exit
```

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

Configuring the Satellite Constellation for GNSS

```
enable
configure terminal
gnss slot r0
constellation[auto | gps | galelio | beidou | qzss]
exit
```

Configuring Pulse Polarity

```
enable
configure terminal
gnss slot r0
```

```
1pps polarity negative
exit
```

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

Configuring Cable Delay

```
enable
configure terminal
gnss slot r0
1pps offset 5 negative
exit
```

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

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

Disabling Anti-Jam Configuration

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

Verifying the Configuration of the GNSS

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

```
Router# show gnss status
GNSS status:

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

 Authentication: Not checked
  Firmware update progress: NA
  Firmware version: 1.3
```

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

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

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

Router# show gnss satellite 21
Selected Satellite Info:

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

Use the show gnss time and show gnss location to display the time and location of the Cisco ASR-920-12SZ-IM router.

```
Router# show gnss time

Current GNSS Time:

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

Router# show gnss location
Current GNSS Location:

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

Use the **show gnss device** to displays the hardware information of the active GNSS module.

```
Router#show gnss device
GNSS device:

  Serial number: NA
  Firmware version: 0.0
  Firmware update progress: NA
  Authentication: Not applicable
```

Swapping the GNSS Module

Hot swap is supported on the RSP3 module of the GNSS.

1. Remove the standby RSP module.
2. Replace the GNSS module on the standby RSP slot.

3. Reinsert the RSP into the chassis and wait for the RSP to boot with standby ready.
4. Check for GNSS Lock Status of the standby RSP. Use command **show platform hardware slot** *<R0/R1>* [**network-clocks** | **sec GNSS**] to verify.
5. Trigger SSO after the GNSS on standby RSP is locked.
6. Repeat steps 1–3 for the other RSP.

Configuration Example For Configuring GNSS

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

Additional References

Standards

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

MIBs

MIB	MIBs Link
• CISCO-GNSS-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 associated RFCs for this feature.

Feature Information for Configuring the GNSS

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 21: Feature Information for Phrase Based on Module Title

Feature Name	Releases	Feature Information
Configuring GNSS	IOS-XE 3.17	This feature was introduced. The following commands were introduced: • **gnss slot** • **anti-jam disable** • **constellation** • **1pps polarity** • **1pps offset**

CHAPTER 17

Configuring Synchronous Ethernet ESMC and SSM

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

Understanding Synchronous Ethernet ESMC and SSM

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

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

When configured to use synchronous Ethernet, the Cisco ASR 920 Series Router synchronizes to the best available clock source. If no better clock sources are available, the router remains synchronized to the current clock source.

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

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

Clock Selection Modes

The Cisco ASR 920 Series Router supports two clock selection modes, which are described in the following sections.

QL-Enabled Mode

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

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

QL-Disabled Mode

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

- Clock availability
- Priority

> **Note** You can use override the default clock selection using the commands described in Specifying a Clock Source, on page 235 and Disabling a Clock Source, on page 237

Managing Clock Selection

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

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

For more information about how to use these features, see Specifying a Clock Source, on page 235 and Disabling a Clock Source, on page 237.

Restrictions and Usage Guidelines

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

- To use the **network-clock synchronization ssm option** command, ensure that the router configuration does not include the following:
    - Input clock source
    - Network clock quality level
    - Network clock source quality source (synchronous Ethernet interfaces)
- The **network-clock synchronization ssm option** command must be compatible with the **network-clock eec** command in the configuration.
- To use the **network-clock synchronization ssm option** command, ensure that there is not a network clocking configuration applied to sychronous Ethernet interfaces, BITS interfaces, and timing port interfaces.
- SSM and ESMC are SSO-coexistent, but not SSO-compliant. The router goes into hold-over mode during switchover and restarts clock selection when the switchover is complete.
- It is recommended that you do not configure multiple input sources with the same priority as this impacts the TSM (Switching message delay).
- You can configure a maximum of 4 clock sources on interface modules, with a maximum of 2 per interface module. This limitation applies to both synchronous Ethernet and TDM interfaces.

Configuring Synchronous Ethernet ESMC and SSM

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

Specifying a Clock Source

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

Selecting a Specific Clock Source

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

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

Command	Purpose
`network-clock switch manual external R0` `Router# network-clock switch manual external r0 crc4`	Manually selects a synchronization source, provided the source is available and is within the range.
network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]} `Router# network-clock clear switch t0`	Disable a clock source selection.

Forcing a Clock Source Selection

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

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

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

Command	Purpose
`network-clock switch force external R0` `Router# network-clock switch force r0`	Forces the router to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.
network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]} `Router# network-clock clear switch t0`	Disable a clock source selection.

Disabling Clock Source Specification Commands

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

Command	Purpose
network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]} `Router#` **`network-clock clear switch t0`**	Disable a clock source selection.

Disabling a Clock Source

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

Locking Out a Clock Source

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

Command	Purpose
network-clock set lockout {**interface** *interface_name slot/card/port* | **external R0** `Router# network-clock set lockout interface GigabitEthernet 0/0/0`	Prevents the router from selecting a specific synchronous Ethernet clock source.
network-clock clear lockout {**interface** *interface_name slot/card/port* | **external R0** `Router# network-clock clear lockout interface GigabitEthernet 0/0/0`	Disable a lockout configuration on a synchronous Ethernet clock source.

Restoring a Clock Source

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

Command	Purpose
network-clock clear lockout {**interface** *interface_name slot/card/port* | **external external R0** `Router# network-clock clear lockout interface GigabitEthernet 0/0/0`	Forces the router to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.

Verifying the Configuration

You can use the following commands to verify your configuration:

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

- show network-clock synchronization detail—Displays the details of network clock synchronization parameters at the global and interface levels.

Troubleshooting

The table below list the debug commands that are available for troubleshooting the SyncE configuration on the Cisco ASR 920 Series Router:

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

Table 22: SyncE Debug Commands

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

`debug esmc error`
`debug esmc event`
`debug esmc packet [interface <interface name>]`
`debug esmc packet rx [interface <interface name>]`
`debug esmc packet tx [interface <interface name>]`
	Verify whether the ESMC packets are transmitted and received with proper quality-level values.

The table below provides the information about troubleshooting your configuration

Table 23: Troubleshooting Scenarios

Problem	Solution
Clock selection	• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command. • Ensure that the nonrevertive configurations are in place. • Reproduce the issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm commands. Contact Cisco Technical Support if the issue persists.

Problem	Solution
Incorrect QL values	• Ensure that there is no framing mismatch with the SSM option. • Reproduce the issue using the debug network-clock errors and debug network-clock event commands.
Alarms	• Reproduce the issue using the debug platform network-clock command. Alternatively, enable the debug network-clock event and debug network-clock errors commands.
Incorrect clock limit set or queue limit disabled mode	• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command. • Use the **show network-clock synchronization** command to confirm if the system is in revertive mode or nonrevertive mode and verify the non-revertive configurations. • Reproduce the current issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm commands.
Incorrect QL values when you use the **show network-clock synchronization detail** command.	• Use the **network clock synchronization SSM** (*option 1* |*option 2*) command to confirm that there is no framing mismatch. Use the **show run interface** command to validate the framing for a specific interface. For the SSM option 1, framing should be SDH or E1, and for SSM option 2, it should be T1. • Reproduce the issue using the debug network-clock errors and debug network-clock event commands.

Sample Configurations

Input Synchronous Ethernet Clocking

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

```
!
Interface GigabitEthernet0/0
    synchronous mode
    network-clock wait-to-restore 720
!
Interface GigabitEthernet0/1
    synchronous mode
!
!
network-clock synchronization automatic
network-clock input-source 1 External R0 e1 crc4
network-clock input-source 1 gigabitethernet 0/0
network-clock input-source 2 gigabitethernet 0/1
network-clock synchronization mode QL-enabled
```

no network-clock revertive

CHAPTER 18

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.
- The SNMP Dying Gasp trap via FPGA is not supported, when core MPLS interface is routed to the port on the Cisco ASR 920-10SZ-PD, ASR-920-8S4Z-PD, ASR-920-4SZ and ASR-920-12CZ routers in Cisco IOS-XE 16.9.x release.
- The SNMP Dying Gasp is supported on the following routers through FPGA:
    - Cisco ASR-920-24SZ-IM
    - Cisco ASR-920-24SZ-M
    - Cisco ASR-920-24TZ-M

  The maximum number of supported SNMP servers for SNMP Dying Gasp is two. The maximum number of supported Link-OAM Dying Gasp is six. This is applicable to releases starting from Cisco IOS XE 16.9.x release.
- Dying Gasp is not supported on default Mgmt-interface for the following routers:
    - Cisco ASR-920-24SZ-IM
    - Cisco ASR-920-24SZ-M
    - Cisco ASR-920-24TZ-M
    - Cisco ASR 920-10SZ-PD and ASR-920-8S4Z-PD
    - Cisco ASR-920-4SZ
    - Cisco ASR-920-12CZ-A
    - Cisco ASR-920-12CZ-D

  This is applicable to releases starting from Cisco IOS XE 16.9.x release.
- The SNMP Dying GASP for Cisco ASR-920-4SZ-A, Cisco ASR-920-4SZ-D, Cisco ASR-920-12CZ-A, Cisco ASR-920-12CZ-D, and Cisco ASR-920-10SZ-PD routers is not supported for Netflow video template in Cisco IOS-XE 16.9.x release. This is because the routers use different and lower FPGA versions than the supported version (0x00040036 and higher).
- Dying GASP is not supported on the following routers for HW-based SNMP:
    - Cisco ASR-920-12SZ-A
    - Cisco ASR-920-12SZ-D
    - Cisco ASR-920-12SZ-IM

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 19

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 254 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.

Procedure

	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:** `Router(config-controller)# end`	Exits controller configuration mode and returns to privileged EXEC mode.

Using CEM Classes

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

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

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

Procedure

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

	Command or Action	Purpose

	`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`
		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:

Procedure

	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:
	`Router(config-if)# no ip address`
	Example:
	`Router(config-if)# cem 4`
		Defines a CEM group.

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.

Procedure

	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	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.

	Command or Action	Purpose
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 248. 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.

Procedure

	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.

	Command or Action	Purpose
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. • (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** {**mpls** [**manual**]} | **pw-class** *pw-class-name* }[**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}] **Example:**	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.

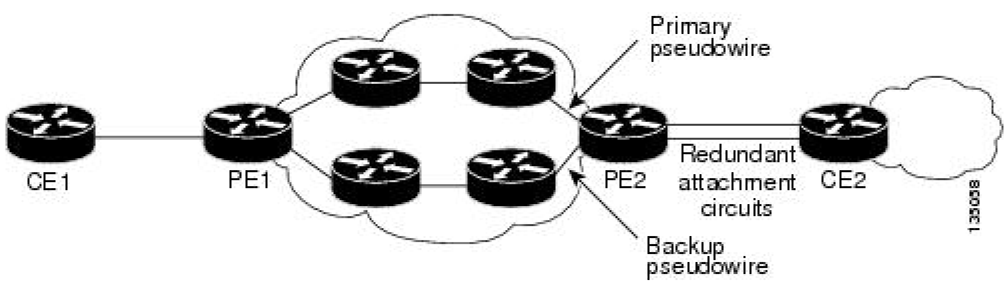
	Command or Action	Purpose
	`Router (config-if-srv)#` **`xconnect 10.1.1.2 101 encapsulation mpls`**	**Note** When creating IP routes for a pseudowire configuration, we recommend that you build a route from the xconnect address (LDP router-id or loopback address) to the next hop IP address, such as **ip 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 11: 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:

Procedure

	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	**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.
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
```

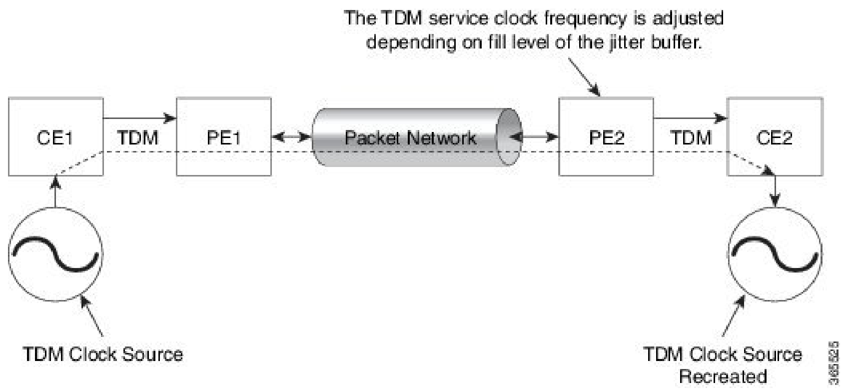
The below configuration example is for BGP PIC with TDM PW:

```
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). ACR is supported on unframed and framed modes of SAToP.

Note Framing type should be maintained same in all routers end to end.



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 and framed 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
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 20

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

Procedure

	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	**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

	Command or Action	Purpose
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]
```

Facility Protocol Status Support

The routers report the protocol status using Syslog or Trap alarm notifications. Few Syslogs and Traps are not cleared when the router gets disconnected or reloaded. As a result, the alarms are not notified.

To avoid this, a new command, **show facility-protocol status**, is introduced that displays the output of the following routing protocols status at any interval of time:

- ISIS
- OSPF
- BGP
- TE Tunnels
- LDP
- Bundles
- PWs
- EVPN PWs
- CFM
- SYncE
- PTP
- HSRP
- BFD
- SensorThresholdViolations

show facility protocol status

The **show facility-protocol status** command helps to backup the protocols syslog information by capturing the current status of the protocols on the system.

Also, when you add a new device, the command can be used to generate a list of the outstanding protocol alarms from the device.

Restrictions

Only 14 routing protocols outputs can be displayed.

Routing Protocols Outputs

The following are the outputs of different routing protocols:

OSPF Output

```
#show facility-protocol status
=========================================================================================
Protocols   Pid  Ver  Interface                  IP-address       Status         Adj-ID
      Router-ID
=========================================================================================
OSPF       22    V2   TenGigabitEthernet0/3/4   10.0.1.2         FULL           21.22.23.25
      15.88.15.89
OSPF       100   V2   FortyGigabitEthernet0/8/1 192.168.1.1       DOWN           N/A
       100.100.100.100
```

MPLS Output

```
#show facility-protocol status
==========================================================================================
Protocols          Name    Interface                  Src-IP         LDP_Neigh_IP     Status
==========================================================================================
MPLS-LDP           LDP     TenGigabitEthernet0/3/4    10.0.1.2         N/A              DOWN

MPLS-LDP           LDP     FortyGigabitEthernet0/8/1 192.168.1.1      N/A              DOWN

MPLS-LDP           LDP     GigabitEthernet0/2/0      22.1.4.1         7.7.7.7:0        UP

MPLS-LDP           LDP     GigabitEthernet0/2/4      22.0.1.1         6.6.6.6:0        UP

MPLS-LDP           LDP     Tunnel2001                5.5.5.5          2.2.2.2:0        DOWN

MPLS-LDP           LDP     Tunnel2002                5.5.5.5          2.2.2.2:0        DOWN

MPLS-LDP           LDP     Tunnel2003                5.5.5.5          2.2.2.2:0        DOWN

MPLS-LDP           LDP     Tunnel2004                5.5.5.5          2.2.2.2:0        DOWN

MPLS-LDP           LDP     Tunnel2005                5.5.5.5          2.2.2.2:0        DOWN

MPLS-LDP           LDP     Tunnel2006                5.5.5.5          2.2.2.2:0        DOWN

MPLS-LDP           LDP     Tunnel2007                5.5.5.5          2.2.2.2:0        DOWN

MPLS-LDP           LDP     Tunnel2008                5.5.5.5          2.2.2.2:0        DOWN

MPLS-LDP           LDP     Tunnel2009                5.5.5.5          2.2.2.2:0        DOWN
```

ISIS Output

```
#show facility-protocol status
==========================================================================================
Protocols      Interface       ISIS-Type         Neigh-IP        Net-ID            Status
     Sys-ID            Hold-Time
==========================================================================================
ISIS   HundredGigE0/7/0           Level-1       NA              NA                DOWN
      NA                    NA
ISIS   HundredGigE0/7/0           Level-2       NA              NA                DOWN
      NA                    NA
ISIS   GigabitEthernet0/3/4       Level-2       10.147.158.2    0000.0000.0158    UP
      NCS4206-158           26
ISIS   BDI72                      Level-2       10.10.72.2      0000.0000.0162    UP
      NCS4K-101-162         29
ISIS   BDI27                      Level-2       10.10.27.2      0000.0000.0162    UP
      NCS4K-101-162         23
ISIS   GigabitEthernet0/0/7       Level-2       NA              NA                UP
      0000.0000.0152        250
ISIS   TenGigabitEthernet0/3/0    Level-2       38.206.1.3      0000.0000.0023    UP
      C101_A                28
ISIS   GigabitEthernet0/2/3       Level-2       38.76.1.3       0000.0000.0007    UP
      ASR9K_CORE            23
ISIS   Tunnel1315                 Level-2       7.7.15.2        0000.0000.0007    UP
      ASR9K_CORE            28
```

BGP Output

```
#show facility-protocol status
==========================================================================================
Protocols  LocalAS   RemoteAS  NeighborIP              Status        Up/Down Time
Remote-RID   VRF-Inst-Name
==========================================================================================
```

```
BGP          123         123         21.22.23.25          DOWN            never
0.0.0.0      NA
BGP          123         123         66.66.66.23          DOWN            never
0.0.0.0      CustomerA
BGP          500         500         1.1.1.158            DOWN            never
0.0.0.0      NA
BGP          500         100         10.147.158.2         DOWN            1
0.0.0.0      SENTHIL
BGP          500                                          DOWN            1
0.0.0.0
```

Pseudowire Output

```
#show facility-protocol status
==========================================================================================
Protocols      Peer-IP              VC-ID        VC-Status       VC-Error
==========================================================================================
PWs            1.1.1.146            2            ADMIN DOWN      NA
PWs            1.1.1.146            9            ADMIN DOWN      NA
PWs            1.1.1.146            10           ADMIN DOWN      NA
PWs            1.1.1.146            54           DOWN            NA
PWs            1.1.1.146            87           DOWN            NA
PWs            1.1.1.146            98           DOWN            NA
```

SYncE Output

```
#show facility-protocol status
==========================================================================================
Protocols   Interface                Mode/QL    QL-IN       QL-Rx-Config   QL-Rx-Overrided

==========================================================================================
SyncE    GigabitEthernet0/1/7        Sync/En    QL-DNU       -                 QL-DNU
SyncE                                Sync/En    QL-DNU       -                 QL-DNU
SyncE                                Sync/En    QL-DNU       -                 QL-DNU
SyncE                                Sync/En    QL-DNU       -                 QL-DNU
```

Bundles Output

```
#show facility-protocol status
==========================================================================================
Protocols          Port-Channel          Bundle-Status       Bundled-Ports       Min-Bundle
==========================================================================================
BUNDLES            Po48                    DOWN                0                   2
```

PTP Output

```
#show facility-protocol status
==========================================================================================
Protocols  Event                Interface              Role     Clock-port-Name    State
       Master-IP
==========================================================================================
PTP CLK_MASTER_PORT_SELECTED   NA                     slave     tomaster            NA
         UNKNOWN

PTP CLK_STATUS_UPDATE     Loopback1588                slave     NA              FREERUN
         NA

PTP CLK_MASTER_PORT_SELECTED   NA                     slave     slave               NA
         21.21.21.21

PTP CLK_STATUS_UPDATE     Loopback0                   slave     NA              ACQUIRING
         NA
```

HSRP Output

```
#show facility-protocol status
=======================================================
Protocols  Interface                 Group       State
========================================================
HSRP      HundredGigE0/7/0            1           Init
```

TE Tunnels Output

```
#show facility-protocol status
==========================================================================================
Protocols          Tunnel-Interface           Status
==========================================================================================
MPLS-TE            Tunnel0                    DOWN
MPLS-TE            Tunnel1                    DOWN
```

BFD Output

```
#show facility-protocol status
==========================================================================================
Protocols    Interface                Status           Neigh-Addr      Local-Descriminator
  Interface_index
==========================================================================================
BFD          FortyGigabitEthernet0/8/1   DOWN            NA                  NA
       22
BFD          TenGigabitEthernet0/3/0     DOWN            NA                  NA
       9
BFD          GigabitEthernet0/5/4        DOWN            NA                  NA
       15
BFD          Tunnel1309                  DOWN            NA                  NA
       1601
```

CFM Output

```
#show facility-protocol status
==========================================================================================
Protocols Event          Interface                L-mpid Level Dir BD/VLAN/XCON  ID
Defect-Condition
==========================================================================================
CFM    ENTER_AIS_INT    GigabitEthernet0/0/4     NA     NA    Up   NA           NA  AIS

CFM    ENTER_AIS        GigabitEthernet0/0/4     2      4     Up   XCON         NA  AIS

CFM    ENTER_AIS_INT    GigabitEthernet0/3/6     NA     NA    Up   NA           NA  AIS

CFM    ENTER_AIS        GigabitEthernet0/3/6     2      4     Up   XCON         NA  AIS

==========================================================================================
Protocols Event           R-mpid Level EVC-NAME MA-NAME  Domain  MAC     Status Event-Code
==========================================================================================
CFM    REMOTE_MEP_DOWN         1    NA    SEN_CFM  SEN_CFM  EVC      NA        UP   NA
CFM    REMOTE_MEP_UP           1    NA    SEN_CFM  SEN_CFM  EVC      NA        UP   NA
CFM    CROSSCHECK_MEP_UNKNOWN  1    NA    NA       SEN_CFM  EVC 0022.bdde.05be NA   NA
CFM    CROSS_CONN_SERVICE      1    4     NA       SEN_CFM  EVC 0022.bdde.05be NA   NA
CFM    CONFIG_ERROR            1    NA    NA       SEN_CFM  EVC 0022.bdde.05be NA   NA
```

EVPN PWs Output

```
#show facility-protocol status
==========================================================================================
Protocols          EVPN-ID       Source       Target       Status
==========================================================================================
```

```
EVPN-PWs             100           41           30           DOWN
```

Sensory Threshold Violations

```
#show facility-protocol status
==========================================================================================
Protocols PhylIndex SenValue SenType SenScale SenPrecision ThresIndex SenThrValue PhyEntryName
==========================================================================================
SENSOR_THRESH 1211 -103 14 9 1 1 -120 subslot 0/2 transceiver 0 Rx Power Sensor

SENSOR_THRESH 1211 -103 14 9 1 2 -140 subslot 0/2 transceiver 0 Rx Power Sensor

SENSOR_THRESH 1253 -400 14 9 1 3 -310 subslot 0/2 transceiver 3 Rx Power Sensor

SENSOR_THRESH 1253 -400 14 9 1 4 -330 subslot 0/2 transceiver 3 Rx Power Sensor

SENSOR_THRESH 1267 -370 14 9 1 3 -296 subslot 0/2 transceiver 4 Rx Power Sensor

SENSOR_THRESH 1267 -370 14 9 1 4 -310 subslot 0/2 transceiver 4 Rx Power Sensor

SENSOR_THRESH 2001 73 6 9 0 1 0 subslot 0/4 power Sensor 0
```

show facility-protocol status command

To backup the protocols syslog information by capturing the current status of the protocols on the system, use the **show facility-protocol status** command.

Syntax Description

Syntax Description:

There are no keywords.

Command Default

There is no default.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.x	Support for this command was introduced on ASR 900, ASR 920, and NCS 4200 Series.

Examples

```
Router# show facility-protocol status
==========================================================================================
Protocols      Peer-IP               VC-ID        VC-Status       VC-Error
==========================================================================================
PWs            1.1.1.146             2            ADMIN DOWN      NA
PWs            1.1.1.146             9            ADMIN DOWN      NA
PWs            1.1.1.146             10           ADMIN DOWN      NA
PWs            1.1.1.146             54           DOWN            NA
PWs            1.1.1.146             87           DOWN            NA
PWs            1.1.1.146             98           DOWN            NA
```

CHAPTER 21

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 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 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 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 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 284 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 24: 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 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 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 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 router, or for all modules within a process on the 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
```