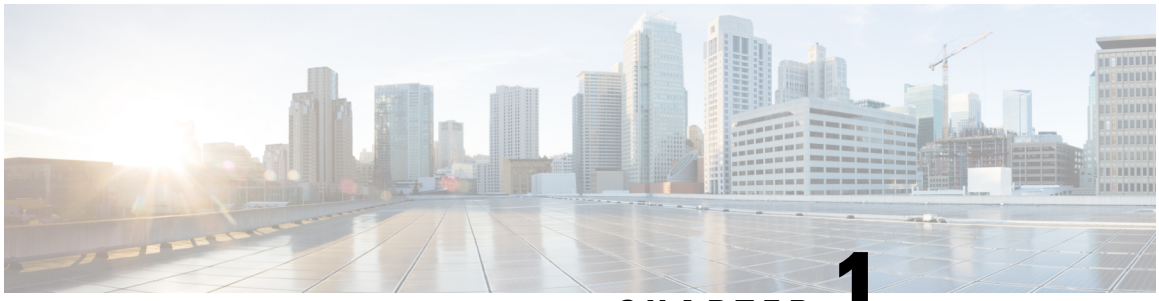
Cisco NCS 520 Series Router Configuration Guide, Cisco IOS XE 16

First Published: 2018-05-04

Last Modified: 2020-05-29

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

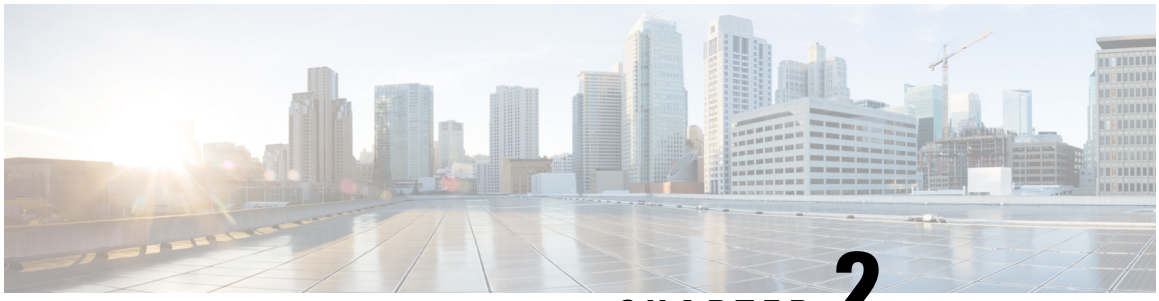


CHAPTER 1

Feature History

The following table lists the new and modified features that are supported in the Cisco NCS 520 Series Router Configuration Guide in Cisco IOS XE 16 releases.

Feature Name	Cisco IOS XE Release
HSRP/VRRP Support	16.12.1
IGMP Snooping	16.12.1
PVST+/RPVST+	16.12.1
Resilient Ethernet Protocol	16.11.1
Y.1564 Support	16.11.1
TWAMP Responder	16.11.1
IPv4 Routing	16.10.1
Switch Port Analyzer	16.10.1
YANG Data Models	16.10.1
Support for Flex Links	16.9.1



CHAPTER 2

Getting Started With the Cisco NCS 520 Series Router

This chapter covers the following topics:

Overview

Cisco NCS 520 family of routers include:

PID	Short Description	Front Panel Ports
N520-4G4Z-A	Base NID, AC Power	2X1GE SFP +2X1GE Cu+ 4X1/10 GE SFP+
N520-X-4G4Z-A	Premium NID, AC Power	
N520-X-4G4Z-D	Premium NID, DC Power(Dual Power supply)	
N520-20G4Z-A	Base Switch/Router, AC Power	16X1GE SFP + 4X1 GE Cu + 4X1/10 GE SFP+ All variants have dual PSU.
N520-20G4Z-D	Base Switch/Router, DC Power	
N520-X-20G4Z-A	Premium Switch/Router, AC Power	
N520-X-20G4Z-D	Premium Switch/Router, DC Power	

In addition to the 1G/10G interfaces, the Cisco NCS 520 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 console port with RJ45 connector
- Time of Day (ToD) port with RS422 interface
- 1PPS port SMA port
- 10M port SMA port

- External Alarm interface with 4 Dry Contact Alarm inputs
- ZTP button for Zero Touch Provisioning

Caution A short press of the ZTP button starts the provisioning of the router. Pressing this button for more than 8 seconds causes the router to reboot.

- Various LEDs for system and interface status

Table 1: Feature Comparison for Cisco NCS 520 Series Routers

Feature or Functionality	N520-4G4Z-A	N520-X-4G4Z-A	N520-X-4G4Z-D	N520-20G4Z-A	N520-20G4Z-D	N520-X-20G4Z-A	N520-X-20G4Z-D
CPU operating at	1 GHz	1 GHz	1 GHz	1 GHz	1 GHz	1 GHz	1 GHz
DRAM	4GB	4GB	4GB	4GB	4GB	4GB	4GB
SD Flash	4GB eMMC	4GB eMMC	4GB eMMC	4GB eMMC	4GB eMMC	4GB eMMC	4GB eMMC
1G-10G Dual Rate Ports	4	4	4	4	4	4	4
Time of Day port	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Auto Media Sel Combo Port	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Copper Ports	2	2	2	4	4	4	4
SFP Ports	2	2	2	16	16	16	16
Smart SFP	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
SFP+ Ports	4	4	4	4	4	4	4
Copper SFP	Supported	Supported	Supported	Supported	Supported	Supported	Supported
XFP Ports	NA	NA	NA	NA	NA	NA	NA
ZTP Button	Supported	Supported	Supported	Supported	Supported	Supported	Supported
PoE	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

Feature or Functionality	N520-4G4Z-A	N520-X-4G4Z-A	N520-X-4G4Z-D	N520-20G4Z-A	N520-20G4Z-D	N520-X-20G4Z-A	N520-X-20G4Z-D
GNSS	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

Restrictions

- The Cisco NCS 520 Series Routers do not support the **hw-module** *slot/subslot* **reload** command.
- Duplicate Address Detection (DAD) is not supported.
- 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.
- Specific License Reservation (SLR) is not supported on Cisco ASR 920 routers.

Interface Naming

The following table shows the interface naming of the N520-4G4Z-A/ N520-X-4G4Z-A/ N520-X-4G4Z-D Cisco ports: Ports 2, 3, 4, and 5 when operating in 1G Mode become operationally up only when the peer connecting interfaces are in Auto negotiation mode.

- Interfaces 0–1 are Copper only ports with RJ45 connector.

1G Cu	1G SFP	10G SFP+/1G SFP	
1	3	5	7
0	2	4	6

- Interfaces 2 and 3 are GigabitEthernet SFP only ports.
- Interfaces 0 through 3 are referred to as GigabitEthernet 0/0/0 and GigabitEthernet 0/0/3, respectively.
- Interfaces 4 to 7 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 NCS 520 Series Aggregation Services Router Hardware Installation Guide*.

- Interfaces 4 to 7 are named as TenGigibitEthernet 0/0/4 and TenGigabitEthernet 0/0/7, 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 N520-20G4Z-A / N520-20G4Z-D / N520-X-20G4Z-A / N520-X-20G4Z-D Cisco ports: Ports 2, 3, 4, and 5 when operating in 1G Mode will become operationally up only when the peer connecting interfaces are in Auto negotiation mode.

- Interfaces 0–3 are Copper only ports with RJ45 connector.

1G Cu		1G SFP								10G SFP+/1G SFP	
1	3	5	7	9	11	13	15	17	19	21	23
0	2	4	6	8	10	12	14	16	18	20	22

- Interfaces 4–19 are GigabitEthernet SFP only ports.
- Interfaces 0 to 19 are referred to as GigabitEthernet 0/0/0 and GigabitEthernet 0/0/19, respectively.
- Interfaces 20 to 23 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 NCS 520 Series Aggregation Services Router Hardware Installation Guide* .

- Interfaces 4 to 7 are named as TenGigibitEthernet 0/0/20 and TenGigabitEthernet 0/0/23, 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.

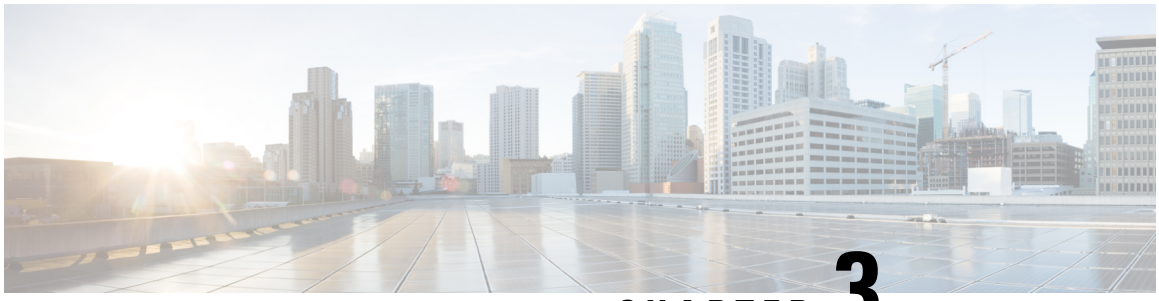
Interface Speed Based on Port Type

	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	Yes	Yes	Yes	Yes	Yes	NA
10G Dual rate ports	NA	NA	NA	NA	Not Supported	Yes	Not Supported	Not Supported	Yes	Yes

Interface Limitations

- Copper ports can work with 1Gbps speed only if auto negotiation is enabled. 10 or 100Mbps can work with both auto negotiation enabled or disabled mode.
- 10G ports cannot operate in 100Mbps speed. 100BASE SFPs are not supported on 10G ports; however, there is no such limitation on 1G ports.

- There are no LEDs to indicate current working speed of the interface. However, duplex LEDs are available only on Copper ports



CHAPTER 3

Using Cisco IOS XE Software

This chapter provides information to prepare you to configure the Cisco NCS 520 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 *Cisco NCS 520 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[1]	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

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

Using the History Buffer to Recall Commands

The history buffer stores the last 10 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[2]	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.

Command	Purpose
`Router# show history`	While in EXEC mode, list the last several commands you have just entered.

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

Getting Help

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

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

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

`Router(config-if)# ?`
`Interface configuration commands:`
`.`
`.`
`.`
`ip Interface Internet Protocol config commands`
`keepalive Enable keepalive`
`lan-name LAN Name command`
`llc2 LLC2 Interface Subcommands`
`load-interval Specify interval for load calculation for an interface`
`locaddr-priority Assign a priority group`
`logging Configure logging for interface`
`loopback Configure internal loopback on an interface`
`mac-address Manually set interface MAC address`
`mls mls router sub/interface commands`
`mpoa MPOA interface configuration commands`
`mtu Set the interface Maximum Transmission Unit (MTU)`
`netbios Use a defined NETBIOS access list or enable`
`name-caching`
`no Negate a command or set its defaults`
`nrzi-encoding Enable use of NRZI encoding`
`ntp Configure NTP`
`.`
`.`
`.`
`Router(config-if)#`
	Enter **?** to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.

`Router(config-if))#service ?` `instance Configure Ether Service Instance`	Enter the command to configure ether service instance. Enter **?** to display what you must enter next on the command line.

Command	Comment

`Router(config-if)# service instance ?`
`  <1-4000>  Service Instance Identifier`
`  trunk     Trunk Service Instance`
	Enter the command to configure the service instance. The value of service instance identifier ranges from 1 to 4000.

`Router(config-if)# service instance 1 ?` `  ethernet  Configure an Ethernet Instance`	Enter the command to configure an ethernet instance. Enter **?** to display what you must enter next on the command line.
`Router(config-if)# service instance 1 ethernet` `Router(config-if-srv)#`	Enter the command to display service ethernet instance configuration.
`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 a TFTP Server

```
Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_ncs520-confg]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)
```

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

Filtering Output from the show and more Commands

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

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

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

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

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is up, line protocol is up
GigabitEthernet0/0/1 is up, line protocol is up
GigabitEthernet0/0/2 is up, line protocol is up
TenGigabitEthernet0/0/5 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.

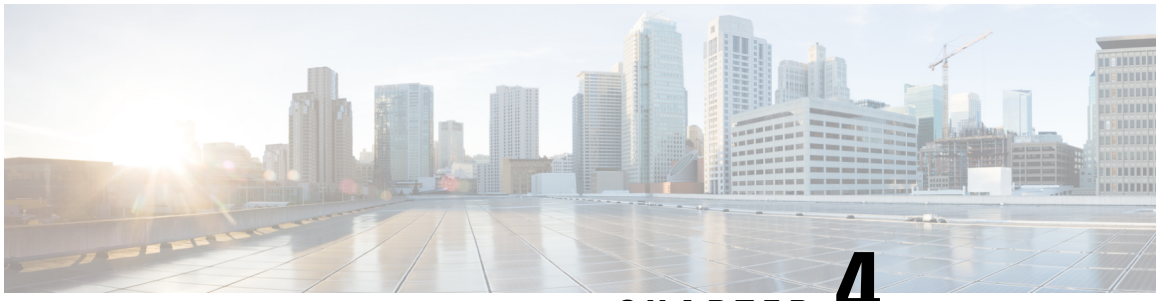
You must be a registered user on Cisco.com to access this tool.

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 4

Using Zero Touch Provisioning

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 interface connected to the CCE must be turned green.
- DHCP server should be configured to ensure reachability to the CCE and the TFTP server.
- It is highly recommended to use free ports that do not need a license to enable, to reach the DHCP and TFTP servers during ZTP. Effective Cisco IOS XE Amsterdam 17.3.1 onwards, the 10G ports are considered as free during ZTP. For more information on port licensing, see Licensing 1G and 10G Ports on the Cisco NCS 520 Series Router.

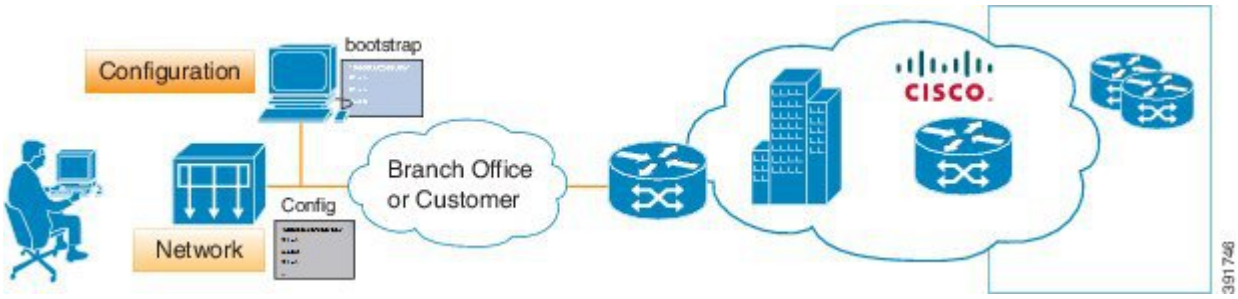
Caution Do not change the ROMMON configuration register to 0x0.

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 also not initialized when the router is already reloading or if the router is in ROMMON prompt.
- ZTP is not initialized if bootflash has files named as 'router-confg'.

Information About Using ZTP

Figure 1: Sample ZTP Topology



On the Cisco NCS 520 Series Routers, ZTP is triggered under any of the following conditions:

- A router without a start up configuration is powered on
- The ZTP button in the front panel is pressed for less than 8 seconds.
- The **write erase** and **reload** commands are executed.

Note The Cisco NCS 520 Series Routers have a ZTP button on the front panel.

Note When **write erase** and **reload** commands are executed and if **Yes** or **No** is requested to save running configuration before reload and 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. Effective Cisco IOS XE 17.3.1 onwards, the router will initiate the DHCP session over untagged interface as soon as the ZTP process is started. If a DHCP session is successfully established, then the below two steps are not relevant.
2. The router detects the management VLAN by listening to any of the following data packets:
   - Broadcast (Gratuitous ARP)
   - ISIS hello packets
   - OSPF hello packets
   - IPv6 router advertisement packets
   - VRRP

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

3. The router willl wait for a certain interval of time to learn all the possible VLAN configurations and try to initiate a DHCP session to a DHCP server over the learned VLANs
4. When connectivity to CCE is established, the bootup process is managed through the CCE engine by means of template configuration or manual intervention from the operations center.

When the ZTP process initiates, the Cisco NCS 520 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 CCE. 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 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

Downloading the Initial Configuration

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

1. The router sends DHCP discover requests on each Ethernet interface. The serial number of the router is used as a client identifier.
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: DOM-<mac-address>, network-confg, router-confg, ciscortr.cfg, or cisconet.cfg.

Note Ensure to use hyphenated hexadecimal notation of MAC address (DOM-78-72-5D-00-A5-80) to name the files.

Effective Cisco IOS XE Amsterdam 17.3.2a, the router tries to learn the reachability to multiple DHCP servers during ZTP. Hence multiple DHCP discovery messages are sent out during this phase. The router goes through all the DHCP offer messages received and selects an appropriate DHCP server based on the priority decided based on below rules:

1. The DHCP server reachable via untagged interface have higher priority than the one via tagged. In case of tagged, the one reachable via an interface learned using VRRP packets has higher priority.
2. If multiple DHCP servers are reachable via similar interfaces mentioned in previous rule, the one reachable via higher physical port number has higher priority.

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
```

Cisco Configuration Engine Server

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

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

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

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

ZTP LED Behavior

On Cisco NCS 520 Series Routers, when ZTP button is pressed:

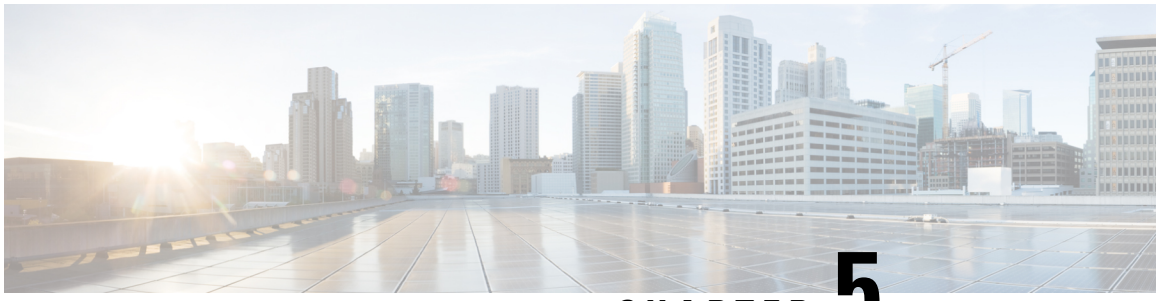
Process	ZTP LED Status
Press ZTP button	Blinking Amber
Loading image	Off
ZTP process running	Blinking Amber
ZTP success	Green
ZTP failure	Red

Verifying the CNS Configuration

Use the following commands to verify the CNS configuration:

On the Cisco NCS 520 Series Router:

- **show cns event connection**
- **show cns image connection**
- **show cns config stats**



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 NCS 520 Hardware Installation Guide*.

Connecting Console Cables

For information about connecting console cables to the Cisco NCS 520 Series Router, see the *NCS 520 Series 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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
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.
		• *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:**	Applies the settings defined in the transport map to the console interface.

	Command or Action	Purpose
	`Router(config)# transport type console 0 input consolehandler`	The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type persistent telnet** *transport-map-name* **Example:**	Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode.

	Command or Action	Purpose
	`Router(config)# transport-map type persistent telnet telnethandler`	
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.
		• **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

	Command or Action	Purpose
		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
```

Configuring Persistent SSH

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

Procedure

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type persistent ssh** *transport-map-name* **Example:** `Router(config)# transport-map type persistent ssh sshhandler`	Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** {**interruptible**} | **none** {**disconnect**}] **Example:** `Router(config-tmap)# connection wait allow interruptible`	Specifies how a persistent SSH connection will be handled using this transport map: • **allow**—The SSH connection waits for the vty line to become available, and exits the router if interrupted. • **allow interruptible**—The SSH connection waits for the vty line to become available, and also allows users to enter diagnostic mode by interrupting a SSH connection waiting for the vty line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The SSH connection immediately enters diagnostic mode. • **none disconnect**—The SSH connection does not wait for the vty line from IOS and does not enter diagnostic mode, so all SSH connections are rejected if no vty line is immediately available.
Step 5	**rsa keypair-name** *rsa-keypair-name* **Example:** `Router(config-tmap)# rsa keypair-name sshkeys`	Names the RSA keypair to be used for persistent SSH connections. For persistent SSH connections, the RSA keypair name must be defined using this command in transport map configuration mode. The RSA keypair definitions defined elsewhere on the router, such as through the use of the **ip ssh rsa keypair-name** command, do not apply to persistent SSH connections.

	Command or Action	Purpose
		No *rsa-keypair-name* is defined by default.
Step 6	authentication-retries number-of-retries **Example:** `Router(config-tmap)# authentication-retries 4`	(Optional) Specifies the number of authentication retries before dropping the connection. The default *number-of-retries* is 3.

Step 7	banner [diagnostic | wait] banner-message
	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 vty line as a result of the persistent SSH configuration.
		• **diagnostic**—Creates a banner message seen by users directed into diagnostic mode as a result of the persistent SSH configuration.
		• **wait**—Creates a banner message seen by users waiting for the vty line to become active.
		• *banner-message*—The banner message, which begins and ends with the same delimiting character.

Step 8	time-out timeout-interval **Example:** `Router(config-tmap)# time-out 30`	(Optional) Specifies the SSH time-out interval in seconds. The default *timeout-interval* is 120 seconds.
Step 9	**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 SSH can only be applied to the Management Ethernet interface on the router.
Step 10	exit **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 11	transport type persistent ssh input *transport-map-name* **Example:** **Example:** `Router(config)# transport type persistent ssh input sshhandler`	Applies the settings defined in the transport map to the Management Ethernet interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type persistent ssh** command .

Examples

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

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

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

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

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

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

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1

Router(config-tmap)# banner diagnostic X

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

--Welcome to Diagnostic Mode--

X

Router(config-tmap)#banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for vty line--
X
Router(config-tmap)#
time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
```

Viewing Console Port, SSH, and Telnet Handling Configurations

Use the **show transport-map all name** *transport-map-name* | **type console 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 :
```

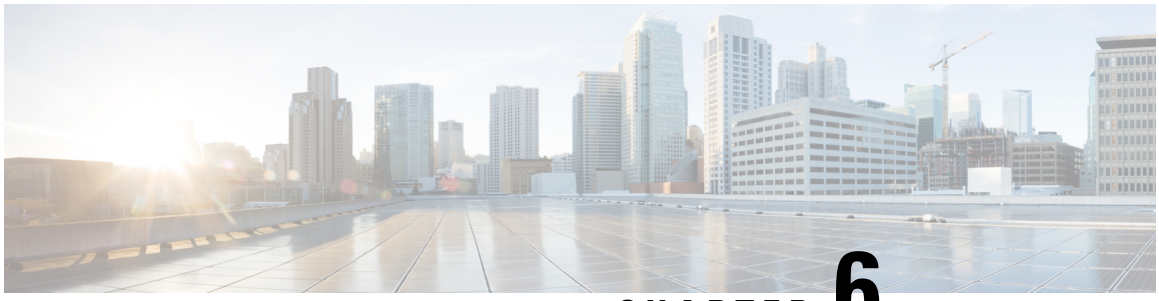
The **show platform software configuration access policy** output is given both before the new transport map is enabled and after the transport map is enabled so the changes to the SSH configuration are illustrated in the output.

```
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 NCS 520 Series Router has one Gigabit Ethernet Management Ethernet interface .

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 38.

BDI interfaces can be used as managment interface. For more information on the configuration of BDI interface, refer the *Ethernet Virtual Connections Configuration* section in *Carrier Ethernet Configuration Guide*.

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 (Gi0) 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 : 295 bytes
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address x.xx.x.xx xxx.xxx.x.x
 speed 100
 no negotiation auto
!
ip route vrf Mgmt-intf x.x.x.x x.x.x.x x.xx.x.x
!
end

Router#
```

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
```

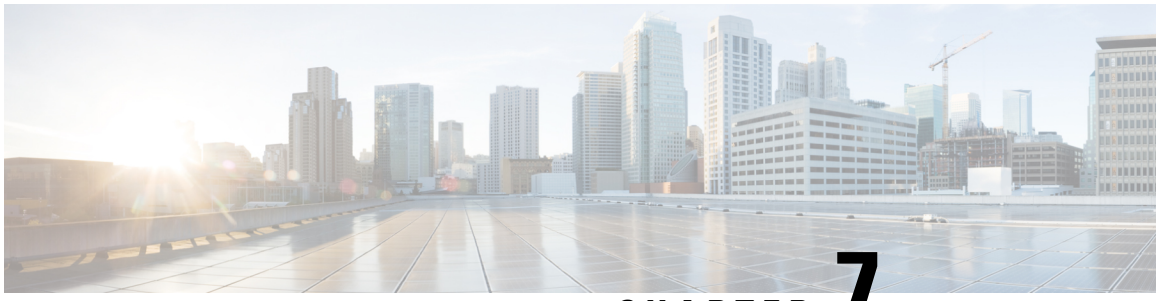
Tacacs+ Server Group Example

```
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

Installing and Upgrading Software

This chapter describes how to update software on the Cisco NCS 520 Series Router.

Upgrading Field Programmable Hardware Devices

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 the router.

File Systems on the Cisco NCS 520 Series Router

The table below provides a list of file systems that can be seen on the Cisco NCS 520 Series Router.

Table 6: 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.
system:	The system memory file system, which includes the running configuration.
tmpsys:	The temporary system files file system.

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.

System Requirements

The following sections describe the system requirements for the Cisco NCS 520 Series Router software:

Memory Recommendations

These are the recommendation for the router images and packages:

- Image size—350 MB
- DRAM memory—4 GB
- Software Image—ncs520-universalk9_npe.BLD_V168_1_THROTTLE_<>.bin

ROMmon Version Requirements

ROMmon Release 1.0 (FAI) is the recommended release for all ROMmon upgradeable components. For more information about ROMmon images, see Release Notes.

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 terminates.

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.

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 7: 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.

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# ncs520-universalk9_npe.BLD_V168_1_THROTTLE_<>.bin:
```

- 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 =  ncs520-universalk9_npe.BLD_V168_1_THROTTLE_<>.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

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:

- Copy the latest ROMMON package into bootlfash.

  ```
  Router# copy tftp://192.168.0.100/FPGA_ROMMON_PKG/ncs520dominica-rommon_0_11.SSA.pkg
  bootflash:
  ```

- Use the following command to upgrade the ROMMON:

  ```
  Router# upgrade rom-monitor filename bootflash:<pkg> all
  ```

- Reload the router for the ROMMON to take effect.

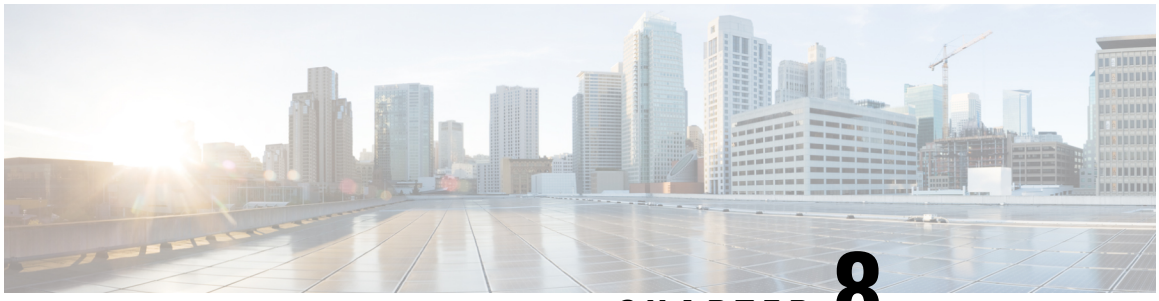
Software Upgrade Example

The following section provide a sample of software upgrade on the router.

```
Router# show bootvar
BOOT variable = bootflash:ncs520-universalk9_npe.BLD_V168_1_THROTTLE_<>.bin;
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]
System Bootstrap, Version 15.4(3r)S4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Boot ROM1
Last reset cause: RSP-Board
UEA platform with 2097152 Kbytes of main memory
Located ncs520-universalk9_npe.BLD_V168_1_THROTTLE_<>.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-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.
(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
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
uptime is 21 minutes
Uptime for this control processor is 25 minutes
System returned to ROM by reload
System image file is "bootflash:ncs520-universalk9_npe.BLD_V168_1_THROTTLE_<>.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
(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 8

Configuring Ethernet Interfaces

This chapter provides information about configuring the Gigabit Ethernet interface on the Cisco NCS 520 Series Router.

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

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 52.

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)# **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 8 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
```

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.

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.

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

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.

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 Gi0/0/0** command.

The following example provides sample output for interface port 0 on the interface located in slot 0 of the router:

```
Router# show interface Gi0/0/0
Gi0/0/0 is up, line protocol is up
Hardware is 8xGE-4x10GE-FIXED, address is 6073.5cff.8087 (bia 6073.5cff.8087)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full Duplex, 1000Mbps, link type is auto, media type is RJ45
output flow-control is off, input flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

Verifying Interface Status

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

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

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

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

Command	Purpose
`Router# show hw-module slot/subslot transceiver port idprom status`	Displays information for the transceiver initialization status. **Note** The transmit and receive optical power that is displayed by this command is useful for troubleshooting Digital Optical Monitoring (DOM). For interfaces to become active, optical power must be within required thresholds.
`Router# show hw-module slot/subslot transceiver port idprom dump`	Displays a dump of all EEPROM content that is stored in the transceiver.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuration Examples

This section includes the following configuration examples:

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.
```

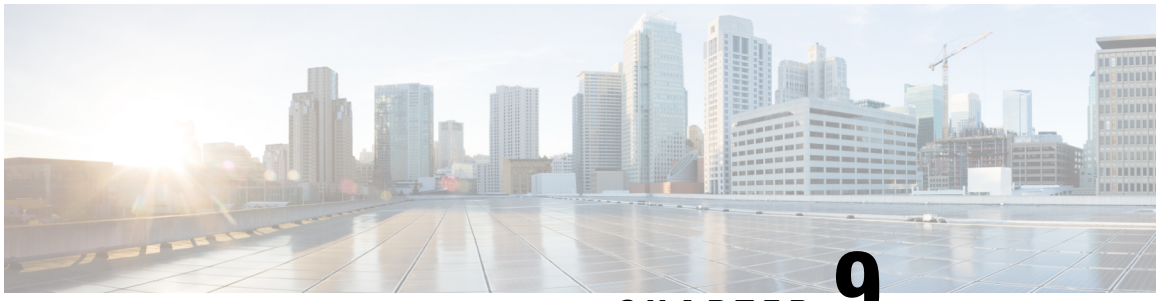
```
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 0/0/1
!
! Configure the interface MTU.
!
Router(config-if)# mtu 9216
```

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 9

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

- 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.

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
```

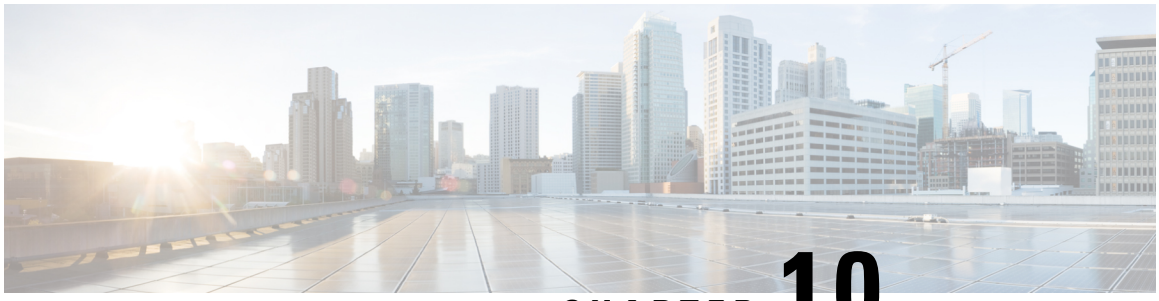
Message Displayed on the Peer Router on Receiving Dying Gasp Notification

```
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 10

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.

Restriction

External Alarms are *not* supported.

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 Routers

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: 3  Major: 0  Minor: 0

Source                    Time                    Severity      Description [Index]
------                    ------                  --------      -------------------
GigabitEthernet0/0/0      Mar 29 2018 00:24:22    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3      Mar 29 2018 00:24:40    CRITICAL      Physical Port Link Down [1]
xcvr container 0/0/4      Mar 29 2018 00:24:20    CRITICAL      Transceiver Missing - Link
 Down [1]
```

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:

```
Chassis type: N520-X-4G4Z-A

Slot: 0, N520-X-4G4Z-A
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:56 (12:37:07 ago)
  Software declared up time   : 00:01:54 (12:36:09 ago)
  CPLD version                : 00030016
  Firmware version            : 0.14(20180301:104121) [ncs520-dev 20572+]

Sub-slot: 0/0, 4xGE-4x10GE-FIXED
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:03:39 (12:34:24 ago)
  Logical insert detect time  : 00:03:39 (12:34:24 ago)

Slot: R0, N520-X-4G4Z-A
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:56 (12:37:07 ago)
  Software declared up time   : 00:00:56 (12:37:07 ago)
  CPLD version                : 00030016
  Firmware version            : 0.14(20180301:104121) [ncs520-dev 20572+]
```

```
Slot: F0,
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:56 (12:37:07 ago)
  Software declared up time   : 00:01:48 (12:36:15 ago)
  Hardware ready signal time  : 00:00:00 (never ago)
  Packet ready signal time    : 00:01:38 (12:36:25 ago)
  CPLD version                : 00030016
  Firmware version            : 0.14(20180301:104121) [ncs520-dev 20572+]

Slot: P0, NCS520-PSU0
  State                       : ok
  Physical insert detect time : 00:00:00 (never ago)

Slot: P1, NA
  State                       : ok
  Physical insert detect time : 00:00:00 (never ago)

Slot: P2, NCS520-FAN
  State                       : ok
  Physical insert detect time : 00:00:00 (never 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.

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:

```
Router# enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# logging alarm 2
Router(config)# exit


Router#show facility-alarm status
System Totals  Critical: 3  Major: 0  Minor: 0

Source                    Time                   Severity      Description [Index]
------                    ------                 --------      -------------------
GigabitEthernet0/0/0      Mar 29 2018 00:24:22   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3      Mar 29 2018 00:24:40   CRITICAL      Physical Port Link Down [1]
xcvr container 0/0/4      Mar 29 2018 00:24:20   CRITICAL      Transceiver Missing - Link
 Down [1]

Router# show logging
```

```
*Jun  8 07:00:35.038: %IOSXE_RP_ALARM-2-PEM: CLEAR MAJOR Fan Tray/Ext. ALARM: Fan Tray/Fan
 8 Failure
*Jun  8 07:00:35.038: %IOSXE_PEM-6-FANOK: The fan in slot P2/8 is functioning properly
Router# show facility-alarm status
System Totals  Critical: 2  Major: 0  Minor: 0
Source                    Time                   Severity      Description [Index]
------                    ------                 --------      -------------------
Power Supply Bay 0        Jun 07 2016 13:36:49   CRITICAL      Power Supply/FAN Module
Missing [0]
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]
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 08 2016 07:09:29   MAJOR         Fan Tray/Fan 11 Failure
[18]
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]
Router# show logging
*Jun  8 07:00:35.038: %IOSXE_RP_ALARM-2-PEM: CLEAR MAJOR Fan Tray/Ext. ALARM: Fan Tray/Fan
 8 Failure
*Jun  8 07:00:35.038: %IOSXE_PEM-6-FANOK: The fan in slot P2/8 is functioning properly
*Jun  8 07:07:59.391: %IOSXE_RP_ALARM-2-PEM: ASSERT MAJOR Fan Tray/Ext. ALARM: Fan Tray/Fan
 11 Failure
*Jun  8 07:07:59.393: %IOSXE_PEM-3-FANFAIL: The fan in slot P2/11 is encountering a failure
 condition
*Jun  8 07:08:17.405: %IOSXE_RP_ALARM-2-PEM: CLEAR MAJOR Fan Tray/Ext. ALARM: Fan Tray/Fan
 11 Failure
*Jun  8 07:08:17.405: %IOSXE_PEM-6-FANOK: The fan in slot P2/11 is functioning properly
*Jun  8 07:09:29.449: %IOSXE_RP_ALARM-2-PEM: ASSERT MAJOR Fan Tray/Ext. ALARM: Fan Tray/Fan
 11 Failure
*Jun  8 07:09:29.449: %IOSXE_PEM-3-FANFAIL: The fan in slot P2/11 is encountering a failure
 condition
```

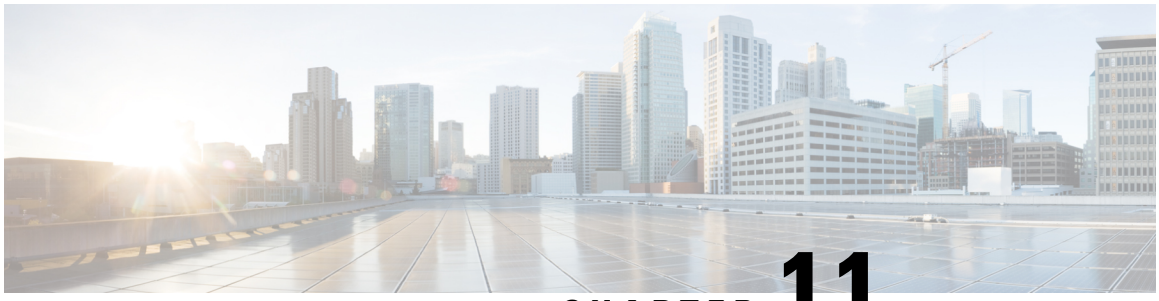
Configuring Alarm Filtering for SNMP Notifications: Example

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: 3  Major: 0  Minor: 0

Source                    Time                   Severity      Description [Index]
------                    ------                 --------      -------------------
GigabitEthernet0/0/0      Mar 29 2018 00:24:22   CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3      Mar 29 2018 00:24:40   CRITICAL      Physical Port Link Down [1]
xcvr container 0/0/4      Mar 29 2018 00:24:20   CRITICAL      Transceiver Missing - Link
 Down [1]
```



CHAPTER 11

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 76 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 8: 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
bfd                              Notice
binos                            Notice
bipc                             Notice
bridge-domain                    Notice
bsignal                          Notice
btrace                           Notice
bump_ptr_alloc                   Notice
cce                              Notice
cdllib                           Notice
cef                              Notice
chasfs                           Notice
chasutil                         Notice
cos-marking                      Notice
cyan                             Notice
efp                              Notice
eoam                             Notice
ether-channel                    Notice
ether-dplb                       Notice
evlib                            Notice
evutil                           Notice
fhrp                             Notice
file_alloc                       Notice
flash                            Notice
fman_rp                          Notice
inject-marking                   Notice
interfaces                       Notice
ipc                              Notice
ipclog                           Notice
ipp-to-cos                       Notice
```

```
ipsec                           Notice
ipsla                           Notice
l2cp                            Notice
l2fib                           Notice
local_span                      Notice
macinmac                        Notice
mgmte-acl                       Notice
mqipc                           Notice
om                              Notice
pbr                             Notice
peer                            Notice
protection                      Notice
protocol-marking                Notice
punt-police                     Notice
qos                             Notice
qos-account                     Notice
qos-event                       Notice
qos-hqf                         Notice
qos-infra                       Notice
qos-init                        Notice
qos-police                      Notice
qos-set                         Notice
qos-stats                       Notice
remote_span                     Notice
route-map                       Notice
services                        Notice
source                          Notice
subsys                          Notice
sw_wdog                         Notice
syshw                           Notice
tdl_acl_db                      Notice
tdl_bdomain_common              Notice
tdl_bdomain_db                  Notice
tdl_cdlcore                     Notice
tdl_cef_config                  Notice
tdl_cef_config_common           Notice
tdl_cef_route                   Notice
tdl_dpidb_config                Notice
tdl_dpidb_db                    Notice
tdl_ether_efp                   Notice
tdl_ether_efp_db                Notice
tdl_fman_rp_uea                 Notice
tdl_ipc_ack                     Notice
tdl_l2cp_db                     Notice
tdl_l2fib_config                Notice
tdl_l2fib_db                    Notice
tdl_om                          Notice
tdl_tdl_toc                     Notice
tdl_ui                          Notice
tdl_urpf_config                 Notice
tdl_urpf_db                     Notice
tdl_vrf_config                  Notice
tdl_vrf_db                      Notice
tdllib                          Notice
trans_avl                       Notice
trans_gbt                       Notice
trccfg                          Notice
uihandler                       Notice
uipeer                          Notice
uistatus                        Notice
urpf                            Notice
virtual-ethernet                Notice
vista                           Notice
vs_flock                        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
```