Cisco 8100 Series Secure Routers Software Configuration Guide

First Published: 2025-09-11

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 32

CHAPTER 33

CHAPTER 34

CHAPTER 1

Preface

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

- Objectives, on page 1
- Document revision history, on page 1

Objectives

This document provides an overview of software functionality for Cisco 8100 Series Secure Routers.

It is not intended as a comprehensive guide to all of the software features that can be run using the Cisco 8100 Series Secure Routers but only the software aspects that are specific to this platform.

For information on general software features that are also available on the Cisco 8100 Series Secure Routers, see the Cisco IOS XE technology guide for that specific software feature.

Document revision history

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

Release number	Date	Change summary
Cisco IOS XE 17.18.1	September 05, 2025	C8130-G2, C8140-G2, C8151-G2, and C8161-G2 routers were introduced.

CHAPTER 2

Read Me First

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related references

- Cisco IOS Command References, All Releases

Obtaining documentation and submitting a service request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

CHAPTER 3

Introduction to Cisco 8100 Series Secure Routers

The Cisco 8100 Series Secure Routers empowers small sites to operate securely and reliably—simplifying management while scaling with your business needs.

The Cisco 8100 Series Secure Routers deliver robust, platform-level security, advanced performance engineering via routing and SD-WAN, and on-premises, infrastructure-as-code, or cloud management flexibility that enables businesses to seamlessly scale and grow

This document covers configuration details for these models:

- C8130-G2
- C8140-G2
- C8151-G2
- C8161-G2

The 8-port platforms are high-performance managed service provider and enterprise platforms having:

- 8-port integrated front panel switch ports.
- Only C8161-G2 comes with PoE support.
- Only C8151-G2 and C8161-G2 support 4G LTE advanced and 5G Sub-6GHz support with carrier aggregation.

The 4-port platforms are midrange performance managed service provider platforms and enterprise platforms with the following specifications:

- 4-port integrated front panel switch ports.

CHAPTER 4

Use Cisco IOS XE software

Access the CLI using a router console

Cisco 8100 Series Secure Routers have console port with modem support.

The following sections describe the main methods of accessing the router:

- Accessing the CLI using a directly connected console, on page 7
- Access the CLI from a remote console using telnet, on page 9
- Access the CLI from a remote console using a modem, on page 10

Accessing the CLI using a directly connected console

The CON port is an EIA/TIA-232 asynchronous, serial connection with no-flow control and an RJ-45 connector. The CON port is located on the front panel of the chassis.

The following sections describe the procedure to access the control interface:

Connect to the Console Port

Procedure

Step 1 Configure your terminal emulation software with the following settings:

- 9600 bits per second (bps)
- 8 data bits
- No parity
- No flow control

Step 2 Connect to the CON port using the RJ-45-to-RJ-45 cable and the RJ-45-to-DB-25 DTE adapter or the RJ-45-to-DB-9 DTE adapter (labeled Terminal).

Use the console interface

Procedure

Step 1 Enter the following command:

```
Router > enable
```

Step 2 (Go to Step 3 if the enable password has not been configured.) At the password prompt, enter your system password:

```
Password: enablepass
```

When your password is accepted, the privileged EXEC mode prompt is displayed.

```
Router#
```

You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 3 If you enter the **setup** command, see “Using Cisco Setup Command Facility” in the “Initial Configuration” section of the Hardware Installation Guide for the Cisco 8100 Series Secure Routers.

Step 4 To exit the console session, enter the **exit** command:

```
Router# exit
```

Use SSH to Access Console

Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. To enable SSH support on the device:

Procedure

Step 1 Configure the hostname:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname xxx_lab
```

Here, *host name* is the router hostname or IP address.

Step 2 Configure the DNS domain of the router:

```
xxx_lab(config)# ip domain-name xxx.cisco.com
```

Step 3 Generate an SSH key to be used with SSH:

```
xxx_lab(config)#  crypto key generate rsa
The name for the keys will be: xxx_lab.xxx.cisco.com Choose the size of the key modulus in the range
```

```
of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few
minutes.
How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
xxx_lab(config)#
```

Step 4 By default, the vtys? transport is Telnet. In this case, Telnet is disabled and only SSH is supported:

```
xxx_lab(config)#line vty 0 4
xxx_lab(config-line)#transport input SSH
```

Step 5 Create a username for SSH authentication and enable login authentication:

```
xxx_lab(config)# username jsmith privilege 15 secret 0 p@ss3456
xxx_lab(config)#line vty 0 4
xxx_lab(config-line)# login local
```

Step 6 Verify remote connection to the device using SSH.

Access the CLI from a remote console using telnet

The following topics describe the procedure to access the CLI from a remote console using Telnet:

Preparing to Connect to the Router Console Using Telnet

To access the router remotely using Telnet from a TCP/IP network, configure the router to support virtual terminal lines using the **line vty** global configuration command. Configure the virtual terminal lines to require users to log in and specify a password.

See the Cisco IOS Terminal Services Command Reference document for more information about the line **vty global** configuration command.

To prevent disabling login on a line, specify a password with the **password** command when you configure the **login** command.

If you are using authentication, authorization, and accounting (AAA), configure the **login authentication** command. To prevent disabling login on a line for AAA authentication when you configure a list with the login authentication command, you must also configure that list using the **aaa authentication login** global configuration command.

For more information about AAA services, see the Cisco IOS XE Security Configuration Guide: Secure Connectivity and the Cisco IOS Security Command Reference documents. For more information about the **login line-configuration** command, see the Cisco IOS Terminal Services Command Reference document.

In addition, before you make a Telnet connection to the router, you must have a valid hostname for the router or have an IP address configured on the router. For more information about the requirements for connecting to the router using Telnet, information about customizing your Telnet services, and using Telnet key sequences, see the Cisco IOS Configuration Fundamentals Configuration Guide.

Use the console interface

Procedure

Step 1 Enter the following command:

```
Router > enable
```

Step 2 (Go to Step 3 if the enable password has not been configured.) At the password prompt, enter your system password:

```
Password: enablepass
```

When your password is accepted, the privileged EXEC mode prompt is displayed.

```
Router#
```

You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 3 If you enter the **setup** command, see “Using Cisco Setup Command Facility” in the “Initial Configuration” section of the Hardware Installation Guide for the Cisco 8100 Series Secure Routers.

Step 4 To exit the console session, enter the **exit** command:

```
Router# exit
```

Access the CLI from a remote console using a modem

To access the router remotely using a modem through an asynchronous connection, connect the modem to the port. For more information, see the "Configuring Console Port for Modem Connection" section.

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 following table lists the keyboard shortcuts for entering and editing commands.

Table 1: Keyboard shortcuts

Key Name	Purpose
Ctrl-B or the **Left Arrow** key[1]	Move the cursor back one character.
Ctrl-F or the **Right Arrow** key[1]	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.

Key Name	Purpose
Esc F	Move the cursor forward one word.

Use the History Buffer to Recall Commands

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

The following table lists the history substitution commands.

Table 2: History substitution commands

Command	Purpose
Ctrl-P or the **Up Arrow** key[1]	Recalls 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** key[1]	Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the **Up Arrow** key.
Router# show history	While in EXEC mode, lists the last few commands you entered.

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

Command Modes

The command modes available in Cisco IOS XE are the same as those available in traditional Cisco IOS. 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 following table 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 3: 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** command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** 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.

Command Mode	Access Method	Prompt	Exit Method
Diagnostic	The router boots up or accesses diagnostic mode in the following scenarios: • In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload. • A user-configured access policy is configured using the **transport-map** command that directs a user into diagnostic mode. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) is entered and the router is configured to go to diagnostic mode when the break signal is received.	`Router(diag)#`	If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco 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 by using a method that is configured to connect to the Cisco IOS CLI.
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.	`rommon#>`	To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded.

Diagnostic Mode

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the system resets when the IOS process or processes fail.
- A user-configured access policy was configured using the **transport-map** command that directs the user into the diagnostic mode.
- A send break signal (**Ctrl-C** or **Ctrl-Shift-6**) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

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

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

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMMON, to diagnose and troubleshoot Cisco IOS problems. The diagnostic mode commands can work when the Cisco IOS process is not working properly. These commands are also available in privileged EXEC mode on the router when the router is working normally.

Get 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 that is specific to a command mode, a command, a keyword, or an argument, use one of the following commands.

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. **Note** There is no space between the command and the question mark.
abbreviated-command-entry<Tab>	Completes a partial command name.
?	Lists all the commands that are available for a particular command mode.
command ?	Lists the keywords or arguments that you must enter next on the command line. **Note** There is a space between the command and the question mark.

Find command options

This section provides information about how to display the 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 a part of a command followed by a space. The Cisco IOS XE software displays a list and brief descriptions of the available keywords and arguments. For example, if you are in global configuration mode and want to see all the keywords and arguments for the **arap** command, you should 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 following table shows examples of using the question mark (**?**) to assist you in entering commands.

Table 4: Finding Command Options

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>  GigabitEthernet interface number`
 	
`Router(config)#interface GigabitEthernet 0/?`
`  <0-6>  Port Adapter number`
 	
`Router(config)#interface GigabitEthernet 0/0/?`
`  <0-143>  GigabitEthernet interface number`
 	
`Router(config)#interface GigabitEthernet 0/0/0?`
`.  <0-151>`
 	
`Router(config-if)#`
	Enter interface configuration mode by specifying the interface that you want to configure, using the **interface GigabitEthernet** global configuration command.
	Enter **?** to display what you must enter next on the command line.
	When the <cr> symbol is displayed, you can press **Enter** to complete the command.
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`

<table>
<tr><th>Command</th><th>Comment</th></tr>
<tr><td>

```
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)#
```

</td><td>Enter <b>?</b> to display a list of all the interface configuration commands available for the interface. This example shows only some of the available interface configuration commands.</td></tr>
</table>

Command	Comment

Router(config-if)# **ip ?**
Interface IP configuration subcommands:
  access-group   Specify access control
for packets
  accounting   Enable IP accounting on
this interface
  address   Set the IP address of an
 interface
  authentication   authentication subcommands
 	
  bandwidth-percent   Set EIGRP bandwidth limit
 	
  broadcast-address   Set the broadcast address
 of an interface
  cgmp   Enable/disable CGMP
  directed-broadcast Enable forwarding of
directed broadcasts
  dvmrp   DVMRP interface commands
  hello-interval   Configures IP-EIGRP hello
 interval
  helper-address   Specify a destination
address for UDP broadcasts
  hold-time   Configures IP-EIGRP hold
 time
  .
  .
  .
Router(config-if)# **ip**
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Router(config-if)# **ip address ?** A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# **ip address**	Enter the command that you want to configure for the interface. This example uses the **ip address** command. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword. A carriage return (<cr>) is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.
Router(config-if)# ip address 192.0.2.13 ? A.B.C.D IP address dhcp IP Address negotiated via DHCP pool IP Address autoconfigured from a local DHCP pool Router(config-if)# **ip address 192.0.2.13**	Enter the keyword or argument that you want to use. This example uses the 192.0.2.13 IP address. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. <cr> is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.

Command	Comment

`Router(config-if)# ip address 192.0.2.13 255.255.255.0 ?`
`  secondary           Make this IP address a secondary address`
`  <cr>`
`Router(config-if)# ip address 192.0.2.13 255.255.255.0`
	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.
	Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**.
	<cr> is displayed. Press **Enter** to complete the command, or enter another keyword.

`Router(config-if)# ip address 192.0.2.13 255.255.255.0`
`Router(config-if)#`
	Press **Enter** to complete the command.

Use the no and default Forms of Commands

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

Many CLI commands also have a **default** form. By issuing the *<command>* **default** command-name, you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function from a **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.

Use the Factory Reset commands

The **factory reset** commands are used to remove all the customer specific data on a router/switch that has been added. The data can be configuration, log files, boot variables, core files, and so on.

The **factory-reset all** command erases the bootflash, nvram, rommon variables, licenses, and logs.

```
Router#factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
*Enter*

*May 12 09:55:45.831: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.

***Return to ROMMON Prompt
```

Save 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 may take a few minutes to save the configuration. After the configuration has been saved, the following output is displayed:

```
[OK]
Router#
```

This task saves the configuration to the NVRAM.

Manage Configuration Files

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 also used on several other Cisco router platforms.

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

The **copy** command can be used to back up startup configuration files.

For more detailed information on managing configuration files, see the "Managing Configuration Files" section in the Cisco IOS XE Configuration Fundamentals Configuration Guide.

Filter 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.

Example

In this example, a modifier of the **show interface** command (**include protocol**) is used to provide only the output lines in which the expression **protocol** is displayed:

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/1 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/2 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/3 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0 is up, line protocol is up
     0 unknown protocol drops
Loopback0 is up, line protocol is up
     0 unknown protocol drops
```

Power off a router

Before you begin

The router can be safely turned off at any time by moving the router's power supply switch to the Off position. However, any changes to the running config since the last WRITE of the config to the NVRAM is lost.

Ensure that any configuration needed after startup is saved before powering off the router. The **copy running-config startup-config** command saves the configuration in NVRAM and after the router is powered up, the router initializes with the saved configuration.

CLI session management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that the other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access a router.

Information about CLI session management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that each other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access the router.

Change the CLI session timeout

Procedure

Step 1 `configure terminal`

Enters global configuration mode

Step 2 `line console 0`

Step 3 `session-timeout` *`minutes`*

The value of *`minutes`* sets the amount of time that the CLI waits before timing out. Setting the CLI session timeout increases the security of a CLI session. Specify a value of 0 for *`minutes`* to disable session timeout.

Step 4 `show line console 0`

Verifies the value to which the session timeout has been set, which is shown as the value for `"Idle Session"`.

Lock a CLI session

Before you begin

To configure a temporary password on a CLI session, use the **lock** command in EXEC mode. Before you can use the **lock** command, you need to configure the line using the **lockable** command. In this example the line is configured as **lockable**, and then the **lock** command is used and a temporary password is assigned.

Procedure

Step 1

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 Enter the line upon which you want to be able to use the **lock** command.

```
Router(config)# line console 0
```

Step 3

```
Router(config)# lockable
```

Enables the line to be locked.

Step 4

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

Step 5

```
Router# lock
```

The system prompts you for a password, which you must enter twice.

```
Password: <password>
Again: <password>
Locked
```

Initial bootup security

This section contains the following:

Enforce changing default password

The Enforce Changing Default Password feature allows you to change the default password and set a new password for a better encryption algorithm. The enable secret is a command that allows you to set a new password which helps to protect the access to different modes such as a privileged EXEC and configuration mode.

With the earlier software versions, you can bypass the option to set a new enabled password. When the device first boots up after the factory reset or fresh from the factory, the following prompt is displayed on the console:

Would you like to enter the initial configuration dialog? [yes/no]:

The earlier versions of the software allow you to answer **no** and the device changes to the **Router>** prompt with a blank enable password. At this point, you can configure the device and bring it into service with a blank enable password.

In the earlier documentation, Cisco recommended using the **enable secret** command instead of the **enable password** command because this provides an improved encryption algorithm.

Starting with Cisco IOS XE Release 17.18.1a, the initial dialog is changed to force setting a new enable password and also using the **enable secret** command instead. The following is an example:

```
Would you like to enter basic management setup? [yes/no]:yes
Configuring global parameters

Enter host name [Router]:router-1

The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
Secret should be of minimum 10 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
Enter enable secret: ********
Confirm enable secret:********

The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
Enter enable password: ********

The virtual terminal password is used to protect
  access to the router over a network interface.
Enter virtual terminal password:********
Configure SNMP Network Management?no

Enter interface name used to connect to the
management network from the above interface summary:Ethernet0/0

Configuring interface Ethernet0/0
Configure IP on this interface? [yes]:no

The following configuration command script was created:
hostname router-1
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
.
.
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:2
.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
```

The following is an example of what happens if you answer **no** to the initial configuration dialog:

```
Would you like to enter the initial configuration dialog? [yes/no]:no
The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret:********
  Confirm enable secret:********
Would you like to terminate autoinstall? [yes]:yes

.
.
```

```
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
```

After the enable secret is prompted during the first login, you can enter a password and this password is always masked. If you enter a weak password, the device will prompt again to enter a strong password. For example, you must use the standard mix of upper-case and lower-case characters, special characters, numbers, and so on. The device will continue to prompt until you enter a strong password. You should enter the strong secret password twice for confirming and configuring the device.”

CHAPTER 5

Install the software

This chapter contains the following sections:

Install a software

Installing software on the router involves installing a consolidated package (bootable image). This consists of a bundle of subpackages (modular software units), with each subpackage controlling a different set of functions.

Licensing for Cisco 8000 Series Secure Routers

Cisco 8000 Series Secure Routers support platform-based licensing, a way of grouping licenses and devices based on platform-classes. A platform class is a hierarchical categorization based on the product family and place in the network. In this platform-based licensing model, Essentials and Advantage licenses are available. License portability is supported across devices within the same platform class and usage of the same license across different modes is also possible.

For more information, see Cisco 8000 Series Secure Routers Licensing.

Provisioning files

The consolidated package on a router consists of a collection of subpackages and a provisioning file titled `packages.conf`. To run the software, the usual method used is to boot the consolidated package, which is copied into memory, expanded, mounted, and run within memory. The provisioning file's name can be renamed but subpackage file's names cannot be renamed. The provisioning file and subpackage files must be kept in the same directory. The provisioning file does not work properly if any individual subpackage file is contained within a different directory.

Note An exception to this is that if a new or upgraded module firmware package is subsequently installed, it need not be in the same directory as the provisioning file.

Configuring a router to boot, using the provisioning file packages.conf, is beneficial because no changes have to be made to the boot statement after the Cisco IOS XE software is upgraded.

File systems

The following table provides a list of file systems that can be seen on the Cisco 8100 Series Secure Routers.

Table 5: Router File Systems

File System	Description
bootflash:	Boot flash memory file system.
flash:	Alias to the boot flash memory file system above.
cns:	Cisco Networking Services file directory.
nvram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
obfl:	File system for Onboard Failure Logging (OBFL) files.
system:	System memory file system, which includes the running configuration.
tar:	Archive file system.
tmpsys:	Temporary system files file system.
usb0:	The Universal Serial Bus (USB) flash drive file systems. **Note** The USB flash drive file system is visible only if a USB drive is installed in usb0: port.

Use the **?** help option, or use the **copy** command in command reference guides, if you find a file system that is not listed in the table above.

Autogenerated file directories and files

This section discusses the autogenerated files and directories that can be created, and how the files in these directories can be managed.

Table 6: Autogenerated files

File or Directory	Description
crashinfo files	Crashinfo files may appear in the bootflash: file system. These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes. However, the files are not part of router operations, and can be erased without impacting the functioning of the router.
core directory	The storage area for .core files. If this directory is erased, it will automatically regenerate itself at bootup. The .core files in this directory can be erased without impacting any router functionality, but the directory itself should not be erased.
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 directory	The storage area for trace files. Trace files are useful for troubleshooting. If the Cisco IOS process fails, for instance, users or troubleshooting personnel can access trace files using diagnostic mode to gather information related to the Cisco IOS failure. Trace files, however, are not a part of router operations, and can be erased without impacting the router's performance.

Important notes about autogenerated directories

Important information about autogenerated directories include:

- Autogenerated files on the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by Cisco customer support.

Note Altering autogenerating files on the bootflash: may have unpredictable consequences for system performance.

- Crashinfo, core, and trace files can be deleted.

Flash storage

Subpackages are installed to local media storage, such as flash memory. For flash storage, use the **dir bootflash:** command to list the file names.

Note Flash storage is required for successful operation of a router.

Configuring the configuration register for autoboot

The configuration register can be used to change router behavior. This includes controlling how the router boots. Set the configuration register to 0x0 to boot into ROM, by using one of the following commands:

- In Cisco IOS configuration mode, use the **config-reg** 0x0 command.
- From the ROMMON prompt, use the **confreg** 0x0 command.

For more information about the configuration register, see Configuring a router to boot the consolidated package via TFTP using the boot command, on page 33.

Note Setting the configuration register to 0x2102 will set the router to autoboot the Cisco IOS XE software.

Note The console baud rate is set to 9600 after changing the **confreg** to 0x2102 or 0x0. If you cannot establish a console session after setting **confreg**, or garbage output appears, change the setting on your terminal emulation software to 9600.

LED indicators

For information on LEDs on the router, see the LED Indicators section of the Hardware Installation Guide for the Cisco 8100 Series Secure Routers.

How to install and upgrade the software

Installing software on the router involves installing a consolidated package (bootable image). This consists of a bundle of subpackages (modular software units), with each subpackage controlling a different set of functions.

Managing and configuring a consolidated package using copy and boot commands

To upgrade a consolidated package, copy the consolidated package to the **bootflash:** directory on the router using the **copy** command. After making this copy of the consolidated package, configure the router to boot using the consolidated package file.

The following example shows the consolidated package file being copied to the **bootflash:** file system via TFTP. The config register is then set to boot using **boot system** commands, and the **boot system** commands instruct the router to boot using the consolidated package stored in the **bootflash:** file system. The new configuration is then saved using the **copy running-config startup-config** command, and the system is then reloaded to complete the process.

```
Router# dir bootflash:
Directory of bootflash:/

915713  drwx            49152   Sep 4 2025 04:38:55 +00:00  tracelogs
654081  drwx             4096   Sep 3 2025 07:13:05 +00:00  .installer
19      -rw-               30   Sep 3 2025 07:04:12 +00:00  throughput_monitor_params
130819  drwx             4096   Sep 3 2025 07:04:09 +00:00  license_evlog
13      -rw-           143021   Sep 3 2025 07:04:08 +00:00  memleak.tcl
130817  drwx             4096   Sep 3 2025 07:04:01 +00:00  .prst_sync
12      -rwx             3050   Sep 3 2025 07:03:52 +00:00  mode_event_log
1046529  drwx             4096   Sep 3 2025 07:03:20 +00:00  sysboot
130832  drwx             4096  Aug 22 2025 04:16:36 +00:00  .product_analytics
44      -rw-        770581540  Aug 15 2025 03:44:43 +00:00
c81g2be-universalk9.17.18.01a.0.176.SSA.bin
392452  drwx             4096  Aug 15 2025 03:31:43 +00:00  .geo
43      -rw-             1426  Aug 15 2025 03:30:09 +00:00  .iomcu_autoupgd.log
42      -rw-         12028620  Aug 15 2025 03:27:35 +00:00
c81g2be_rel_rommon_1718_1r_20250717.SSA.pkg
21      -rw-        772960084  Aug 15 2025 03:26:56 +00:00
c81g2be-universalk9.2025-08-05_18.44_mingfli_0x2e_iomcu_upd.SSA.bin
130821  drwx             4096  Aug 15 2025 02:40:45 +00:00  pnp-tech
11      -rw-              255  Aug 15 2025 02:38:57 +00:00  .iox_dir_list
1046534  drwx             4096  Mar 28 2025 03:27:33 +00:00  .dbpersist
392449  drwx             4096  Mar 28 2025 03:25:27 +00:00  .rollback_timer
41      -rw-             6734  Mar 28 2025 03:25:07 +00:00  packages.conf
34      -rw-             6734  Mar 28 2025 03:24:43 +00:00
c81g2be-universalk9.17.17.01eftr3.20250305.for_Charon_MFG_Pilot_Build.SPA.conf
25      -rw-         83144848  Mar 28 2025 03:24:35 +00:00
c81g2be-rpboot.17.17.01eftr3.SPA.pkg
23      drwx             4096  Mar 28 2025 03:24:30 +00:00  .images
22      drwx             4096  Mar 28 2025 03:21:18 +00:00  iox_host_data_share
523266  drwx             4096  Mar 28 2025 03:21:14 +00:00  core
17      drwx             4096  Mar 28 2025 03:21:13 +00:00  .attrib
392451  drwx             4096  Mar 28 2025 03:20:57 +00:00  guest-share
915812  drwx             4096  Mar 28 2025 03:20:54 +00:00  onep
261635  drwx             4096  Mar 28 2025 03:20:54 +00:00  pnp-info
16      drwx             4096  Mar 28 2025 03:20:49 +00:00  virtual-instance
14      -rw-            34967  Mar 28 2025 03:20:44 +00:00  ios_core.p7b
15      -rw-             1939  Mar 28 2025 03:20:44 +00:00  trustidrootx3_ca_062035.ca
523265  drwx             4096  Mar 28 2025 03:20:08 +00:00  SHARED-IOX
261633  drwx             4096  Mar 28 2025 03:20:08 +00:00  pcap
30      -rw-        663396352   Mar 3 2025 14:12:26 +00:00
c81g2be-mono-universalk9.17.17.01eftr3.SPA.pkg
29      -rw-            49152   Mar 3 2025 14:10:18 +00:00
c81g2be-firmware_pse_si3470a.17.17.01eftr3.SPA.pkg
28      -rw-           200704   Mar 3 2025 14:10:18 +00:00
c81g2be-firmware_charon_mcu.17.17.01eftr3.SPA.pkg



Router# copy tftp: bootflash:
Address or name of remote host []? 172.17.16.81
Source filename []? auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.bin
Destination filename [c81g2be-universalk9.17.18.01a.SPA.bin]?
Accessing tftp://172.17.16.81/auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.bin...
Loading auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.bin from 172.17.16.81 (via
GigabitEthernet0/0/0):

[OK - 770579420 bytes]

770579420 bytes copied in 981.504 secs (785101 bytes/sec)

Router# dir bootflash:
Directory of bootflash:/
```

```
654081  drwx             4096   Sep 4 2025 06:46:09 +00:00  .installer
45      -rw-        770579420   Sep 4 2025 06:45:15 +00:00
c81g2be-universalk9.17.18.01a.SPA.bin
915713  drwx            49152   Sep 4 2025 06:31:00 +00:00  tracelogs
19      -rw-               30   Sep 3 2025 07:04:12 +00:00  throughput_monitor_params
130819  drwx             4096   Sep 3 2025 07:04:09 +00:00  license_evlog
13      -rw-           143021   Sep 3 2025 07:04:08 +00:00  memleak.tcl
130817  drwx             4096   Sep 3 2025 07:04:01 +00:00  .prst_sync
12      -rwx             3050   Sep 3 2025 07:03:52 +00:00  mode_event_log
1046529  drwx             4096   Sep 3 2025 07:03:20 +00:00  sysboot
130832  drwx             4096  Aug 22 2025 04:16:36 +00:00  .product_analytics
44      -rw-        770581540  Aug 15 2025 03:44:43 +00:00
c81g2be-universalk9.17.18.01a.0.176.SSA.bin
392452  drwx             4096  Aug 15 2025 03:31:43 +00:00  .geo
43      -rw-             1426  Aug 15 2025 03:30:09 +00:00  .iomcu_autoupgd.log
42      -rw-         12028620  Aug 15 2025 03:27:35 +00:00
c81g2be_rel_rommon_1718_1r_20250717.SSA.pkg
21      -rw-        772960084  Aug 15 2025 03:26:56 +00:00
c81g2be-universalk9.2025-08-05_18.44_mingfli_0x2e_iomcu_upd.SSA.bin
130821  drwx             4096  Aug 15 2025 02:40:45 +00:00  pnp-tech
11      -rw-              255  Aug 15 2025 02:38:57 +00:00  .iox_dir_list
1046534  drwx             4096  Mar 28 2025 03:27:33 +00:00  .dbpersist
392449  drwx             4096  Mar 28 2025 03:25:27 +00:00  .rollback_timer
41      -rw-             6734  Mar 28 2025 03:25:07 +00:00  packages.conf
34      -rw-             6734  Mar 28 2025 03:24:43 +00:00
c81g2be-universalk9.17.17.01eftr3.20250305.for_Charon_MFG_Pilot_Build.SPA.conf
25      -rw-         83144848  Mar 28 2025 03:24:35 +00:00
c81g2be-rpboot.17.17.01eftr3.SPA.pkg
23      drwx             4096  Mar 28 2025 03:24:30 +00:00  .images
22      drwx             4096  Mar 28 2025 03:21:18 +00:00  iox_host_data_share
523266  drwx             4096  Mar 28 2025 03:21:14 +00:00  core
17      drwx             4096  Mar 28 2025 03:21:13 +00:00  .attrib
392451  drwx             4096  Mar 28 2025 03:20:57 +00:00  guest-share
915812  drwx             4096  Mar 28 2025 03:20:54 +00:00  onep
261635  drwx             4096  Mar 28 2025 03:20:54 +00:00  pnp-info
16      drwx             4096  Mar 28 2025 03:20:49 +00:00  virtual-instance
14      -rw-            34967  Mar 28 2025 03:20:44 +00:00  ios_core.p7b
15      -rw-             1939  Mar 28 2025 03:20:44 +00:00  trustidrootx3_ca_062035.ca
523265  drwx             4096  Mar 28 2025 03:20:08 +00:00  SHARED-IOX
261633  drwx             4096  Mar 28 2025 03:20:08 +00:00  pcap
30      -rw-        663396352   Mar 3 2025 14:12:26 +00:00
c81g2be-mono-universalk9.17.17.01eftr3.SPA.pkg
29      -rw-            49152   Mar 3 2025 14:10:18 +00:00
c81g2be-firmware_pse_si3470a.17.17.01eftr3.SPA.pkg
28      -rw-           200704   Mar 3 2025 14:10:18 +00:00
c81g2be-firmware_charon_mcu.17.17.01eftr3.SPA.pkg


Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash bootflash:c81g2be-universalk9.17.18.01a.SPA.bin
Router(config)# config-reg 0x2102
Router(config)# exit

Router# show run | include boot
boot-start-marker
boot system flash bootflash:c81g2be-universalk9.17.18.01a.SPA.bin
boot-end-marker

Router# copy run start
Destination filename [startup-config]? Building configuration...
[OK]
```

```
Router# reload
Proceed with reload? [confirm]
Sep  4 07:50:38.121: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: process
exit with reload chassis code


[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]


System Bootstrap, Version 17.18(1r), RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8140-G2 platform with 4194304 Kbytes of main memory
......
Located bootflash:c81g2be-universalk9.17.18.01a.SPA.bin
####################################################################################################################################################################################################################################################################################################################################################

Package header rev 3 structure detected
IsoSize = 690106368
Performing Integrity Check ...
Performing Signature Verification ...
Image validated
Sep  4 07:51:46.744: %SYS-4-ROUTER_RUNNING_BUNDLE_BOOT_MODE: R0/0: Warning: Booting with
bundle mode will be deprecated in the near future. Migration to install mode is required.
Sep  4 07:51:56.307: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

              Restricted Rights Legend

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

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



Cisco IOS Software [IOSXE], c81g2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.18.1a, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 15-Aug-25 07:05 by mcpre


This software version supports only Smart Licensing as the software licensing mechanism.


Please read the following carefully before proceeding. By downloading,
installing, and/or using any Cisco software product, application, feature,
license, or license key (collectively, the "Software"), you accept and
agree to the following terms. If you do not agree, do not proceed and do not
use this Software.

This Software and its use are governed by Cisco's General Terms and any
relevant supplemental terms found at
https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html.
If you have a negotiated agreement with Cisco that includes this Software, the
```

```
terms of that agreement apply as well. In the event of a conflict, the order
of precedence stated in your negotiated agreement controls.

Cisco Software is licensed on a term and/or subscription-basis. The license to
the Software is valid only for the duration of the specified term, or in the
case of a subscription-based license, only so long as all required subscription
payments are current and fully paid-up. While Cisco may provide you
licensing-related alerts, it is your sole responsibility to monitor your usage.
Using Cisco Software without a valid license is not permitted and may result in
fees charged to your account. Cisco reserves the right to terminate access to,
or restrict the functionality of, any Cisco Software, or any features thereof,
that are being used without a valid license.


cisco C8140-G2 (1RU) processor with 1327599K/6147K bytes of memory.
Processor board ID FCW2913Y00D
Router operating mode: Autonomous
1 Virtual Ethernet interface
10 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
20270079K bytes of flash memory at bootflash:.


 WARNING: ** NOTICE **  The H.323 protocol is no longer supported from IOS-XE release 17.6.1.
 Please consider using SIP for multimedia applications.



Press RETURN to get started!

Router>enable
Router#show version
Cisco IOS XE Software, Version 17.18.01a
Cisco IOS Software [IOSXE], c81g2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.18.1a, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 15-Aug-25 07:05 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: 17.18(1r)
Router uptime is 1 minute
Uptime for this control processor is 2 minutes
System returned to ROM by Reload Command
System image file is "bootflash:c81g2be-universalk9.17.18.01a.SPA.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.


Technology Package License Information:

-----------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
-----------------------------------------------------------------
Smart License  Perpetual    essentials         essentials

The current crypto throughput level is 250000 kbps (Aggregate)


Smart Licensing Status: Smart Licensing Using Policy

cisco C8140-G2 (1RU) processor with 1327599K/6147K bytes of memory.
Processor board ID FCW2913Y00D
Router operating mode: Autonomous
1 Virtual Ethernet interface
10 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
20270079K bytes of flash memory at bootflash:.

Configuration register is 0x2102
```

Configuring a router to boot the consolidated package via TFTP using the boot command

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system
tftp://172.17.16.81/auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.bin
Router(config)#config-register 0x2102
Router(config)#exit

Router# show run | include boot
boot-start-marker
boot system tftp://172.17.16.81/auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.bin
boot-end-marker
diagnostic bootup level minimal
Router#

Router# copy running-config startup-config
Destination filename [startup-config]? Building configuration...
[OK]
```

```
Router# reload
Proceed with reload? [confirm]
Sep  3
[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]


System Bootstrap, Version 17.18(1r), RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8140-G2 platform with 4194304 Kbytes of main memory
......
          IP_ADDRESS: 192.168.45.2
      IP_SUBNET_MASK: 255.255.255.0
     DEFAULT_GATEWAY: 192.168.45.1
         TFTP_SERVER: 172.17.16.81
           TFTP_FILE: 
auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.bin/c81g2be-universalk9.17.18.01a.SPA.bin

        TFTP_MACADDR: A4:A5:84:4A:98:C0
          ETHER_PORT: 0
Downloading tftp://172.17.16.81/auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.bin
|---------+---------+---------+---------+---------|
...................................................
Located tftp://172.17.16.81/auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.bin
######################################################################################################################################################

Package header rev 3 structure detected
IsoSize = 690106368
Performing Integrity Check ...
Performing Signature Verification ...
Image validated
Sep  3 07:03:42.337: %SYS-4-ROUTER_RUNNING_BUNDLE_BOOT_MODE: R0/0: Warning: Booting with
bundle mode will be deprecated in the near future. Migration to install mode is required.
Sep  3 07:03:52.038: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

              Restricted Rights Legend

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

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



Cisco IOS Software [IOSXE], c81g2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.18.1a, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 15-Aug-25 07:05 by mcpre


This software version supports only Smart Licensing as the software licensing mechanism.


Please read the following carefully before proceeding. By downloading,
installing, and/or using any Cisco software product, application, feature,
license, or license key (collectively, the "Software"), you accept and
agree to the following terms. If you do not agree, do not proceed and do not
use this Software.

This Software and its use are governed by Cisco's General Terms and any
relevant supplemental terms found at
https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html.
If you have a negotiated agreement with Cisco that includes this Software, the
terms of that agreement apply as well. In the event of a conflict, the order
of precedence stated in your negotiated agreement controls.

Cisco Software is licensed on a term and/or subscription-basis. The license to
the Software is valid only for the duration of the specified term, or in the
case of a subscription-based license, only so long as all required subscription
payments are current and fully paid-up. While Cisco may provide you
licensing-related alerts, it is your sole responsibility to monitor your usage.
Using Cisco Software without a valid license is not permitted and may result in
fees charged to your account. Cisco reserves the right to terminate access to,
or restrict the functionality of, any Cisco Software, or any features thereof,
that are being used without a valid license.


cisco C8140-G2 (1RU) processor with 1327599K/6147K bytes of memory.
Processor board ID FCW2913Y00D
Router operating mode: Autonomous
1 Virtual Ethernet interface
10 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
20270079K bytes of flash memory at bootflash:.


 WARNING: ** NOTICE **  The H.323 protocol is no longer supported from IOS-XE release 17.6.1.
 Please consider using SIP for multimedia applications.



Press RETURN to get started!


Router>enable
Router#show version
Cisco IOS XE Software, Version 17.18.01a
Cisco IOS Software [IOSXE], c81g2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.18.1a, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 15-Aug-25 07:05 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: 17.18(1r)
Router uptime is 0 minutes
```

```
Uptime for this control processor is 1 minute
System returned to ROM by Reload Command
System image file is
"tftp://172.17.16.81/auto/tftp-users/user/c81g2be-universalk9.17.18.01a.SPA.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.


Technology Package License Information:

-----------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
-----------------------------------------------------------------
Smart License  Perpetual    essentials         essentials

The current crypto throughput level is 250000 kbps (Aggregate)


Smart Licensing Status: Smart Licensing Using Policy

cisco C8140-G2 (1RU) processor with 1327599K/6147K bytes of memory.
Processor board ID FCW2913Y00D
Router operating mode: Autonomous
1 Virtual Ethernet interface
10 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
20270079K bytes of flash memory at bootflash:.

Configuration register is 0x2102


Router#
```

CHAPTER 6

Install the software using commands

Install the software using install commands

From Cisco IOS XE 17.18.1a, all Cisco IOS XE platforms are shipped in install mode by default. Users can boot the platform, and upgrade or downgrade to Cisco IOS XE software versions using a set of **install** commands.

Restrictions for installing the software using install commands

- ISSU is not covered in this feature.
- Install mode requires a reboot of the system.

Information about installing the software using install commands

For routers shipped in install mode, a set of **install** commands can be used for starting, upgrading and downgrading of platforms in install mode.

From Cisco IOS XE 17.18.1a release, this update is applicable to all Cisco IOS XE platforms.

The following table describes the differences between Bundle mode and Install mode:

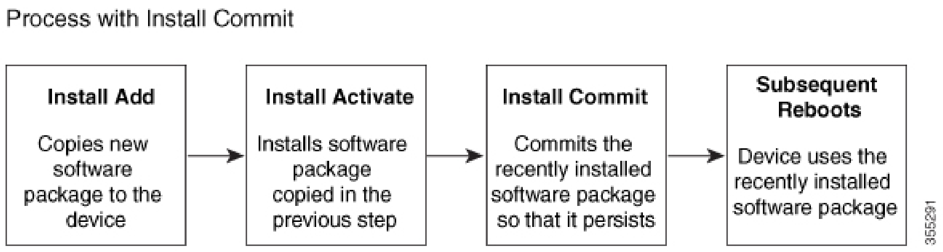
Table 7: Bundle mode vs Install mode

Bundle mode	**Install mode**
This mode provides a consolidated boot process, using local (hard disk, flash) or remote (TFTP) .bin image. **Note** Bundle boot from USB and TFTPBoot is not supported.	This mode uses the local (bootflash) packages.conf file for the boot process.
This mode uses a single .bin file.	.bin file is replaced with expanded .pkg files in this mode.
CLI: `#boot system file <filename>`	CLI: `#install add file bootflash: [activate commit]`
To upgrade in this mode, point the boot system to the new image.	To upgrade in this mode, use the **install** commands.
Image Auto-Upgrade: When a new Field-Replaceable Unit (FRU) is inserted in a modular chassis, manual intervention is required to get the new FRU running with the same version as the active FRUs.	Image Auto-Upgrade: When a new FRU is inserted in a modular chassis, the joining FRU is auto-upgraded to the image version in sync with the active FRUs.
Rollback: Rollback to the previous image with multiple Software Maintenance Updates (SMUs) may require multiple reloads.	Rollback: Enables rollback to an earlier version of Cisco IOS XE software, including multiple patches in single reload.

Install mode process flow

The install mode process flow comprises three commands to perform installation and upgrade of software on platforms–**install add**, **install activate**, and **install commit**.

The following flow chart explains the install process with **install** commands:


Process with Install Commit
Install Add
Copies new software package to the device
Install Activate
Installs software package copied in the previous step
Install Commit
Commits the recently installed software package so that it persists
Subsequent Reboots
Device uses the recently installed software package
355291

The **install add** command copies the software package from a local or remote location to the platform. The location can be FTP, HTTP, HTTPs, or TFTP. The command extracts individual components of the .package file into subpackages and packages.conf files. It also validates the file to ensure that the image file is specific to the platform on which it is being installed.

The **install activate** command performs the required validations and provisions the packages previously added using the **install add** command. It also triggers a system reload.

The **install commit** command confirms the packages previously activated using the **install activate** command, and makes the updates persistent over reloads.

Note Installing an update replaces any previously installed software image. At any time, only one image can be installed in a device.

The following set of install commands is available:

Table 8: List of install Commands

Command	Syntax	Purpose
install add	**install add file** *location:filename.bin*	Copies the contents of the image, package, and SMUs to the software repository. File location may be local or remote. This command does the following: • Validates the file–checksum, platform compatibility checks, and so on. • Extracts individual components of the package into subpackages and packages.conf • Copies the image into the local inventory and makes it available for the next steps.
install activate	**install activate**	Activates the package added using the **install add** command. • Use the **show install summary** command to see which image is inactive. This image will get activated. • System reloads on executing this command. Confirm if you want to proceed with the activation. Use this command with the **prompt-level none** keyword to automatically ignore any confirmation prompts.

Command	Syntax	Purpose
(install activate) auto abort-timer	**install activate auto-abort timer** *<30-1200>*	The **auto-abort timer** starts automatically, with a default value of 120 minutes. If the **install commit** command is not executed within the time provided, the activation process is terminated, and the system returns to the last-committed state. • You can change the time value while executing the **install activate** command. • The **install commit** command stops the timer, and continues the installation process. • The **install activate auto-abort timer stop** command stops the timer without committing the package. • Use this command with the **prompt-level none** keyword to automatically ignore any confirmation prompts. • This command is valid only in the three-step install variant.
install commit	**install commit**	Commits the package activated using the **install activate** command, and makes it persistent over reloads. • Use the **show install summary** command to see which image is uncommitted. This image will get committed.

Command	Syntax	Purpose
install abort	**install abort**	Terminates the installation and returns the system to the last-committed state. • This command is applicable only when the package is in activated status (uncommitted state). • If you have already committed the image using the **install commit** command, use the **install rollback to** command to return to the preferred version.
install remove	**install remove {file** *<filename>* **| inactive}**	Deletes inactive packages from the platform repository. Use this command to free up space. • **file**: Removes specified files. • **inactive**: Removes all the inactive files.
install rollback to	**install rollback to {base | label | committed | id}**	Rolls back the software set to a saved installation point or to the last-committed installation point. The following are the characteristics of this command: • Requires reload. • Is applicable only when the package is in committed state. • Use this command with the **prompt-level none** keyword to automatically ignore any confirmation prompts. **Note** If you are performing install rollback to a previous image, the previous image must be installed in install mode. Only SMU rollback is possible in bundle mode.

Command	Syntax	Purpose
install deactivate	**install deactivate file** <*filename*>	Removes a package from the platform repository. This command is supported only for SMUs. • Use this command with the **prompt-level none** keyword to automatically ignore any confirmation prompts.

The following show commands are also available:

Table 9: List of show Commands

Command	Syntax	Purpose
show install log	**show install log**	Provides the history and details of all install operations that have been performed since the platform was booted.
show install package	**show install package** <*filename*>	Provides details about the .pkg/.bin file that is specified.
show install summary	**show install summary**	Provides an overview of the image versions and their corresponding install states for all the FRUs. • The table that is displayed will state for which FRUs this information is applicable. • If all the FRUs are in sync in terms of the images present and their state, only one table is displayed. • If, however, there is a difference in the image or state information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.
show install active	**show install active**	Provides information about the active packages for all the FRUs. If there is a difference in the information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.

Command	Syntax	Purpose
show install inactive	**show install inactive**	Provides information about the inactive packages, if any, for all the FRUs. If there is a difference in the information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.
show install committed	**show install committed**	Provides information about the committed packages for all the FRUs. If there is a difference in the information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.
show install uncommitted	**show install uncommitted**	Provides information about uncommitted packages, if any, for all the FRUs. If there is a difference in the information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.
show install rollback	**show install rollback {point-id | label}**	Displays the package associated with a saved installation point.
show version	**show version [rp-slot] [installed [user-interface] | provisioned | running]**	Displays information about the current package, along with hardware and platform information.

Boot the platform in install mode

You can install, activate, and commit a software package using a single command (one-step install) or multiple separate commands (three-step install).

If the platform is working in bundle mode, the one-step install procedure must be used to initially convert the platform from bundle mode to install mode. Subsequent installs and upgrades on the platform can be done with either one-step or three-step variants.

One step installation or converting from bundle mode to install mode

Note

- All the CLI actions (for example, add, activate, and so on) are executed on all the available FRUs.
- The configuration save prompt will appear if an unsaved configuration is detected.
- The reload prompt will appear after the second step in this workflow. Use the **prompt-level none** keyword to automatically ignore the confirmation prompts.
- If the prompt-level is set to None, and there is an unsaved configuration, the install fails. You must save the configuration before reissuing the command.

Use the one-step install procedure described below to convert a platform running in bundle boot mode to install mode. After the command is executed, the platform reboots in install boot mode.

Later, the one-step install procedure can also be used to upgrade the platform.

This procedure uses the **install add file activate commit** command in privileged EXEC mode to install a software package, and to upgrade the platform to a new version.

SUMMARY STEPS

1. **enable**
2. **install add file location:** *filename* [**activate commit**]
3. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**install add file location:** *filename* [**activate commit**] **Example:** `Device#install add file bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin activate commit`	Copies the software install package from a local or remote location (through FTP, HTTP, HTTPs, or TFTP) to the platform and extracts the individual components of the .package file into subpackages and packages.conf files. It also performs a validation and compatibility check for the platform and image versions, activates the package, and commits the package to make it persistent across reloads. The platform reloads after this command is run.
Step 3	**exit** **Example:** `Device#exit`	Exits privileged EXEC mode and returns to user EXEC mode.

Three step installation

Note

- All the CLI actions (for example, add, activate, and so on) are executed on all the available FRUs.
- The configuration save prompt will appear if an unsaved configuration is detected.
- The reload prompt will appear after the install activate step in this workflow. Use the **prompt-level none** keyword to automatically ignore the confirmation prompts.

The three-step installation procedure can be used only after the platform is in install mode. This option provides more flexibility and control to the customer during installation.

This procedure uses individual **install add**, **install activate**, and **install commit** commands for installing a software package, and to upgrade the platform to a new version.

SUMMARY STEPS

1. **enable**
2. **install add file location:** *filename*
3. **show install summary**
4. **install activate** [**auto-abort-timer** <*time*>]
5. **install abort**
6. **install commit**
7. **install rollback to committed**
8. **install remove** {**file** *filesystem: filename* | **inactive**}
9. **show install summary**
10. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**install add file location:** *filename* **Example:** `Device#install add file bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin`	Copies the software install package from a remote location (through FTP, HTTP, HTTPs, or TFTP) to the platform, and extracts the individual components of the .package file into subpackages and packages.conf files.
Step 3	**show install summary** **Example:** `Device#show install summary`	(Optional) Provides an overview of the image versions and their corresponding install state for all the FRUs.

	Command or Action	Purpose
Step 4	**install activate** [**auto-abort-timer** <*time*>] **Example:** `Device# install activate auto-abort-timer 120`	Activates the previously added package and reloads the platform. • When doing a full software install, do not provide a package filename. • In the three-step variant, **auto-abort-timer** starts automatically with the **install activate** command; the default for the timer is 120 minutes. If the **install commit** command is not run before the timer expires, the install process is automatically terminated. The platform reloads and boots up with the last committed version.
Step 5	**install abort** **Example:** `Device#install abort`	(Optional) Terminates the software install activation and returns the platform to the last committed version. • Use this command only when the image is in activated state, and not when the image is in committed state.
Step 6	**install commit** **Example:** `Device#install commit`	Commits the new package installation and makes the changes persistent over reloads.
Step 7	**install rollback to committed** **Example:** `Device#install rollback to committed`	(Optional) Rolls back the platform to the last committed state.

Step 8	**install remove** {**file** *filesystem: filename* | **inactive**}
	Example:
	`Device#install remove inactive`
		(Optional) Deletes software installation files.
		• **file**: Deletes a specific file
		• **inactive**: Deletes all the unused and inactive installation files.

Step 9	**show install summary** **Example:** `Device#show install summary`	(Optional) Displays information about the current state of the system. The output of this command varies according to the **install** commands run prior to this command.
Step 10	**exit** **Example:** `Device#exit`	Exits privileged EXEC mode and returns to user EXEC mode.

Upgrade in the install mode

Use either the one-step installation or the three-step installation to upgrade the platform in install mode.

Downgrade in the install mode

Use the **install rollback** command to downgrade the platform to a previous version by pointing it to the appropriate image, provided the image you are downgrading to was installed in install mode.

The **install rollback** command reloads the platform and boots it with the previous image.

Note The **install rollback** command succeeds only if you have not removed the previous file using the **install remove inactive** command.

Alternatively, you can downgrade by installing the older image using the **install** commands.

Terminate a software installation

You can terminate the activation of a software package in the following ways:

- When the platform reloads after activating a new image, the auto-abort-timer is triggered (in the three-step install variant). If the timer expires before issuing the **install commit** command, the installation process is terminated, and the platform reloads and boots with the last committed version of the software image.

  Alternatively, use the **install auto-abort-timer stop** command to stop this timer, without using the **install commit** command. The new image remains uncommitted in this process.

- Using the **install abort** command returns the platform to the version that was running before installing the new software. Use this command before issuing the **install commit** command.

Configuration examples for installing the software using install commands

The following is an example of the one-step installation or converting from bundle mode to install mode:

```
Router#install add file bootflash:c81g2be-universalk9.17.18.01a.SPA.bin activate commit

*Aug 28 02:08:20.193: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
add_activate_commit
bootflash:c81g2be-universalk9.17.18.01a.SPA.bininstall_add_activate_commit: START Thu Aug
28 02:08:20 UTC 2025
install_add: START Thu Aug 28 02:08:20 UTC 2025
install_add: Adding IMG
--- Starting initial file syncing ---
Copying bootflash:c81g2be-universalk9.17.18.01a.SPA.bin from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
Checking status of Add on [R0]
Add: Passed on [R0]
Image added. Version: 17.18.01a.0.182
```

```
Finished Add

install_activate: START Thu Aug 28 02:08:28 UTC 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c81g2be-firmware_device_mcu.17.18.01a.SPA.pkg
/bootflash/c81g2be-mono-universalk9.17.18.01a.SPA.pkg
/bootflash/c81g2be-firmware_pse_si3470a.17.18.01a.SPA.pkg
/bootflash/c81g2be-rpboot.17.18.01a.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]
*Aug 28 02:08:28.832: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
activate NONEy

--- Starting Activate ---
Performing Activate on all members

 [1] Activate package(s) on  R0

*Aug 28 02:08:59.279: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds
Warning: Booting with bundle mode will be deprecated in the near future. Migration to install
 mode is required.
Building configuration...
[OK]
*Aug 28 02:09:13.122: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
 file [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
 [1] Commit package(s) on  R0
 [1] Finished Commit on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_add_activate_commit Thu Aug 28 02:09:30 UTC 2025

Router#
*Aug 28 02:09:30.058: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 add_activate_commitAug 28 02:09:

[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]

Warning: MFG Key Enabled !!!

System Bootstrap, Version 17.18(1r), RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8161-G2 platform with 8388608 Kbytes of main memory
Warning: MFG key enabled, bypassing BIOS protection feature
......
Located bootflash:packages.conf
#

Package header rev 3 structure detected
IsoSize = 0
Performing Integrity Check ...
Performing Signature Verification ...
Image validated
Aug 28 02:11:30.058: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Router#show version
Cisco IOS XE Software, Version 17.18.01a
Cisco IOS Software [IOSXE], c81g2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.18.1a, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 15-Aug-25 07:05 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: 17.18(1r)

Router uptime is 3 days, 26 minutes
Uptime for this control processor is 3 days, 27 minutes
```

The following is an example of the three-step installation:

```
Router#install add file bootflash:c81g2be-universalk9.17.18.01a.SPA.bin

*Sep  1 12:46:01.370: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install add
 bootflash:c81g2be-universalk9.17.18.01a.SPA.bininstall_add: START Mon Sep 01 12:46:01 UTC
 2025
install_add: Adding IMG
--- Starting initial file syncing ---
Copying bootflash:c81g2be-universalk9.17.18.01a.SPA.bin from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
Checking status of Add on [R0]
Add: Passed on [R0]
Image added. Version: 17.18.01a.0.182

Finished Add

SUCCESS: install_add /bootflash/c81g2be-universalk9.17.18.01a.SPA.bin Mon Sep 01 12:47:03
UTC 2025

Router#
*Sep  1 12:47:03.698: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 add bootflash:/c81g2be-universalk9.17.18.01a.SPA.bin

Router#show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
```

```
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.17.01.0.6
IMG   I    17.18.01a.0.182

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------

Router#install activate

*Sep  1 12:53:48.533: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
activate NONEinstall_activate: START Mon Sep 01 12:53:48 UTC 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c81g2be-firmware_device_mcu.17.18.01a.SPA.pkg
/bootflash/c81g2be-mono-universalk9.17.18.01a.SPA.pkg
/bootflash/c81g2be-firmware_pse_si3470a.17.18.01a.SPA.pkg
/bootflash/c81g2be-rpboot.17.18.01a.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members

 [1] Activate package(s) on  R0

*Sep  1 12:55:55.135: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

SUCCESS: install_activate Mon Sep 01 12:56:07 UTC 2025

Router#
*Sep  1 12:56:07.855: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 activate

[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]

Warning: MFG Key Enabled !!!

System Bootstrap, Version 17.18(1r), RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8161-G2 platform with 8388608 Kbytes of main memory
Warning: MFG key enabled, bypassing BIOS protection feature
......
Located bootflash:packages.conf
#

Package header rev 3 structure detected
IsoSize = 0
Performing Integrity Check ...
Performing Signature Verification ...
Image validated
Sep  1 12:58:00.562: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Router# install commit
*Sep  1 13:01:30.773: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
```

```
commitinstall_commit: START Mon Sep 01 13:01:30 UTC 2025
--- Starting Commit ---
Performing Commit on all members
 [1] Commit packages(s) on  R0
 [1] Finished Commit packages(s) on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_commit Mon Sep 01 13:01:34 UTC 2025

Router#
*Sep  1 13:01:34.870: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 commit

Router#show version
Cisco IOS XE Software, Version 17.18.01a
Cisco IOS Software [IOSXE], c81g2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.18.1a, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 15-Aug-25 07:05 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: 17.18(1r)

Router uptime is 48 minutes
Uptime for this control processor is 49 minutes
System returned to ROM by Image Install
System image file is "bootflash:packages.conf"
Last reload reason: Image Install



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.


Technology Package License Information:

-----------------------------------------------------------------
```

```
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
-----------------------------------------------------------------
Smart License  Perpetual    essentials         essentials

The current crypto throughput level is 250000 kbps (Aggregate)


Smart Licensing Status: Smart Licensing Using Policy

cisco C8161-G2 (1RU) processor with 1901039K/6147K bytes of memory.
Processor board ID FGL2909L1MK
Router operating mode: Autonomous
1 Virtual Ethernet interface
10 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
18271231K bytes of flash memory at bootflash:.

Configuration register is 0x2102
```

The following is an example of terminating the software install activation:

```
Router#install add file bootflash:c81g2be-universalk9.17.17.01eftr3.SPA.bin

*Sep  1 07:03:03.363: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install add
 bootflash:c81g2be-universalk9.17.17.01eftr3.SPA.bininstall_add: START Mon Sep 01 07:03:03
 UTC 2025
install_add: Adding IMG


--- Starting initial file syncing ---
Copying bootflash:c81g2be-universalk9.17.17.01eftr3.SPA.bin from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members

*Sep  1 07:03:57.186: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Sep  1 07:03:58.187: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
 changed state to upChecking status of Add on [R0]
Add: Passed on [R0]
Image added. Version: 17.17.01.0.6

Finished Add

SUCCESS: install_add /bootflash/c81g2be-universalk9.17.17.01eftr3.SPA.bin Mon Sep 01 07:04:03
 UTC 2025

Router#
*Sep  1 07:04:03.635: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 add bootflash:/c81g2be-universalk9.17.17.01eftr3.SPA.bin

Router#install activate

*Sep  1 10:18:41.330: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
activate NONEinstall_activate: START Mon Sep 01 10:18:41 UTC 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c81g2be-firmware_device_mcu.17.17.01eftr3.SPA.pkg
/bootflash/c81g2be-rpboot.17.17.01eftr3.SPA.pkg
/bootflash/c81g2be-firmware_pse_si3470a.17.17.01eftr3.SPA.pkg
```

```
/bootflash/c81g2be-mono-universalk9.17.17.01eftr3.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members

 [1] Activate package(s) on  R0



*Sep  1 10:20:36.317: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

SUCCESS: install_activate Mon Sep 01 10:20:48 UTC 2025

Router#
*Sep  1 10:20:48.628: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 activateSep  1

[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]

Warning: MFG Key Enabled !!!

System Bootstrap, Version 17.17.01eftr3, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8161-G2 platform with 8388608 Kbytes of main memory
Warning: MFG key enabled, bypassing BIOS protection feature
......
Located bootflash:packages.conf
#

Package header rev 3 structure detected
IsoSize = 0
Performing Integrity Check ...
Performing Signature Verification ...
Image validated
Sep  1 10:22:00.562: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Router#show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.18.01a.0.182
IMG   U    17.17.01.0.6

--------------------------------------------------------------------------------
Auto abort timer: active , time before rollback - 01:48:10
--------------------------------------------------------------------------------

Router>enable

Router#install abort
```

```
*Sep  1 10:35:41.477: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
cancelinstall_abort: START Mon Sep 01 10:35:41 UTC 2025

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Abort ---
Performing Abort on all members

 [1] Abort packages(s) on  R0


Checking status of Abort on [R0]
Abort: Passed on [R0]
Finished Abort operation

SUCCESS: install_abort Mon Sep 01 10:36:31 UTC 2025

Router#
*Sep  1 10:36:31.863: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 abort

Router#show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.18.01a.0.182

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

The following is an example of downgrading in install mode:

```
ROUTER# install add file bootflash:c81g2be-universalk9.17.17.01eftr3.SPA.bin activate commit


*Sep  1 13:51:06.918: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
add_activate_commit
bootflash:c81g2be-universalk9.17.17.01eftr3.SPA.bininstall_add_activate_commit: START Mon
Sep 01 13:51:06 UTC 2025
install_add: START Mon Sep 01 13:51:06 UTC 2025
install_add: Adding IMG
--- Starting initial file syncing ---
Copying bootflash:c81g2be-universalk9.17.17.01eftr3.SPA.bin from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
Checking status of Add on [R0]
Add: Passed on [R0]
Image added. Version: 17.17.01.0.6

Finished Add

install_activate: START Mon Sep 01 13:52:06 UTC 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c81g2be-firmware_device_mcu.17.17.01eftr3.SPA.pkg
/bootflash/c81g2be-rpboot.17.17.01eftr3.SPA.pkg
```

```
/bootflash/c81g2be-firmware_pse_si3470a.17.17.01eftr3.SPA.pkg
/bootflash/c81g2be-mono-universalk9.17.17.01eftr3.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]
*Sep  1 13:52:06.555: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
activate NONEy

--- Starting Activate ---
Performing Activate on all members

 [1] Activate package(s) on  R0

*Sep  1 13:54:03.583: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
 [1] Commit package(s) on  R0
 [1] Finished Commit on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_add_activate_commit Mon Sep 01 13:54:29 UTC 2025

Router#
*Sep  1 13:54:29.118: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 add_activate_commit


[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]

Warning: MFG Key Enabled !!!

System Bootstrap, Version 17.17.01eftr3, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8161-G2 platform with 8388608 Kbytes of main memory
Warning: MFG key enabled, bypassing BIOS protection feature
......
Located bootflash:packages.conf
#

Package header rev 3 structure detected
IsoSize = 0
Performing Integrity Check ...
Performing Signature Verification ...
Image validated
Sep  1 13:56:00.562: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Router>enable

Router#show version
Cisco IOS XE Software, Version 17.17.01eftr3
Cisco IOS Software [IOSXE], c81g2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.17.1eftr3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
```

```
Compiled Mon 03-Mar-25 05:51 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 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.
```

The following is an example of rolling back the platform to the last committed version

```
Router#show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.17.01.0.6

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------

Router#install rollback to committed
install_rollback: START Mon Sep 01 14:03:12 UTC 2025
install_rollback: Rolling back to committed

*Sep  1 14:03:12.114: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
rollback
This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Rollback ---
Performing Rollback on all members

 [1] Rollback package(s) on  R0
 [1] Finished Rollback package(s) on  R0
Checking status of Rollback on [R0]
Rollback: Passed on [R0]
Finished Rollback operation

SUCCESS: install_rollback Mon Sep 01 14:04:36 UTC 2025

Router#
*Sep  1 14:04:36.726: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 rollback


[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]

Warning: MFG Key Enabled !!!

System Bootstrap, Version 17.18(1r), RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8161-G2 platform with 8388608 Kbytes of main memory
```

```
Warning: MFG key enabled, bypassing BIOS protection feature
......
Located bootflash:packages.conf
#

Package header rev 3 structure detected
IsoSize = 0
Performing Integrity Check ...
Performing Signature Verification ...
Image validated
Sep  1 14:06:00.562: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Router#show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.18.01a.0.182

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

The following are sample outputs for show commands:

show install log

```
Router#show install log
[0|install_op_boot]: START Mon Sep  1 13:55:20 Universal 2025
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS  Mon Sep  1 13:55:21 Universal 2025
```

show install summary

```
Router#show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.18.01a.0.182

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

show install package *filesystem: filename*

```
Router#show install package bootflash:c81g2be-universalk9.17.18.01a.SPA.bin
  Package: c81g2be-universalk9.17.18.01a.SPA.bin
    Size: 770579420
    Timestamp:
  Canonical path: /bootflash/c81g2be-universalk9.17.18.01a.SPA.bin

    Raw disk-file SHA1sum:
      7ad1937824348118d3139d25e9f76974bdab836c
  Header size:     1084 bytes
  Package type:    30000
  Package flags:   0
  Header version:  3
```

```
Internal package information:
  Name: rp_super
  BuildTime: 2025-08-15_07.13
  ReleaseDate: 2025-08-15_06.47
  BootArchitecture: arm64
  RouteProcessor: device
  Platform: C81G2BE
  User: mcpre
  PackageName: universalk9
  Build: 17.18.01a
  CardTypes:

Package is bootable from media and tftp.
Package contents:

Package: c81g2be-mono-universalk9.17.18.01a.SPA.pkg
  Size: 690905088
  Timestamp:

  Raw disk-file SHA1sum:
    9f13173d385de7033ab5fd64fc81a80bce3749b1
  Header size:     4096 bytes
  Package type:    30000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: mono
    BuildTime: 2025-08-15_07.13
    ReleaseDate: 2025-08-15_06.47
    BootArchitecture: arm64
    RouteProcessor: device
    Platform: C81G2BE
    User: mcpre
    PackageName: mono-universalk9
    Build: 17.18.01a
    CardTypes:

  Package is bootable from media and tftp.
  Package contents:

Package: c81g2be-firmware_charon_mcu.17.18.01a.SPA.pkg
  Size: 200704
  Timestamp:

  Raw disk-file SHA1sum:
    6fdb949a0495d87dec59d77f6070e68bacb93024
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_device_mcu
    BuildTime: 2025-08-15_07.13
    ReleaseDate: 2025-08-15_06.47
    BootArchitecture: none
    RouteProcessor: device
    Platform: C81G2BE
    User: mcpre
    PackageName: firmware_device_mcu
    Build: 17.18.01a
    CardTypes:
```

```
    Package is not bootable.
  Package: c81g2be-firmware_pse_si3470a.17.18.01a.SPA.pkg
    Size: 49152
    Timestamp:

    Raw disk-file SHA1sum:
      cdde430bf4f45824743e7ae6bdacb7fca2216929
    Header size:     4096 bytes
    Package type:    40000
    Package flags:   0
    Header version:  3

    Internal package information:
      Name: firmware_pse_si3470a
      BuildTime: 2025-08-15_07.13
      ReleaseDate: 2025-08-15_06.47
      BootArchitecture: none
      RouteProcessor: device
      Platform: C81G2BE
      User: mcpre
      PackageName: firmware_pse_si3470a
      Build: 17.18.01a
      CardTypes:

    Package is not bootable.
```

show install active

```
Router#show install active
[ R0 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.18.01a.0.182

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

show install inactive

```
Router#show install inactive
[ R0 ] Inactive Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
No Inactive Packages
```

show install committed

```
Router#show install committed
[ R0 ] Committed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.18.01a.0.182

--------------------------------------------------------------------------------
```

```
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

show install uncommitted

```
Router#show install uncommitted
[ R0 ] Uncommitted Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
No Uncommitted Packages
```

Troubleshooting software installation using install commands

Problem Troubleshooting the software installation

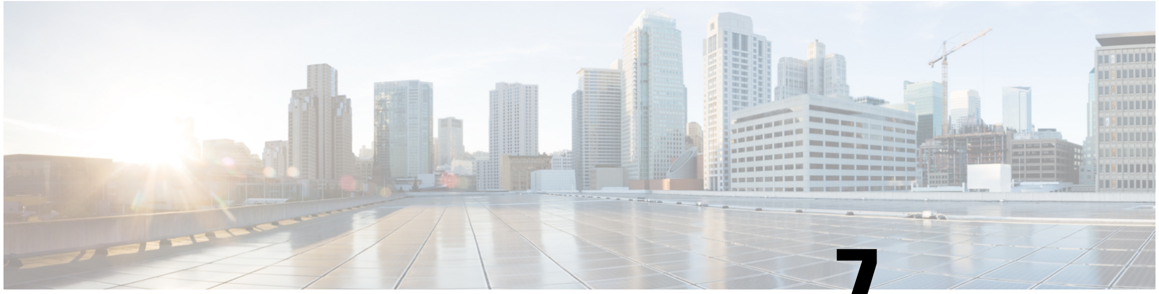
Solution Use the following show commands to view installation summary, logs, and software versions.

- **show install summary**
- **show install log**
- **show version**
- **show version running**

Problem Other installation issues

Solution Use the following commands to resolve installation issue:

- **dir** <*install directory*>
- **more location:***packages.conf*
- **show tech-support install**: this command automatically runs the **show** commands that display information specific to installation.
- **request platform software trace archive target bootflash** <*location*>: this command archives all the trace logs relevant to all the processes running on the system since the last reload, and saves this information in the specified location.



CHAPTER 7

Blue beacon LED

Introduction to blue beacon LED

The Blue Beacon LED is a visual indicator feature designed to assist you in physically identifying a specific router within a rack or data center.

The Blue Beacon LED, labeled **BEACON** on the front panel of Cisco 8100 Series Secure Routers, serves as a visual aid for users. Its primary function is to allow easy physical identification of a router that requires attention or is being operated. By turning this LED on or making it blink, you can quickly locate the specific device among many, especially in dense network environments.

The blue beacon LED feature operates with specific functionalities:

- The Blue Beacon LED can only be controlled via Command Line Interface (CLI). There is no physical button on the front panel to turn it on or off.
- Once the beacon is activated (turned on or set to blink) using the CLI, it remains in that state indefinitely until explicitly turned off by a subsequent CLI command. There is no built-in timeout mechanism to automatically reset the LED to the off state.
- After a router reload or reboot, the Blue Beacon LED always resets to its default **off** state, regardless of its state prior to the reload.

How to configure blue beacon LED

The Blue Beacon LED is controlled using a simple `hw-module` CLI command.

Turning the Beacon LED On (Blink)

To activate the Blue Beacon LED and make it blink for identification purposes, use this command:

```
Router# hw-module beacon R0 on
```

Turning the Beacon LED Off

To deactivate the Blue Beacon LED and turn it off, use this command:

```
Router# hw-module beacon R0 off
```

Get the Beacon LED status

To get the Blue Beacon LED status, use this command:

```
Router# hw-module beacon R0 status
```

Examples

To activate the Blue Beacon LED, connect to the router via console or SSH and execute the command:

```
Router# hw-module beacon blink
```

After executing this command, the BEACON LED on the front panel of the router starts blinking blue, allowing you to easily locate it physically.

To deactivate the Blue Beacon LED, after completing the necessary tasks on router, you can turn it off using:

```
Router# hw-module beacon off
```

The Blue Beacon LED on the front panel is now turned off.

Behavior after router reloads

When the Blue Beacon LED was set to blink on the router, if the router needs to be reloaded or powered cycled:

```
Router# reload
```

Once the router finishes its boot-up sequence and comes back online, the Blue Beacon LED automatically goes in the **off** state, regardless of its previous **blink** state. You would need to re-issue the **hw-module beacon blink** command if you need to activate it again.

CHAPTER 8

Configure ROMMON

This chapter contains the following sections:

ROMmon images

A ROMmon image is a software package used by ROM Monitor (ROMmon) software on a router. The software package is separate from the consolidated package normally used to boot the router. For more information on ROMmon, see the "ROM Monitor Overview and Basic Procedures" section in the Cisco 8100 Series Secure Routers Hardware Installation Guide.

An independent ROMmon image (software package) may occasionally be released and the router can be upgraded with the new ROMmon software. For detailed instructions, see the documentation that accompanies the ROMmon image.

Note A new version of the ROMmon image is not necessarily released at the same time as a consolidated package for a router.

Table 10: Cisco 8100 Series Secure Routers ROMmon compatibility matrix

Cisco IOS XE release	Minimum ROMmon release supported for IOS XE	Recommended ROMmon release supported for IOS XE
17.18.x	17.18(1r)	17.18(1r)

Note The ROMmon image is not available for download on software.cisco.com:

Instead the ROMmon image is bundled along with the IOS XE image. When you install the IOS XE image, if the version of ROMmon bundled is higher than the existing version of ROMmon, an upgrade is performed automatically.

CHAPTER 9

Basic router configuration

This chapter contains the following sections:

Default configuration

When you boot up the router for the first time, the router looks for a default file name-the PID of the router. For example, C8161-G2 looks for a file named **C8161-G2.cfg**. The Cisco 8100 Series Secure Routers looks for this file before finding the standard files-**router-confg** or the **ciscortr.cfg**.

The C8161-G2 looks for a file named **C8161-G2.cfg** file in the bootflash. If the file is not found in the bootflash, the router then looks for the standard files-**router-confg** and **ciscortr.cfg**. If none of the files are found, the router then checks for any inserted USB that may have stored these files in the same particular order.

Note If there is a configuration file with the PID as its name in an inserted USB, but one of the standard files are in bootflash, the system finds the standard file for use.

Use the **show running-config** command to view the initial configuration, as shown in the following example:

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

Current configuration : 6118 bytes
!
! Last configuration change at 18:09:54 UTC Tue Sep 9 2025
!
version 17.18
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform resource service-plane-heavy
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
!
!
aaa session-id common
!
!
!
!
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
!
!
!
!
!
!
!
!
product-analytics
!
!
crypto pki trustpoint TP-self-signed-303776382
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-303776382
 revocation-check none
 rsakeypair TP-self-signed-303776382
 hash sha512
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha512
!
!
crypto pki certificate chain TP-self-signed-303776382
 certificate self-signed 01
```

```
  3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
  30312E30 2C060355 04030C25 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303337 37363338 32301E17 0D323530 38323730 36303931
  315A170D 33353038 32373036 30393131 5A303031 2E302C06 03550403 0C25494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3330 33373736
  33383230 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
  82010100 B2521F68 C09E24B1 89E40B24 853626B1 7F3F531D 6D02C649 66F1BD76
  8D5E402E 96D34B24 94E7FFE6 3CDFE83B C5FF2734 BCB5C95B 96A8470F F73A5DD4
  7F5CEF51 17BF69F9 61E8921D 4DB29641 DEA5DC94 DEEEF577 F8BC38AF 5EDA4DFD
  7BEC6B6F 22B387E9 228C26B8 24E6874F 15E37DDE 2DACAB5B CE9145A7 D927CC5F
  E406C5FB E0644A0A 5DD223AA D7BE44A3 9BECB90B 770B033E 31F3D7F3 818BF19A
  7249E78C F746D6B0 E2ECD2CC C6338E9D 67292CC0 2B4C0C5E 2FBE57A0 CCBBDF1B
  C0732BC7 55D55A5D AC2C8511 F9AEE8DE F36678A2 08B4693D 5325AB35 A67724F8
  CCC604BA C0D2BB14 E26CC9C4 50B9818E F311FE57 F397FD1A FCAE2041 A1B2DDEC
  79EB45C1 02030100 01A35330 51301D06 03551D0E 04160414 0AB72B54 4F5A1C91
  6B4D0922 B5EB5529 24638466 301F0603 551D2304 18301680 140AB72B 544F5A1C
  916B4D09 22B5EB55 29246384 66300F06 03551D13 0101FF04 05300301 01FF300D
  06092A86 4886F70D 01010D05 00038201 0100A9D5 BAE37659 4226FF9A 59835CAC
  9ECC9170 BCCC78AE EE48674A DFCF359C AD363065 61706435 50E96ACB 82B30090
  6A417C53 4E7E9000 77AAAC84 887A5006 E1DE278B 0F3B59DF 306A6240 7344AE5B
  C8B75372 EDEB27A4 E4497541 D67ECD79 97F5910A 17181502 CE1417BE 867C2151
  8CBE3380 8BE23C6A BC633AAB 252491A5 E3B40685 F5AE5AFE 3184884D AD0AEA0F
  BA2EC3D7 3C8BF748 84BFF882 99DA3471 11BE6758 29144FC9 18CAE5FB 2399743C
  30FC8AFC 84E61852 BAEA0CD7 14B13BC3 67D58D25 5408266B 2A442399 926169A0
  4ADBE01B F7F7F790 075B37D7 C2B9EDCF 3427C015 9401B552 3DE68D26 88B24C19
  FDF935A7 9CB0CD21 273FBF2C 77BC31CF 080F
        quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
!
!
!
!
!
!
!
!
```

```
!
diagnostic bootup level minimal
!
license udi pid C8161-G2 sn FCW2832Y4YB
memory free low-watermark processor 63127
!
spanning-tree extend system-id
!
!
!
!
redundancy
 mode none
!
!
!
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0/1/4
!
interface GigabitEthernet0/1/5
!
interface GigabitEthernet0/1/6
```

```
 switchport
!
interface GigabitEthernet0/1/7
 switchport
!
interface Vlan1
 no ip address
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
ip forward-protocol nd
ip forward-protocol udp
ip http server
ip http authentication local
ip http secure-server
!
ip ssh bulk-mode 131072
!
!
!
!
!
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
line con 0
 activation-character 13
 stopbits 1
line vty 0 4
 activation-character 13
 transport input ssh
line vty 5 14
 activation-character 13
 transport input ssh
!
!
!
!
!
!
!
```

Configuring global parameters

To configure the global parameters for your router, follow these steps.

SUMMARY STEPS

1. **configure terminal**
2. **hostname** *name*
3. **enable password** *password*
4. **no ip domain-lookup**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`Router> enable`
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode when using the console port.
		Use the following to connect to the router with a remote terminal:
		`telnet router-name or address`
		`Login: login-id`
		`Password: *********`
		`Router> enable`

Step 2	**hostname** *name* **Example:** `Router(config)# hostname Router`	Specifies the name for the router.
Step 3	**enable password** *password* **Example:** `Router(config)# enable password cr1ny5ho`	Specifies a password to prevent unauthorized access to the router. **Note** In this form of the command, password is not encrypted.
Step 4	**no ip domain-lookup** **Example:** `Router(config)# no ip domain-lookup`	Disables the router from translating unfamiliar words (typos) into IP addresses. For complete information on global parameter commands, see the Cisco IOS Release Configuration Guide documentation set.

Configuring gigabit ethernet interfaces

To manually define onboard Gigabit Ethernet interfaces, follow these steps, beginning from global configuration mode.

SUMMARY STEPS

1. **interface** *slot/bay/port*
2. **ip address** *ip-address mask*
3. **ipv6 address** *ipv6-address/prefix*
4. **no shutdown**
5. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**interface** *slot/bay/port* **Example:** `Router(config)# interface 0/0/1`	Enters the configuration mode for an interface on the router.
Step 2	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 192.0.2.2 255.255.255.0`	Sets the IP address and subnet mask for the specified interface. Use this Step if you are configuring an IPv4 address.
Step 3	**ipv6 address** *ipv6-address/prefix* **Example:** `Router(config-if)# ipv6 address 2001.db8::ffff:1/128`	Sets the IPv6 address and prefix for the specified interface. Use this step instead of Step 2, if you are configuring an IPv6 address.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface and changes its state from administratively down to administratively up.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the configuration mode of interface and returns to the global configuration mode.

Configuring a loopback interface

Before you begin

The loopback interface acts as a placeholder for the static IP address and provides default routing information.

To configure a loopback interface, follow these steps.

SUMMARY STEPS

1. **interface** *type number*
2. (Option 1) **ip address** *ip-address mask*
3. (Option 2) **ipv6 address** *ipv6-address/prefix*
4. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface Loopback 0`	Enters configuration mode on the loopback interface.
Step 2	(Option 1) **ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.10.1.1 255.255.255.0`	Sets the IP address and subnet mask on the loopback interface. (If you are configuring an IPv6 address, use the **ipv6 address** *ipv6-address/prefix* command described below.
Step 3	(Option 2) **ipv6 address** *ipv6-address/prefix* **Example:** `Router(config-if)# 2001:db8::ffff:1/128`	Sets the IPv6 address and prefix on the loopback interface.
Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the loopback interface and returns to global configuration mode.

The loopback interface in this sample configuration is used to support Network Address Translation (NAT) on the virtual-template interface. This configuration example shows the loopback interface configured on the Gigabit Ethernet interface with an IP address of 192.0.2.0/16, which acts as a static IP address. The loopback interface points back to virtual-template1, which has a negotiated IP address.

```
!
interface loopback 0
ip address 192.0.2.1 255.255.0.0 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
```

Verifying Loopback Interface Configuration

Enter the **show interface loopback** command. You should see an output similar to the following example:

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 192.0.2.0/16
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  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 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Alternatively, use the **ping** command to verify the loopback interface, as shown in the following example:

```
Router# ping 192.0.2.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.0, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Configuring command-line access

To configure parameters to control access to the router, follow these steps.

SUMMARY STEPS

1. **line** [**console** | **tty** | **vty**] *line-number*
2. **password** *password*
3. **login**
4. **exec-timeout** *minutes* [*seconds*]
5. **exit**
6. **line** [**console** | **tty** | **vty**] *line-number*

7. **password** `password`
8. **login**
9. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**line** [**console** | **tty** | **vty**] *line-number* **Example:** `Router(config)# line console 0`	Enters line configuration mode, and specifies the type of line. The example provided here specifies a console terminal for access.
Step 2	**password** *password* **Example:** `Router(config-line)# password 5dr4Hepw3`	Specifies a unique password for the console terminal line.
Step 3	**login** **Example:** `Router(config-line)# login`	Enables password checking at terminal session login.

Step 4	**exec-timeout** *minutes* [*seconds*]
	Example:
	`Router(config-line)# exec-timeout 5 30`
	`Router(config-line)#`
		Sets the interval during which the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, adds seconds to the interval value.
		The example provided here shows a timeout of 5 minutes and 30 seconds. Entering a timeout of **0 0** specifies never to time out.

Step 5	**exit** **Example:** `Router(config-line)# exit`	Exits line configuration mode to re-enter global configuration mode.

Step 6	**line** [**console** | **tty** | **vty**] *line-number*
	Example:
	`Router(config)# line vty 0 4`
	`Router(config-line)#`
		Specifies a virtual terminal for remote console access.

Step 7	**password** `password` **Example:** `Router(config-line)# password aldf2ad1`	Specifies a unique password for the virtual terminal line.

	Command or Action	Purpose
Step 8	**login** **Example:** `Router(config-line)# login`	Enables password checking at the virtual terminal session login.

Step 9	**end**
	Example:
	`Router(config-line)# end`
		Exits line configuration mode, and returns to privileged EXEC mode.

Example

The following configuration shows the command-line access commands.

You do not have to input the commands marked **default**. These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

```
!
line console 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

Configuring static routes

Static routes provide fixed routing paths through the network. They are manually configured on the router. If the network topology changes, the static route must be updated with a new route. Static routes are private routes unless they are redistributed by a routing protocol.

To configure static routes, follow these steps.

SUMMARY STEPS

1. (Option 1) **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. (Option 2) **ipv6 route** *prefix/mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]}
3. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	(Option 1) **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	Example:
	`Router(config)# ip route 192.0.2.1 255.255.0.0 10.10.10.2`
		Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the **ipv6 route** command described below.)

Step 2	(Option 2) **ipv6 route** *prefix/mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]}
	Example:
	`Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0`
		Specifies a static route for the IP packets.

Step 3	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and enters privileged EXEC mode.

In the following configuration example, the static route sends out all IP packets with a destination IP address of 192.168.1.0 and a subnet mask of 255.255.255.0 on the Gigabit Ethernet interface to another device with an IP address of 10.10.10.2. Specifically, the packets are sent to the configured PVC.

You do not have to enter the command marked **default**. This command appears automatically in the configuration file generated when you use the **running-config** command.

```
!
ip classless (default)
ip route 2001:db8:2::/64 2001:db8:3::0
```

Verifying Configuration

To verify that you have configured static routing correctly, enter the **show ip route** command (or **show ipv6 route** command) and look for static routes marked with the letter S.

When you use an IPv4 address, you should see verification output similar to the following:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, FastEthernet0
```

When you use an IPv6 address, you should see verification output similar to the following:

```
Router# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       ls - LISP site, ld - LISP dyn-EID, a - Application

C   2001:DB8:3::/64 [0/0]
       via GigabitEthernet0/0/2, directly connected
S   2001:DB8:2::/64 [1/0]
       via 2001:DB8:3::1
```

Configuring dynamic routes

In dynamic routing, the network protocol adjusts the path automatically, based on network traffic or topology. Changes in dynamic routes are shared with other routers in the network.

A router can use IP routing protocols, such as Routing Information Protocol (RIP) or Enhanced Interior Gateway Routing Protocol (EIGRP), to learn about routes dynamically.

Configuring routing information protocol

To configure the RIP on a router, follow these steps.

SUMMARY STEPS

1. **router rip**
2. **version** {**1** | **2**}
3. **network** *ip-address*
4. **no auto-summary**
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**router rip** **Example:**	Enters router configuration mode, and enables RIP on the router.

	Command or Action	Purpose
	`Router(config)# router rip`	

Step 2	**version** {**1** | **2**}
	Example:
	`Router(config-router)# version 2`
		Specifies use of RIP version 1 or 2.

Step 3	**network** *ip-address*
	Example:
	`Router(config-router)# network 192.168.1.1`
	`Router(config-router)# network 10.10.7.1`
		Specifies a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.

Step 4	**no auto-summary** **Example:** `Router(config-router)# no auto-summary`	Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classful network boundaries.

Step 5	**end**
	Example:
	`Router(config-router)# end`
		Exits router configuration mode, and enters privileged EXEC mode.

The following configuration example shows RIP Version 2 enabled in IP networks 10.0.0.0 and 192.168.1.0. To see this configuration, use the **show running-config** command from privileged EXEC mode.

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

Current configuration : 6118 bytes
!
! Last configuration change at 18:09:54 UTC Tue Sep 9 2025
!
version 17.18
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform resource service-plane-heavy
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
!
!
```

```
aaa session-id common
!
!
!
!
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
!
!
!
!
!
!
!
!
product-analytics
!
!
crypto pki trustpoint TP-self-signed-303776382
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-303776382
 revocation-check none
 rsakeypair TP-self-signed-303776382
 hash sha512
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha512
!
!
crypto pki certificate chain TP-self-signed-303776382
 certificate self-signed 01
  3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
  30312E30 2C060355 04030C25 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303337 37363338 32301E17 0D323530 38323730 36303931
  315A170D 33353038 32373036 30393131 5A303031 2E302C06 03550403 0C25494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3330 33373736
  33383230 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
  82010100 B2521F68 C09E24B1 89E40B24 853626B1 7F3F531D 6D02C649 66F1BD76
  8D5E402E 96D34B24 94E7FFE6 3CDFE83B C5FF2734 BCB5C95B 96A8470F F73A5DD4
  7F5CEF51 17BF69F9 61E8921D 4DB29641 DEA5DC94 DEEEF577 F8BC38AF 5EDA4DFD
  7BEC6B6F 22B387E9 228C26B8 24E6874F 15E37DDE 2DACAB5B CE9145A7 D927CC5F
  E406C5FB E0644A0A 5DD223AA D7BE44A3 9BECB90B 770B033E 31F3D7F3 818BF19A
  7249E78C F746D6B0 E2ECD2CC C6338E9D 67292CC0 2B4C0C5E 2FBE57A0 CCBBDF1B
  C0732BC7 55D55A5D AC2C8511 F9AEE8DE F36678A2 08B4693D 5325AB35 A67724F8
  CCC604BA C0D2BB14 E26CC9C4 50B9818E F311FE57 F397FD1A FCAE2041 A1B2DDEC
  79EB45C1 02030100 01A35330 51301D06 03551D0E 04160414 0AB72B54 4F5A1C91
  6B4D0922 B5EB5529 24638466 301F0603 551D2304 18301680 140AB72B 544F5A1C
  916B4D09 22B5EB55 29246384 66300F06 03551D13 0101FF04 05300301 01FF300D
  06092A86 4886F70D 01010D05 00038201 0100A9D5 BAE37659 4226FF9A 59835CAC
  9ECC9170 BCCC78AE EE48674A DFCF359C AD363065 61706435 50E96ACB 82B30090
  6A417C53 4E7E9000 77AAAC84 887A5006 E1DE278B 0F3B59DF 306A6240 7344AE5B
  C8B75372 EDEB27A4 E4497541 D67ECD79 97F5910A 17181502 CE1417BE 867C2151
  8CBE3380 8BE23C6A BC633AAB 252491A5 E3B40685 F5AE5AFE 3184884D AD0AEA0F
  BA2EC3D7 3C8BF748 84BFF882 99DA3471 11BE6758 29144FC9 18CAE5FB 2399743C
  30FC8AFC 84E61852 BAEA0CD7 14B13BC3 67D58D25 5408266B 2A442399 926169A0
  4ADBE01B F7F7F790 075B37D7 C2B9EDCF 3427C015 9401B552 3DE68D26 88B24C19
  FDF935A7 9CB0CD21 273FBF2C 77BC31CF 080F
        quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
!
!
!
!
!
!
!
!
!
diagnostic bootup level minimal
!
license udi pid C8161-G2 sn FCW2832Y4YB
memory free low-watermark processor 63127
!
spanning-tree extend system-id
!
!
!
!
redundancy
 mode none
```

```
!
!
!
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0/1/4
!
interface GigabitEthernet0/1/5
!
interface GigabitEthernet0/1/6
 switchport
!
interface GigabitEthernet0/1/7
 switchport
!
interface Vlan1
 no ip address
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
```

```
!
ip forward-protocol nd
ip forward-protocol udp
ip http server
ip http authentication local
ip http secure-server
!
ip ssh bulk-mode 131072
!
!
!
!
!
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
line con 0
 activation-character 13
 stopbits 1
line vty 0 4
 activation-character 13
 transport input ssh
line vty 5 14
 activation-character 13
 transport input ssh
!
!
!
!
!
!
!
end

Router#
```

Verifying Configuration

To verify that you have configured RIP correctly, enter the **show ip route** command and look for RIP routes marked with the letter R. You should see an output similar to the one shown in the following example:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
R    192.0.2.2/8 [120/1] via 192.0.2.1, 00:00:02, Ethernet0/0/0
```

Configuring enhanced interior gateway routing protocol

To configure Enhanced Interior Gateway Routing Protocol (EIGRP), follow these steps.

SUMMARY STEPS

1. **router eigrp** *as-number*
2. **network** *ip-address*
3. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 109`	Enters router configuration mode, and enables EIGRP on the router. The autonomous system number identifies the route to other EIGRP routers and is used to tag the EIGRP information.

Step 2	**network** *ip-address*
	Example:
	`Router(config)# network 192.168.1.0`
	`Router(config)# network 10.10.12.115`
		Specifies a list of networks on which EIGRP is to be applied, using the IP address of the network of directly connected networks.

Step 3	**end**
	Example:
	`Router(config-router)# end`
		Exits router configuration mode, and enters privileged EXEC mode.

Example

The following configuration example shows the EIGRP routing protocol enabled in IP networks 192.168.1.0 and 10.10.12.115. The EIGRP autonomous system number is 109. To see this configuration, use the **show running-config** command.

```
Router# show running-config
.
.
.
!
router eigrp 109
```

```
 network 192.168.1.0
  network 10.10.12.115
!
.
.
.
```

Verifying Configuration

To verify that you have configured IP EIGRP correctly, enter the **show ip route** command, and look for EIGRP routes marked by the letter D. You should see verification output similar to the following:

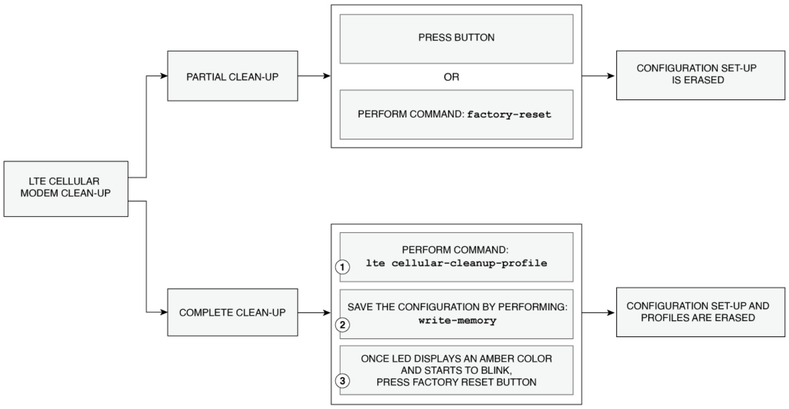
```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D     3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```

Erase configuration setup and cellular profiles on LTE modems

When using a cellular LTE modem, users have the option to perform a clean-up on the device. There are two types of clean-ups available for users: partial and complete.

A partial clean-up will remove the configuration set-up, while leaving user profiles intact. On the other hand, a complete clean-up will wipe the device of both configuration and profiles present in the modem.

It is up to the user to decide which clean-up option best suits their needs. The figure below shows the two types of clean-ups available for users:


LTE CELLULAR MODEM CLEAN-UP
PARTIAL CLEAN-UP
PRESS BUTTON
OR
PERFORM COMMAND: factory-reset
CONFIGURATION SET-UP IS ERASED
COMPLETE CLEAN-UP
1 PERFORM COMMAND: lte cellular-cleanup-profile
2 SAVE THE CONFIGURATION BY PERFORMING: write-memory
3 ONCE LED DISPLAYS AN AMBER COLOR AND STARTS TO BLINK, PRESS FACTORY RESET BUTTON
CONFIGURATION SET-UP AND PROFILES ARE ERASED

Partial clean-up

The partial clean-up of an LTE cellular device involves removing the existing IOS XE configuration to ensure optimal clean-up of the device before it is repurposed.

There are two ways to enable the partial clean-up process: by pressing the factory reset button or by configuring the **factory-reset** command.

Prerequisites for erasing the configuration set-up

- Pressing the button: When the Router boots up, the LED displays an Amber color and starts to blink, take a pin or a toothpick and gently press on factory reset button for about 10 to 20 seconds.
- There are no pre-requisites before performing the **factory-reset** command.

Restrictions partial clean-up

- When using the partial clean-up method on a cellular LTE modem, only the configuration setup will be erased, leaving the profiles intact on the device.

Configuring partial cellular modem clean-up

Before you begin

Performing the **factory-reset** command is one of the ways to partially erase profiles on a cellular modem. Here are the steps:

SUMMARY STEPS

1. **configure terminal**
2. **factory-reset**
3. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`Router> enable`
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 2	**factory-reset**
	Example:
	`Router#factory-reset ?`
	`all  All factory reset operations`
		Performs a partial clean-up of the cellular modem that erases the configuration setup.

	Command or Action	Purpose

	`keep-licensing-info Keep license usage info`
	`Router#`**`factory-reset`**	

Step 3	**exit** **Example:** `Router(config-if)#` **`exit`**	Exits the configuration mode.

The following configuration example shows partial clean-up of the cellular modem that erases the configuration set-up:

```
Router#factory-r
Router#factory-reset ?
  all                  All factory reset operations
  keep-licensing-info  Keep license usage info
```

CHAPTER 10

Factory reset

This chapter describes Factory Reset feature and how it can be used to protect or restore a router to an earlier, fully functional state.

Information about factory reset

Factory Reset is a process of clearing the current running and start-up configuration information on a device, and resetting the device to an earlier, fully-functional state.

The factory reset process uses the **factory-reset all** command to take backup of existing configuration and resets the router to an earlier fully functional state. The duration of the factory reset process is dependent on the storage size of the router. It varies from 10 to 30 minutes on Cisco 8100 Series Secure Routers .

From Cisco IOS XE 17.18.x release and later, you can use the **factory-reset all secure** command to reset the router and securely clear the files stored in the bootflash memory.

There are several memory components in the device(s), as listed for the Cisco 8100 Series Secure Routers as an example in the following table.

Device or Component	Type	Volatility	Purpose	Data Sanitization
DDR5 Memory On-board	RAM	Volatile	Running system software	All data is removed from DRAM when power is turned off.
TPM	NVRAM	Nonvolatile	Secure boot key and board info	See below
Power Sequencer	NVRAM	Nonvolatile	Power sequencer configuration file	N/A

Device or Component	Type	Volatility	Purpose	Data Sanitization
IO MCU	NVRAM	Nonvolatile	IO MCU configuration file	N/A
SPI NOR FLASH	PROM	Nonvolatile	Boot ROM (ROMMON)	See below.
0.85 V VRM	NVRAM	Nonvolatile	VRM configuration file	N/A
eMMC module	NVRAM	Nonvolatile	Boot OS, OS file system, system configuration	See below.
Clock generator	NVRAM	Nonvolatile	Clock generator configuration file	N/A
PoE controller (C8161-G2 only)	NVRAM	Nonvolatile	PoE configuration file	N/A

	C8130-G2	C8140-G2	C8151-G2	C8161-G2
DDR5 Memory On-board	4GB	4GB	8GB	8GB
TPM	N/A	N/A	N/A	N/A
Power Sequencer	256K	256K	256K	256K
IO MCU	256K	256K	256K	256K
SPI NOR FLASH	256Mb	256Mb	256Mb	256Mb
0.85 V VRM	N/A	N/A	N/A	N/A
eMMC module	16GB	16GB	16GB	16GB
Clock generator	N/A	N/A	N/A	N/A
PoE controller (C8161-G2 only)	N/A	N/A	N/A	N/A

DDR5 Memory (On-Board)

- Volatile memory
- No user data exists on DRAM after power-off.
- Sanitization measures not required.

SPI NOR Flash

- Non-volatile memory
- Holds user data after power-off.

Configuring the **factory-reset all** command is the most common method used to erase customer data from the router’s memory resources. Factory reset will clear the current running and start-up configuration information.

From Cisco IOS XE 17.18.1a and later, the **factory-reset all secure** command will also clear the data held in SPI NOR FLASH in the same manner as the **factory-reset all** command.

From Cisco IOS XE 17.18.1a, the factory-reset all secure command will clear the data held in SPI NOR FLASH including the config-register and ROMMON variables.

```
factory-reset keep licensing-info: yes
factory-reset all: yes
factory-reset all secure 3-pass: yes
factory-reset all secure 7-pass: yes
factory-reset all secure: yes
```

eMMC Boot Flash/NVRAM

- Non-volatile memory
- Holds user data after power-off.

A factory reset, **factory-reset all** command, is the most common method used when erasing customer data from the router’s memory resources. Factory reset will clear the current running and startup configuration information, thereby resetting the router to a fully functional state as it was shipped from factory.

As of Cisco IOS XE 17.18.1a and later, the **factory-reset all secure** command to reset the router and securely clear the files stored in the eMMC Boot Flash /NVRAM.

```
factory-reset keep licensing-info: yes
factory-reset all: yes
factory-reset all secure 3-pass: yes
factory-reset all secure 7-pass: yes
factory-reset all secure: yes
```

TPM

- Non-volatile memory
- Holds user data after power-off.

From Cisco IOS XE 17.18.1a, a factory reset command, **factory-reset all secure** unlinks customer data in the TPM and makes it unreadable by host, including the dev keys installed by consent-token. But you can keep the manufacturing install data like, SUDI, cookies.

```
factory-reset keep licensing-info: no
factory-reset all: no
factory-reset all secure 3-pass: no
factory-reset all secure 7-pass: no
factory-reset all secure: yes, but keep the manufacturing installed data
```

After the factory reset process is complete, the router reboots to ROMMON mode.

Software and hardware support for factory reset

- Factory Reset process is supported on standalone routers as well as on routers configured for high availability.

Prerequisites for performing factory reset

- Ensure that all the software images, configurations and personal data are backed up before performing factory reset.
- Ensure that there is uninterrupted power supply when factory reset is in progress.
- The **factory-reset all secure** command erases all files, including the boot image.

Restrictions for performing a factory reset

- Any software patches that are installed on the router are not restored after the factory reset operation.
- The CLI command "factory-reset all secure" is only supported in the console, not in the Virtual Teletype (VTY).

When to perform factory reset

- Return Material Authorization (RMA): If a router is returned back to Cisco for RMA, it is important that all sensitive information is removed.
- Router is compromised: If the router data is compromised due to a malicious attack, the router must be reset to factory configuration and then reconfigured once again for further use.
- Repurposing: The router needs to be moved to a new topology or market from the existing site to a different site.

How to perform a factory reset

Before you begin

Procedure

Step 1 Log in to a Cisco 8100 Series Secure Routers.

Step 2 This step is divided into two parts (a and b). If you need to retain the licensing information while performing the **factory-reset** command, follow step 2. a. If you do not need to retain licensing information and want all the data to be erased, perform step 2. b.

a) Execute **factory-reset keep-licensing-info** command to retain the licensing data.

The system displays the following message when you use the **factory-reset keep-licensing-info** command:

```
Router#factory-reset keep-licensing-info
The factory reset operation is irreversible for Keeping license usage. Are you sure? [confirm]

This operation may take 20 minutes or more. Please do not power cycle.


*Sep  1 14:40:09.827: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.Sep
 1




in the keep_lic_info_loop 2 3 6
Sep 01 14:40:39.835: Factory reset operation completed.


[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]


Warning: monitor Nvram area is corrupt ... using default values
Warning: MFG Key Enabled !!!

System Bootstrap, Version 17.18(1r), RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8161-G2 platform with 8388608 Kbytes of main memory
Warning: MFG key enabled, bypassing BIOS protection feature
rommon 1 >
```

b) Execute the **factory-reset all secure** command to securely erase all data.

Enter confirm to proceed with the factory reset.

The system displays the following message when you use the **factory-reset all secure** command:

```
Router#factory-reset all secure
*Sep  1 14:48:45.310: %CMRP-5-CHASSIS_MONITOR_BOOT_TIME_PRINT: R0/0: cmand: Card F0 took 63 secs
 to boot
*Sep  1 14:48:45.310: %CMRP-5-CHASSIS_MONITOR_BOOT_TIME_PRINT: R0/0: cmand: Card 0 took 58 secs
to boot
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]
*Sep  1 14:48:46.262: %IOXN_APP-6-IOX_START_STOP_REQ: Got IOX DOWN COMPLETE event, invoking
registered callback(s)


This operation may take hours. Please do not power cycle.


*Sep  1 14:48:49.671: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.Sep
 1 14

Enabling factory reset for this reload cycle
Enabling factory reset for this reload cycle

Sep 01 14:49:04.433: NIST 800 88r1 compliant factory reset starts.
Sep 01 14:49:04.511: #CISCO DATA SANITIZATION REPORT:# C8161-G2
Sep 01 14:49:04.593: start to purge non-volatile storage.
Executing Data Sanitization...
eMMC Data Sanitization started ...
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - Reading EXT_CSD !!!
!!! Please, wait - Erasing(Secure) /dev/mmcblk0 !!!
!!! Please, wait - Erasing(Secure) /dev/mmcblk0 !!!
!!! Please, wait - Erasing(Secure) /dev/mmcblk0 !!!
!!! Please, wait - Erasing(Secure) /dev/mmcblk0 !!!
!!! Please, wait - Erasing(Secure) /dev/mmcblk0 !!!
!!! Please, wait - Sanitizing /dev/mmcblk0 !!!
!!! Please, wait - Validating Erase for /dev/mmcblk0 !!!
eMMC Data Sanitization completed ...
Data Sanitization Success! Exiting...
Sep 01 14:53:15.065: purge non-volatile storage done.
========================
#CISCO C8100 DATA SANITIZATION REPORT#
START : 01-09-2025, 14:49:07
  END : 01-09-2025, 14:53:12
-eMMC-
MID : SanDisk
PNM : 'DA6064'
SN : 0xa0611433
Status : SUCCESS
NIST : PURGE
========================
Sep 01 14:53:15.406: start to check bootflash.
Sep 01 14:57:32.838: bootflash check done.
Sep 01 14:57:32.894: start to cleanup ROMMON variables.
Sep 01 14:57:33.805: ROMMON cleanup variables done.
Sep 01 14:57:33.869: start to cleanup ACT2/AIKIDO/TPM chip
Sep 01 14:57:35.747: ACT2/AIKIDO/TPM cleanup done.
Sep 01 14:57:38.152: report save done.
Sep 01 14:57:38.198: Factory reset operation completed.


[BootramDDR v7 RELEASE SOFTWARE (P) compiled 2025-07-16T12:06:41-07:00]


Warning: monitor Nvram area is corrupt ... using default values
Warning: MFG Key Enabled !!!

System Bootstrap, Version 17.18(1r), RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
C8161-G2 platform with 8388608 Kbytes of main memory
Warning: MFG key enabled, bypassing BIOS protection feature
rommon 1 >
```

What happens after a factory reset

After the factory reset is successfully completed, the router boots up. However, before the factory reset process started, if the configuration register was set to manually boot from ROMMON, the router stops at ROMMON.

After you configure Smart Licensing, execute the **#show license status** command, to check whether Smart Licensing is enabled for your instance.

Note If you had Specific License Reservation enabled before you performed the factory reset, use the same license and enter the same license key that you received from the smart agent.

CHAPTER 11

Control router access with passwords and privilege levels

One of the restriction for controlling router access with passwords and privileges is - disabling password recovery does not work if you have set the router to boot up manually by using the **boot manual** global configuration command. This command produces the boot loader prompt (*router:*) after the router is power cycled.

Restrictions and guidelines for reversible password types

- Password type 0 and 7 are replaced with password type 6. So password type 0 and 7, which were used for administrator login to the console, Telnet, SSH, webUI, and NETCONF must be migrated to password type 6. No action is required if username and password are type 0 and 7 for local authentication such as CHAP, EAP, and so on.

Note Type 6 encrypted password and Autoconversion to password type 6 are supported from is supported from Cisco IOS XE 17.18.x release and later releases.

- If the startup configuration of the device has type 6 password and you downgrade to a version in which type 6 password is not supported, you will be locked out of the device.

Restrictions and guidelines for irreversible password types

- Username secret password type 5 and enable secret password type 5 must be migrated to the stronger password type 8 or 9. For more information, see Protecting enable and enable secret passwords with encryption, on page 100.

- If the startup configuration of the device has convoluted type 9 secret (password that starts with $14$), then a downgrade can only be performed to a release in which the convoluted type 9 secret is supported.

  Before you downgrade to any release in which convoluted type 9 secret is not supported, ensure that the type 9 secret (password that starts with $9$) must be part of the startup configuration instead of convoluted type 9 secret (password that starts with $14$) or type 5 secret (password that starts with $1$).

- Plain text passwords are converted to nonreversible encrypted password type 9.
- Secret password type 4 is not supported.

Information about controlling router access with passwords and privileges

This section provides information about controlling router access with passwords and privileges.

Preventing unauthorized access

You can prevent unauthorized users from reconfiguring your switch and viewing configuration information. Typically, you want network administrators to have access to your switch while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your switch, you should configure one or more of these security features:

- At a minimum, you should configure passwords and privileges at each switch port. These passwords are locally stored on the switch. When users attempt to access the switch through a port or line, they must enter the password specified for the port or line before they can access the switch.
- For an additional layer of security, you can also configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.
- If you want to use username and password pairs, but you want to store them centrally on a server instead of locally, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information.
- You can also enable the login enhancements feature, which logs both failed and unsuccessful login attempts. Login enhancements can also be configured to block future login attempts after a set number of unsuccessful attempts are made.

Default password and privilege level configuration

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

This table shows the default password and privilege level configuration.

Table 11: Default Password and Privilege Levels

Feature	Default Setting
Enable password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.
Enable secret password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	No password is defined.

Additional password security

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the **enable password** or **enable secret** global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

Password recovery

By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted.

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

To re-enable password recovery, use the **service password-recovery** global configuration command.

Terminal line telnet configuration

When you power-up your switch for the first time, an automatic setup program runs to assign IP information and to create a default configuration for continued use. The setup program also prompts you to configure your switch for Telnet access through a password. If you did not configure this password during the setup program, you can configure it when you set a Telnet password for a terminal line.

Username and password pairs

You can configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Privilege levels

Cisco devices use privilege levels to provide password security for different levels of switch operation. By default, the Cisco IOS XE software operates in two modes (privilege levels) of password security: user EXEC (Level 1) and privileged EXEC (Level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

Privilege Levels on Lines

Users can override the privilege level you set using the **privilege level** line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to a more restricted group of users.

Command Privilege Levels

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip traffic** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15 unless you set them individually to different levels.

AES password encryption and primary encryption keys

You can enable strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as type 6 encryption. To start using type 6 encryption, enable the AES Password Encryption feature and configure a primary encryption key to encrypt and decrypt passwords.

After you enable AES password encryption and configure a primary key, all the existing and newly created cleartext passwords for the supported applications are stored in type 6 encrypted format, unless you disable type 6 password encryption. You can also configure the device to convert all the existing weakly encrypted passwords to type 6 encrypted passwords.

Type 0 and 7 passwords can be autoconverted to type 6 if the AES Password Encryption feature and primary encryption key are configured.

How to configure the router access with passwords and privileges

Setting or changing a static enable password

The enable password controls access to the privileged EXEC mode. Follow these steps to set or change a static enable password:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**enable password** *password* **Example:** `Device(config)# enable password secret321`	Defines a new password or changes an existing password for access to privileged EXEC mode. By default, no password is defined. For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Crtl-v when you create the password; for example, to create the password abc?123, do this: **a.** Enter **abc**.

	Command or Action	Purpose
		b. Enter **Crtl-v**. **c.** Enter **?123**. When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Protecting enable and enable secret passwords with encryption

Follow these steps to establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Use one of the following:
   - **enable password** [**level** *level*] {*unencrypted-password* | *encryption-type encrypted-password*}
   - **enable secret** [**level** *level*] {*unencrypted-password* | *encryption-type encrypted-password*}
4. **service password-encryption**
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Use one of the following:	• Defines a new password or changes an existing password for access to privileged EXEC mode.

	Command or Action	Purpose
	• **enable password** [**level** *level*] {*unencrypted-password* | *encryption-type encrypted-password*} • **enable secret** [**level** *level*] {*unencrypted-password* | *encryption-type encrypted-password*} **Example:** `Device(config)# `**`enable password level 12 example123`** or `Device(config)# `**`enable secret 9 $9$sMLBsTFXLnnHTk$0L82`**	• Defines a secret password, which is saved using a nonreversible encryption method. • (Optional) For *level*, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges). • For *unencrypted-password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. • For *encryption-type*, the available options for **enable password** are type 0 and 7, and type 0, 5, 8, and 9 for **enable secret**. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration. Secret encryption type 9 is more secure, so we recommend that you select type 9 to avoid any issues while upgrading or downgrading. **Note** • If you do not specify an encryption type for the secret password, the password is auto converted to type 9. This is applicable in Cisco IOS XE Gibraltar 16.10.1 and later releases. • If you specify an encryption type and then enter a clear text password, it will result in an error. • You can also configure type 9 encryption for the secret password manually by using the **algorithm-type scrypt** command in global configuration mode. For example: `Device(config)# `**`username user1 algorithm-type scrypt secret cisco`** Or `Device(config)# `**`enable algorithm-type scrypt secret cisco`** Run the **write memory** command in privileged EXEC mode for the type 9 secret to be permanently written into the startup configuration.

	Command or Action	Purpose
Step 4	**service password-encryption** **Example:** `Device(config)# service password-encryption`	(Optional) Encrypts the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.

Step 5	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Disabling password recovery

Follow these steps to disable password recovery to protect the security of your switch:

Before you begin

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no service password-recovery**
4. **end**

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
Step 3	**no service password-recovery** **Example:** `Device(config)# no service password-recovery`	Disables password recovery. This setting is saved in an area of the flash memory that is accessible by the boot loader and the Cisco IOS image, but is not a part of the file system and is not accessible by any user.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

What to do next

To remove **disable password recovery**, use the **no service password-recovery** global configuration command.

Setting a telnet password for a terminal line

Beginning in user EXEC mode, follow these steps to set a Telnet password for the connected terminal line:

Before you begin

- Attach a PC or workstation with emulation software to the switch console port, or attach a PC to the Ethernet management port.
- The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line vty 0 15**
4. **password** *password*
5. **end**

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**line vty 0 15** **Example:** `Device(config)# line vty 0 15`	Configures the number of Telnet sessions (lines), and enters line configuration mode. There are 16 possible sessions on a command-capable device. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.
Step 4	**password** *password* **Example:** `Device(config-line)# password abcxyz543`	Sets a Telnet password for the line or lines. For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.

Step 5	**end**
	Example:
	`Device(config-line)# end`
		Returns to privileged EXEC mode.

Username and password pairs

You can configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Setting the privilege level for a command

The following example shows how to set the **configure** command to privilege level 14 and define *SecretPswd14* as the password users must enter to use level 14 commands:

```
Device> enable
Device# configure terminal
Device(config)# privilege exec level 14 configure
Device(config)# enable password level 14 SecretPswd14
Device(config)# end
```

Changing the default privilege level for lines

Follow these steps to change the default privilege level for the specified line:

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **line vty** *line*
4. **privilege exec level** *level*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**line vty** *line* **Example:** `Device(config)# line vty 10`	Selects the virtual terminal line on which to restrict access.
Step 4	**privilege exec level** *level* **Example:** `Device(config-line)# privilege exec level 15`	Changes the default privilege level for the line. For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password.

Step 5	**end**
	Example:
	`Device(config-line)# end`
		Exits line configuration mode and returns to privileged EXEC mode.

What to do next

Users can override the privilege level you set using the **privilege level** line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

How to log in and exit a privilege level

Beginning in user EXEC mode, follow these steps to log into a specified privilege level and exit a specified privilege level.

SUMMARY STEPS

1. **enable** *level*
2. **disable** *level*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** *level* **Example:** `Device> enable 15`	Logs in to a specified privilege level. InI the example, Level 15 is privileged EXEC mode. For *level*, the range is 0 to 15.
Step 2	**disable** *level* **Example:** `Device# disable 1`	Exits to a specified privilege level. In the example, Level 1 is user EXEC mode. For *level*, the range is 0 to 15.

Configuring an encrypted preshared key

To configure an encrypted preshared key, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key config-key password-encrypt** [*text*]
4. **password encryption aes**
5. **end**

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**key config-key password-encrypt** [*text*] **Example:** `Device(config)# key config-key password-encrypt`	Stores a type 6 encryption key in private NVRAM. • To key in interactively (using the **Enter** key) and an encrypted key already exists, you will be prompted for the following: Old key, New key, and Confirm key. • To key in interactively, but an encryption key is not present, you will be prompted for the following: New key and Confirm key. • When removing the password that is already encrypted, you will see the following prompt: `WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:"`
Step 4	**password encryption aes** **Example:** `Device(config)# password encryption aes`	Enables the encrypted preshared key.
Step 5	**end** **Example:** to **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Monitoring router access with passwords and privileges

Table 12: Commands for displaying privilege-level information

Command	Information
show privilege	Displays the privilege level configuration.

Configuration examples for router access with passwords and privilege levels

Setting or changing a static enable password

The following example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
Device> enable
Device# configure terminal
Device(config)# enable password l1u2c3k4y5
Device(config)# end
```

Protecting enable and enable secret passwords with encryption

The following example shows how to configure the encrypted password *$9$sMLBsTFXLnnHTk$0L82* for privilege level 2:

```
Device> enable
Device# configure terminal
Device(config)# enable secret level 2 9 $9$sMLBsTFXLnnHTk$0L82
Device(config)# end
```

Setting a telnet password for a terminal line

The following example shows how to set the Telnet password to *let45me67in89*:

```
Device> enable
Device# configure terminal
Device(config)# line vty 10
Device(config-line)# password let45me67in89
Device(config-line)# end
```

Setting the privilege level for a command

The following example shows how to set the **configure** command to privilege level 14 and define *SecretPswd14* as the password users must enter to use level 14 commands:

```
Device> enable
Device# configure terminal
Device(config)# privilege exec level 14 configure
Device(config)# enable password level 14 SecretPswd14
Device(config)# end
```

Configuring an encrypted preshared key

The following example shows a configuration for which a type 6 preshared key has been encrypted. It includes the prompts and messages that a user might see.

```
Device> enable
Device# configure terminal
Device(config)# password encryption aes
Device(config)# key config-key password-encrypt
New key:
Confirm key:
Device(config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Device(config)# end
```

CHAPTER 12

Change of authorization

Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.

Identity-Based Networking Services supports change of authorization (CoA) commands for session query, reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation.

Information about change of authorization

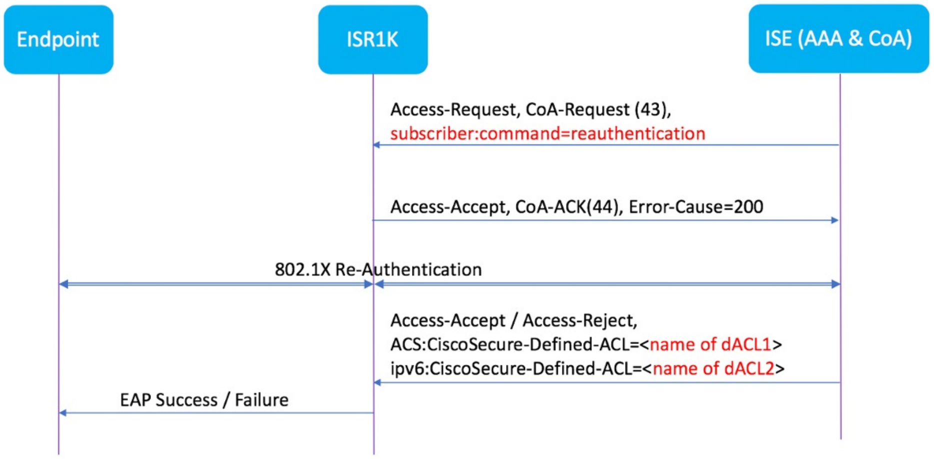
Change of authorization reauthentication procedure

Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. The main steps in this procedure are:

- Authentication
- Posture Assessment
- CoA Re-Authentication
- Network Access Authorization

When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server, such as a Cisco Identity Secure Engine (ISE) to reinitialize authentication and apply the new policy. This section provides an overview of the RADIUS interface including available primitives and how they are used during a CoA.

The RADIUS CoA provides a mechanism to change the attributes of an AAA session after it is authenticated. When policy changed on user or user group in RADIUS server, administrators can initiate RADIUS CoA process from RADIUS server to re-authenticate or re-authorize new policy


Endpoint
ISR1K
ISE (AAA & CoA)
Access-Request, CoA-Request (43),
subscriber:command=reauthentication
Access-Accept, CoA-ACK(44), Error-Cause=200
802.1X Re-Authentication
Access-Accept / Access-Reject,
ACS:CiscoSecure-Defined-ACL=<name of dACL1>
ipv6:CiscoSecure-Defined-ACL=<name of dACL2>
EAP Success / Failure

By default, the RADIUS interface is enabled on the device. However, some basic configuration is required for the following attributes:

- Security and Password
- Accounting

After posture assessment is succeessful, full network access is pushed down to the device for specific client through CoA re-authentication command based on its compliance state derived from last assessment. It is optional to enforce downloadable ACLs with Permit-ALL or limited access to certain resources to corresponding clients. Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

Change of authorization requests

Change of Authorization (CoA) is a critical part of a solution to initiate re-authenticate or re-authorization to an endpoint's network access based on its posture assessment result.

The network topology below shows a typical Cisco 8100 Series Secure Routers as a branch router in a network for secure access with ISE and other network services deployed in Campus or Data Center.

CoA is critical part of the solution to initiate re-authenticate or re-authorization to endpoint's network access based on its posture assessment result. Downloadable ACL is the Target/Purpose of the entire solution. The per-client basis customized security policies are achieved by it.

Restrictions for change of authorization

- Most of CoA and posture features heavily rely on HW TCAMs, such as Downloadable ACL (dACL), Redirect ACL (RACL) and SISF-based device tracking, which can only be supported on Cisco 8100 Series Secure Routers.

- Port ACL (PACL) is not supported on Cisco 8100 Series Secure Routers.
- IPv6 Access Control Entry (ACE) is not supported.
- IPv4 ACE can neither support IPv4 option header nor IP fragment match.
- IPv4 ACE can support TCP/UDP L4 port# match, but only with eq (=) or any (*) match. gt (>), lt (<) or range (A-to-B) is not supported.
- For C8130-G2:
    - Scale up to 128 dACL ACEs and up to 64 RACL ACEs are shared between all switchports.
    - IPv4 ACE L4 match can only support TCP/UDP port# match.
- For C8140-G2, C8151-G2, C8161-G2:
    - Scale up to 2048 dACL ACEs and up to 512 RACL ACEs shared between all switchports.
    - IPv4 ACE L4 match can only support TCP/UDP port# match, and L4 Flags with match-all (no match-any) option.
- SISF-based device tracking policy can support IPv4 address glean (using security-level glean) and tracking (using tracking enable).
- Multi-auth per user VLAN assignment is not supported.
- NEAT/CISP is not supported.

How to configure change of authorization

Essential dot1x|SANet configuration

Procedure

Example:

```
aaa new-model
aaa authentication dot1x default group coa-ise
aaa authorization network default group coa-ise
dot1x system-auth-control
aaa group server radius coa-ise
 server name coa
radius server coa
 address ipv4 10.10.1.10 auth-port 1812 acct-port 1813
 key cisco123
policy-map type control subscriber simple_coa
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
interface gigabitethernet0/1/0
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticator
service-policy type control subscriber simple_coa
```

Configure change of authorization

```
aaa server radius dynamic-author
 client
 server-key ******
 auth-type any
 ignore server-key
ip access-list extended redirect_acl
 20 deny udp any eq bootps any
 25 deny udp any eq domain any
 30 deny udp any any eq bootpc
 40 deny udp any eq bootpc any
 50 deny ip any host %{ise.ip}
 60 permit tcp any any eq www
 70 permit tcp any any eq 443
device-tracking tracking
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
interface 0/1/0
 device-tracking attach-policy tracking_test
```

Configuration examples for change of authorization

Check if the RADIUS server is active

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 10.10.10.1, auth-port 1812, acct-port 1813, hostname host
     State: current UP, duration 188755s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 188755s, previous duration 0s
```

Device tracking policy

```
Device# show aaa group radius coa3 **** port 1813 new-code
User successfully authenticated
USER ATTRIBUTES
username             0   "coa3"
```

To check if the parameters are enabled:

```
Device# show device-tracking policies
Target               Type  Policy               Feature        Target range
```

```
Gi0/1/1             PORT  tracking_test        Device-tracking vlan all
Gi0/1/2             PORT  tracking_test        Device-tracking vlan all
Gi0/1/3             PORT  tracking_test        Device-tracking vlan all
Gi0/1/4             PORT  tracking_test        Device-tracking vlan all
```

To check the SISF table:

```
Device# show device-tracking database
Binding Table has 1 entries, 1 dynamic (limit 100000)
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
Network Address        Link Address       Interface  vlan  prlvl    age    state       Time
 left
ARP 10.11.22.20       0050.5683.3f97      Gi0/1/4     22    0005    11s   REACHABLE
295 s
```

To check if the access-session is authenticated and autorized:

```
Device# show access-session interface gigabitEthernet 0/1/7 detail
            Interface:  GigabitEthernet0/1/7
               IIF-ID:  0x0DB9315A
          MAC Address:  b496.913d.4f9b
         IPv6 Address:  Unknown
         IPv4 Address:  10.10.22.27
            User-Name:  coa2
            Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  611C4B0A00000053F483D7B0
      Acct Session ID:  Unknown
               Handle:  0x21000049
       Current Policy:  POLICY_COA
   Server Policies:  Filter-ID: Filter_ID_COA2
   Method status list:  Method           State
                        dot1x           Authc Success
```

CHAPTER 13

Console port, telnet, SSH handling, and reset button

This chapter contains the following sections:

Restrictions and notes for console port, telnet, and SSH

Configuring the diagnostic and wait banners is optional, but recommended. The banners are especially useful as indicators to users about the status of their Telnet or SSH attempts.

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 Route Processor.

For information on accessing the router using the console port, see Use Cisco IOS XE software, on page 7.

Console port handling overview

If you are using the console port to access the router, you are automatically directed to the Cisco IOS command-line interface (CLI).

If you are trying to access the router through the console port and send a break signal (by entering **Ctrl-C** or **Ctrl-Shift-6**, or by entering the **send break** command at the Telnet prompt) before connecting to the CLI, you are directed to a diagnostic mode if the non-RPIOS subpackages are accessible. 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 SSH on the router can be configured and handled like Telnet and SSH on other Cisco platforms.

Reset button overview

The Reset button functionality is configured on all Cisco 8100 Series Secure Routers by default. You can use the Reset button to recover Cisco 8100 Series Secure Routers that become non-responsive due to incorrect configuration or when users are unable to login due to incorrect credentials.

Information about reset button functionality

The Reset button functionality is enabled by default. To disable this feature, use the **no service password-recovery strict** command.

You can press the reset button on the front panel to trigger the feature when the device is initializing.

Below are the tables that show the behavior of the Reset button feature in various possible combinations under service password recovery and no service password recovery:

Table 13: Service password-recovery

Press Reset Button (STATUS)				**Behavior**			
Sl. No	**Golden Image**	**Golden Config**	**Start up config**	**Image**	**Config**	**Extra**	
1	Exists	Exists	Exists	Golden	Golden	-	
2	Exists	Exists	None	Golden	Golden	-	
3	Exists	None	Exists	Golden	PnP	Delete startup	
4	Exists	None	None	Golden	PnP	-	
5	None	Exists	Exists	Standard	Golden	-	
6	None	Exists	None	Standard	Golden	-	
7	None	None	Exists	Standard	PnP	Delete startup	
8	None	None	None	Standard	PnP	-	

Table 14: No service password-recovery

Press Reset Button (STATUS)	**Behavior**

Sl. No	Golden Image	Golden Config	Start up config	Image	Config	Extra	
1	Exists	In NVRAM	Exists	Golden	PnP	Wipe	
2	Exists	In Bootflash	Exists	Golden	Golden	Wipe	
3	Exists	In NVRAM	None	Golden	PnP	Wipe	
4	Exists	In Bootflash	None	Golden	Golden	Wipe	
5	Exists	None	Exists	Golden	PnP	Wipe	
6	Exists	None	None	Golden	PnP	Wipe	
7	None	In NVRAM	Exists	Standard	PnP	Wipe	
8	None	In Bootflash	Exists	Standard	Golden	Wipe	
9	None	In NVRAM	None	Standard	PnP	Wipe	
10	None	In Bootflash	None	Standard	Golden	Wipe	
11	None	None	Exists	Standard	PnP	Wipe	
12	None	None	None	Standard	PnP	Wipe	

Prerequisites for enabling the reset button functionality

- Ensure that the ROMmon version on the device is at least 17.18(1r)
- Ensure to configure the golden.bin image and golden.cfg configuration.

Restrictions for reset button in controller mode

- Thereset button can erase all SD-WAN configuration, or apply available ciscosdwan.cfg configuration as the default configuration in Cisco 8100 Series Secure Routers. The reset button first attempts to boot the golden.bin image if available. If the golden.bin image is not available, the next attempt is the default bootup configuration. The golden.bin image is not mandatory for the reset feature.
- The Reset button must be pressed when the device is beginning to boot up. The Reset feature does not work when the system is configured in ROMMON or IOS modes.

How to enable the reset button functionality

This task describes how to enable Reset button feature on the Cisco 8100 Series Secure Routers:

SUMMARY STEPS

1. **configure terminal**
2. **service password-recovery**
3. **no service password-recovery**

4. **exit**
5. **no service recovery-service strict**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**service password-recovery** **Example:** `Device(config)# service password-recovery`	Configures the password recovery service on the device.
Step 3	**no service password-recovery** **Example:** `Device(config)# no service password-recovery`	You can recover the non-responsive device; however, the device is reconfigured because all user configurations and keys are deleted. **Note** Ensure that the device has a golden.bin and golden.cfg configurations on the device as a recovery mechanism so that the startup-config file on the IOS NVRAM is not deleted.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits the configuration mode and returns to the priviledge exec mode.

Step 5	**no service recovery-service strict**
	Example:
	`Device(config)# no service recovery-service`
	`strictexit`
		Disables the Reset button feature on the device.
		Note
		From Cisco IOS XE 17.18.x release and later, if you use the **no service recovery-service strict** command, even with a golden.bin or golden.cfg configuration on the device, you will not be able to recover the device, and therefore has to be returned and replaced through Return Material Authorization (RMA) to Cisco.

Enable and disable the reset button functionality

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

Device(config)# service password-recovery
```

```
Executing this command enables the password recovery mechanism.
Device(config)#
```

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# no service password-recovery strict

WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.

Are you sure you want to continue? [yes]: yes
Device(config)#
```

Configuring a console port transport map

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type console** *transport-map-name* **Example:** `Router(config)# transport-map type console consolehandler`	Creates and names a transport map for handling console connections, and enters transport map configuration mode.

	Command or Action	Purpose
Step 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] **Example:** `Router(config-tmap)# connection wait none`	Specifies how a console connection will be handled using this transport map. • **allow interruptible**—The console connection waits for a Cisco IOS VTY line to become available, and also allows users to enter diagnostic mode by interrupting a console connection that is waiting for a Cisco 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	(Optional) **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 Cisco IOS VTY line because of the console transport map configuration.
		• **diagnostic**—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.
		Note
		Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.
		• **wait**—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.
		• *banner-message*—Banner message, which begins and ends with the same delimiting character.

Step 6	**exit** **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	**transport type console** *console-line-number* **input** *transport-map-name* **Example:** `Router(config)# transport type console 0 input consolehandler`	Applies the settings defined in the transport map to the console interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** command.

Examples

The following example shows how to create a transport map to set console port access policies and attach 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
```

Viewing console port, SSH, and telnet handling configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**
- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

show transport-map [**all** | **name** *transport-map-name* | **type** [**console**]]

This command can be used either in user EXEC mode or privileged EXEC mode.

Example

The following example shows transport maps that are configured on the router: console port (`consolehandler`):

```
Router# show transport-map allTransport 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 consoleTransport Map:
Name: consolehandler


REVIEW DRAFT - CISCO CONFIDENTIAL

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 sshTransport 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
```

Use the **show platform software configuration access policy** command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the **show transport-map** command, the **show platform software configuration access policy** command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

Example

The following example shows the **show platform software configuration access policy** command.

```
Router# show platform software configuration access policyThe 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 :
```

Configuring console port for modem connection

Cisco 8100 Series Secure Routers support connecting a modem to the router console port for EXEC dial in connectivity. When a modem is connected to the console port, a remote user can dial in to the router and configure it. To configure a modem on the console port, perform these steps:

Procedure

Step 1 Connect the RJ-45 end of the adapter cable to the console port on the router.

Step 2 Use the **show line** command to determine the async interface of the console port:

```
Router# show  line

 Router#show line
Tty Line Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
* 0 0 CTY - - - - - 0 0 0/0 -
866 866 VTY - - - - - 0 0 0/0 -
867 867 VTY - - - - - 0 0 0/0 -
868 868 VTY - - - - - 0 0 0/0 -
869 869 VTY - - - - - 0 0 0/0 -
870 870 VTY - - - - - 0 0 0/0 -
```

Step 3 Use the following commands to configure the router console line::

```
Router(config)# line con 0

Router(config-line)#modem inOut
Router(config-line)#modem autoconfigure type usr_sportster
Router(config-line)#speed 115200  [Speed to be set according to the modem manual]
Router(config-line)#stopbits 1 [Stopbits to be set according to the modem manual]
Router(config-line)#transport input all
Router(config-line)#flowcontrol hardware [flowcontrol to be set according to the modem manual]
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#end
Router(config)#enable password lab
```

Step 4 Use the reverse telnet method on the modem to verify the modem connectivity and configuration string:

```
Router(config)#int loopback 0
Router(config-if)#ip add 192.0.2.1 255.255.255.0
Router(config-if)#end
Router#telnet 192.0.2.1 2001
Trying 1.1.1.1, 2001 ... Open

User Access Verification

Password: <enter the password given under line configuration>

at    <<<=== Modem command
OK  <<<=== This OK indicates that the modem is connected successully to the console port.
```

Step 5 Use an analog phone to verify that the phone line is active and functions properly. Then, connect the analog phone line to the modem.

Step 6 Initialize an EXEC modem call to the router from another device (PC) to test the modem connection.

Step 7 When the connection is established, the dial in client is prompted for a password. Enter the correct password.

Note: This password should match the one that is configured on the console port line.

CHAPTER 14

Set up factory default device using web UI

Quick Setup Wizard allows you perform the basic router configuration. To configure the router:

Note Before you access the WebUI, you need to have the basic configuration on the device.

Procedure

Step 1 Ensure that the router is in the factory fresh mode. If the router is not in the factory fresh mode, use the write erase option to erase all the configuration from the router.

Step 2 Ensure that the following basic configuration is available on the device.

```
!
!
ip dhcp pool WEBUIPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
username admin privilege 15 password 0 default
!
interface gig 0/0/1
ip address 192.168.1.1 255.255.255.0
!
```

Step 3 Connect the PC to the router using an Ethernet cable to the gig 0/0/1 interface.

Step 4 Set up your PC as a DHCP client to obtain the IP address of the router automatically.

Step 5 Enter the default username (webui) and default password (cisco).

Basic or advanced mode setup wizard

To configure the router using the basic or advanced mode setup:

Procedure

Step 1 Choose the **Basic Mode** or **Advanced Mode** and click **Go To Account Creation Page**.

Step 2 Enter the username and password. Reenter the password to confirm.

Step 3 Click **Create and Launch Wizard**.

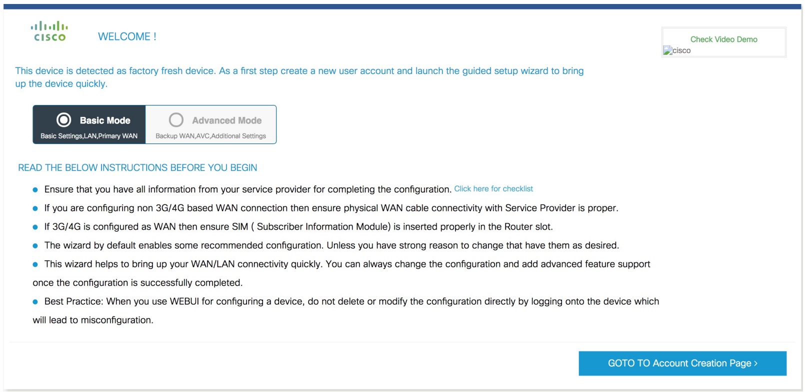
Step 4 Enter the device name and domain name.

Step 5 Select the appropriate time zone from the **Time Zone** drop-down list.

Step 6 Select the appropriate date and time mode from the **Date and Time** drop-down list.

Step 7 Click **LAN Settings**.

Figure 1:



This device is detected as factory fresh device. As a first step create a new user account and launch the guided setup wizard to bring up the device quickly.

● Basic Mode
Basic Settings,LAN,Primary WAN

○ Advanced Mode
Backup WAN,AVC,Additional Settings

READ THE BELOW INSTRUCTIONS BEFORE YOU BEGIN

- Ensure that you have all information from your service provider for completing the configuration. Click here for checklist
- If you are configuring non 3G/4G based WAN connection then ensure physical WAN cable connectivity with Service Provider is proper.
- If 3G/4G is configured as WAN then ensure SIM (Subscriber Information Module) is inserted properly in the Router slot.
- The wizard by default enables some recommended configuration. Unless you have strong reason to change that have them as desired.
- This wizard helps to bring up your WAN/LAN connectivity quickly. You can always change the configuration and add advanced feature support once the configuration is successfully completed.
- Best Practice: When you use WEBUI for configuring a device, do not delete or modify the configuration directly by logging onto the device which will lead to misconfiguration.

Configure LAN settings

Procedure

Step 1 Choose the **Web DHCP Pool/DHCP Pool** name or the **Create and Associate Access VLAN** option.

a) If you choose the Web DHCP Pool, specify the following:

Pool Name—Enter the DHCP Pool Name.

Network—Enter network address and the subnet mask.

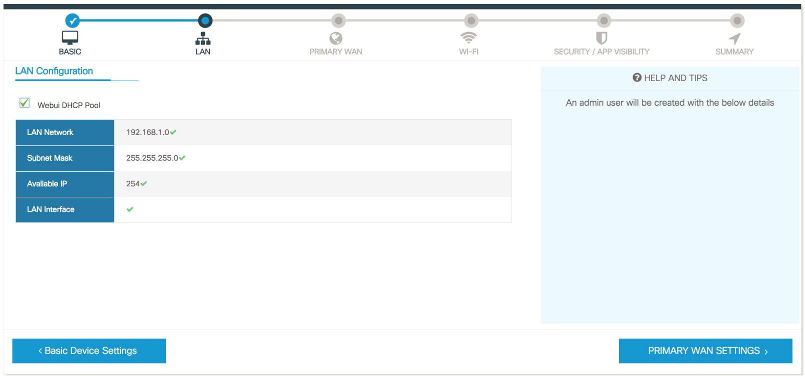
b) If you choose the Create and Associate Access VLAN option, specify the following:

Access VLAN—Enter the Access VLAN identification number. The range is from 1 to 4094.

Network—Enter the IP address of the VLAN.

Management Interfaces—Select the interface and move to the selected list box using the right and left arrows. You can also double click or drag and drop to move the interface to the selected list box.

Step 2 Click **Primary WAN Settings**.



☑ Webui DHCP Pool

LAN Network	192.168.1.0✓
Subnet Mask	255.255.255.0✓
Available IP	254✓
LAN Interface	✓

An admin user will be created with the below details

Configure primary WAN settings

Procedure

Step 1 Select the primary WAN type. You con configure Serial, 3G/4G, Ethernet, or Broadband (xDSL) as primary WAN depending on the WAN types supported by the router.

Step 2 Select the interface from the drop-down list.

Step 3 Check the **Get DNS Server info directly from ISP** check box to get the DNS server information directly from the service provider. You can also manually enter the Primary DNS and Secondary DNS.

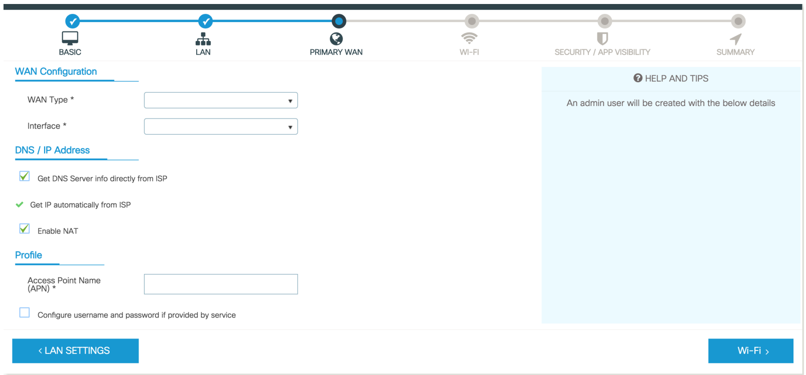
Step 4 Check the **Get IP automatically from ISP** check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.

Step 5 Check the **Enable NAT** check box to enable NAT. It is recommended to enable NAT.

Step 6 Check the **Enable PPPOE** check box to enable PPPoE. If you have enabled PPPoE, select the required authentication mode. The options are: **PAP** and **CHAP**.

Step 7 Enter the user name and password provided by the service provider.

Step 8 Click **Security / APP Visibility WAN Settings**.



WAN Configuration

WAN Type * ▾

Interface * ▾

DNS / IP Address

☑ Get DNS Server info directly from ISP

✓ Get IP automatically from ISP

☑ Enable NAT

Profile

Access Point Name (APN) *

□ Configure username and password if provided by service

HELP AND TIPS

An admin user will be created with the below details

Configure secondary WAN settings

For advanced configuration, you should configure the secondary WAN connection.

Procedure

Step 1 Select the secondary WAN type. You con configure Serial, 3G/4G, Ethernet, or Broadband (xDSL) as a secondary WAN depending on the WAN types supported by the router.

Step 2 Select the interface from the drop-down list.

Step 3 Check the **Get DNS Server info directly from ISP** check box to get the DNS server information directly from the service provider. You can also manually enter the Primary DNS and Secondary DNS.

Step 4 Check the **Get IP automatically from ISP** check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.

Step 5 Check the **Enable NAT** check box to enable NAT. It is recommended to enable NAT.

Step 6 Check the **Enable PPPOE** check box to enable PPPoE. If you have enabled PPPoE, select the required authentication mode. The options are **PAP** and **CHAP** .

Step 7 Enter the user name and password provided by the service provider.

Step 8 Click **Security / APP Visibility WAN Settings**.

Configure security settings

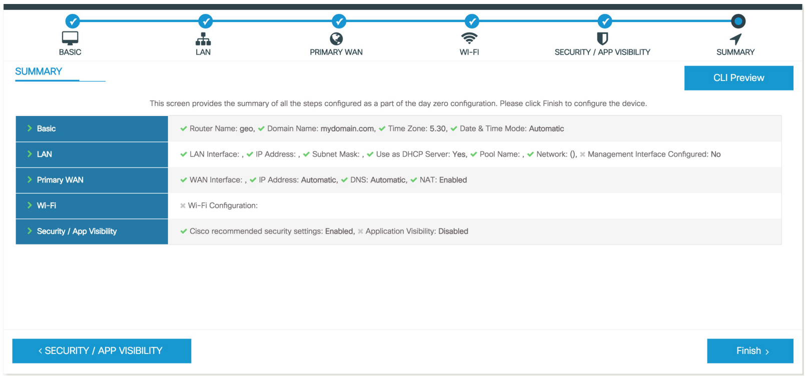
Procedure

Step 1 Check the **Enable Cisco Recommended Security Settings** check box to ensure that all passwords are not shown in plain text. The passwords are encrypted.

Step 2 Click **Day 0 Config Summary**.

Step 3 To preview the configuration, click **CLI Preview** to preview the configuration.

Step 4 Click **Finish** to complete the Day Zero setup.



This screen provides the summary of all the steps configured as a part of the day zero configuration. Please click Finish to configure the device.

› Basic	✓ Router Name: geo, ✓ Domain Name: mydomain.com, ✓ Time Zone: 5.30, ✓ Date & Time Mode: Automatic
› LAN	✓ LAN Interface: , ✓ IP Address: , ✓ Subnet Mask: , ✓ Use as DHCP Server: Yes, ✓ Pool Name: , ✓ Network: (), ✗ Management Interface Configured: No
› Primary WAN	✓ WAN Interface: , ✓ IP Address: Automatic, ✓ DNS: Automatic, ✓ NAT: Enabled
› Wi-Fi	✗ Wi-Fi Configuration:
› Security / App Visibility	✓ Cisco recommended security settings: Enabled, ✗ Application Visibility: Disabled

Using web user interface for day one setup

To configure the Web user interface:

Procedure

Step 1 Configure the HTTP server. By default, the HTTP server configuration should be present on the device. Ensure the configuration by checking if the **ip http server** and **ip http secure-server** commands are present in the running configuration.

```
Device #configure terminal
Device (config)#ip http server
Device (config)#ip http secure-server
```

Step 2 Set up the authentication options to log into Web UI. You can use one of these methods to authenticate:

a) You can authenicate using local database. To use a local database for Web UI authentication, ensure to have the **ip http authentication local** command in the running configuration. This command is preconfigured on the device. If the command is not present, configure the device as shown in this example:

```
Device #configure terminal
Device (config)#ip http authentication local
```

Note

You need a user with privilege 15 to access the configuration screens on Web UI. If the privilege is less than 15, you can access only the Dashboard and Monitoring screens on Web UI.

To create a user account, use the **username** <username> **privilege** <privilege> **password 0** <passwordtext>

```
Device #configure terminal
Device (config)# username <username> privilege <privilege> password 0 <passwordtext>
```

b) Authenticate using AAA options. To use AAA authentication for Web UI, ensure to configure ‘ip http authentication aaa’ on the device. Also, ensure that the required AAA server configuration is present on the device.

```
Device #configure terminal
Device (config)#ip http authentication local
```

Step 3 Launch the browser. In the address bar, type the IP address of the device. For a secure connection, type https://ip-address.

Step 4 Enter the default username (cisco) and password provided with the device

Step 5 Click **Log In**.

Monitor and troubleshoot device plug and play (PnP) onboarding using webUI

A device can be automatically onboarded to Cisco vManage through either Zero Touch Provisioning (ZTP) or the Plug and Play (PnP) process. This section describes the procedure to monitor and troubleshoot device onboarding through the PnP method. This feature on WebUI enables you to monitor and troubleshoot the PnP onboarding process, and also see its real-time status. If this onboarding is stuck or fails, you can terminate the process and onboard your device manually.

Prerequisites

- Your device (a computer that can run a web browser) running the WebUI and the device you are onboarding must be connected through an L2 switch port (NIM) on the device.
- The DHCP client-identifier on your device must be set to string “webui”.
- Your device must support Cisco SD-WAN Day-0 device onboarding on WebUI.

Troubleshoot Device PnP Onboarding

To troubleshoot device onboarding through PnP in controller mode:

1. Enter the controller mode in WebUI:

   Switching from autonomous mode to controller mode:

   Usually, when you boot your device for the first time it is in autonomous mode. Go to the URL https://192.168.1.1/webui/ and log in using the default credentials— webui/cisco. If your device supports Cisco SD-WAN Day-0 device onboarding on WebUI, you can switch to the controller mode by selecting **Controller Mode.** A dialogue box appears, asking if you want to continue. Click **Yes.** Your device reloads to switch to controller mode.

   Booting your device in controller mode:

   If your device is already in the controller mode, you do not have to make any changes to the mode. Go to the URL https://192.168.1.1 or https://192.168.1.1/webui. If your device supports Cisco SD-WAN Day-0 device onboarding on WebUI, the URL is redirected to https://192.168.1.1/ciscosdwan/ and you can log in using the default credentials for Cisco IOS XE SD-WAN devices - admin/admin.

Note If the device does not have start-up configuration at the time of PnP onboarding, the WebUI is enabled by default on supported devices.

2. On the **Welcome to Cisco SDWAN Onboarding Wizard** page, click **Reset Default Password.**

Note The default password of your Day-0 device is weak. Therefore, for a secure log in, you must reset the password when you first log in to the device on WebUI. The WebUI configuration is automatically deleted after the device is onboarded successfully. In rare cases where the template configuration for your device on Cisco vManage has the WebUI configuration, it is not deleted even after a successful device onboarding.

3. You are redirected to the Device hardware and software details page. Enter your password and click **Submit.**

4. The next page displays the onboarding progress and lists statuses of different components of the PnP Connect Portal and Cisco SD-WAN controllers. If the PnP IPv4 component fails, it indicates that the device PnP onboarding has failed.

   To view and download logs for the onboarding process, click the information icon on the right hand side of the SDWAN Onboarding Progress bar.

5. If the automated PnP onboarding fails, click **Terminate Automated Onboarding.** This allows you to onboard your device manually.

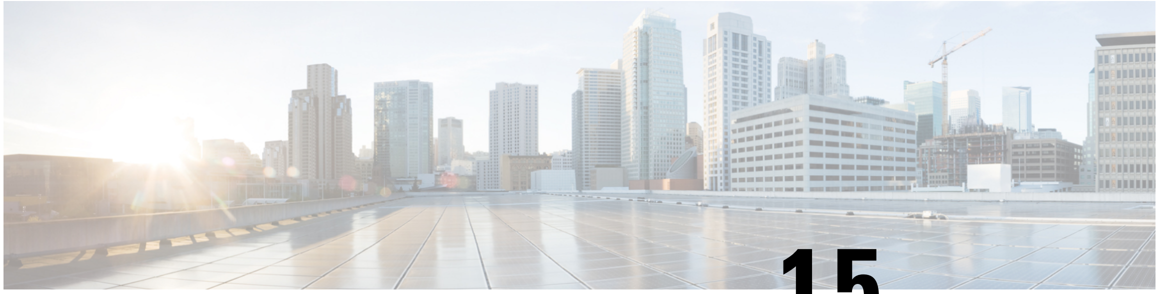
6. A dialogue box appears. To continue with the termination, click **Yes**. It might take a few minutes for the termination to complete.

7. On the Bootstrap Configuration page click **Select File** and choose the bootstrap file for your device. This file can be either a generic bootstrap file (common platform-specific file) or a full configuration bootstrap file that you can download from Cisco SD-WAN Manager. This file must contain details such as the vBond number, UUID, WAN interface, root CA and configuration.

8. Click **Upload**.

9. After your file is successfully uploaded, click **Submit.**

10. You can see the SDWAN Onboarding Progress page again with statuses of the Cisco SD-WAN controllers. To open the Controller Connection History table click the information icon on the right hand side of the SDWAN Control Connections bar. In this table you can see the state of your onboarded device. After the onboarding is complete, the state of your device changes to **connect**.



CHAPTER 15

Monitor control plane resources

The following sections explain the of memory and CPU monitoring from the perspective of the Cisco IOS process and the overall control plane:

Avoid problems through regular monitoring

Processes should provide monitoring and notification of their status/health to ensure correct operation. When a process fails, a syslog error message is displayed and either the process is restarted or the device is rebooted. A syslog error message is displayed when a monitor detects that a process is stuck or has crashed. If the process can be restarted, it is restarted; else, the device is restarted.

Monitoring system resources enables you to detect potential problems before they occur, thus avoiding outages. The advantages of regular monitoring:

- Lack of memory on line cards that are in operation for a few years can lead to major outages. Monitoring memory usage helps to identify memory issues in the line cards and enables you to prevent an outage.

- Regular monitoring establishes a baseline for a normal system load. You can use this information as a basis for comparison when you upgrade hardware or software—to see if the upgrade has affected resource usage.

Cisco IOS process resources

You can view CPU utilization statistics on active processes and see the amount of memory being used in these processes using the **show memory** command and the **show process cpu** command. These commands provide a representation of memory and CPU utilization from the perspective of only the Cisco IOS process; they do not include information for resources on the entire platform. For example, when the **show memory** command is used in a system with 8 GB RAM running a single Cisco IOS process, the memory usage is example shows:

```
Router# show memory
Tracekey : 1#cb0b8989b15e46da15c7630297789582

                                                                          Head    Total(b)
     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor  FFFF59A6B048   20578847040   289787696   20289059344   655646464   19922943908
reserve P  FFFF59A6B0A0      102404           92      102312      102312      102312
lsmpi_io  FFFF434FA1A8     6295128     6294304         824         824         412
Dynamic heap limit(MB) 19000     Use(MB) 0
```

The **show process cpu** command displays Cisco IOS CPU utilization average:

```
Router# show process cpu
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)      Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           1          14          71  0.00%  0.00%  0.00%   0 Chunk Manager
   2         127         872         145  0.00%  0.00%  0.00%   0 Load Meter
   3           0           1           0  0.00%  0.00%  0.00%   0 Policy bind Proc
   4           0           1           0  0.00%  0.00%  0.00%   0 Retransmission o
   5           0           1           0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6          11          13         846  0.00%  0.00%  0.00%   0 RF Slave Main Th
   7           0           1           0  0.00%  0.00%  0.00%   0 EDDRI_MAIN
   8           0           1           0  0.00%  0.00%  0.00%   0 RO Notify Timers
   9        1092         597        1829  0.00%  0.01%  0.00%   0 Check heaps
  10           8          73         109  0.00%  0.00%  0.00%   0 Pool Manager
  11           0           1           0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
  12           0           2           0  0.00%  0.00%  0.00%   0 Timers
  13           0          32           0  0.00%  0.00%  0.00%   0 WATCH_AFS
  14           0           1           0  0.00%  0.00%  0.00%   0 MEMLEAK PROCESS
  15        1227       40758          30  0.00%  0.02%  0.00%   0 ARP Input
  16          41        4568           8  0.00%  0.00%  0.00%   0 ARP Background
  17           0           2           0  0.00%  0.00%  0.00%   0 ATM Idle Timer
  18           0           1           0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
  19           0           1           0  0.00%  0.00%  0.00%   0 CEF MIB API
  20           0           1           0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  21           0           1           0  0.00%  0.00%  0.00%   0 Policy Manager
  22           0           2           0  0.00%  0.00%  0.00%   0 DDR Timers
  23          60          23        2608  0.00%  0.00%  0.00%   0 Entity MIB API
  24          43          45         955  0.00%  0.00%  0.00%   0 PrstVbl
  25           0           2           0  0.00%  0.00%  0.00%   0 Serial Backgroun
  26           0           1           0  0.00%  0.00%  0.00%   0 RMI RM Notify Wa
  27           0           2           0  0.00%  0.00%  0.00%   0 ATM AutoVC Perio
  28           0           2           0  0.00%  0.00%  0.00%   0 ATM VC Auto Crea
  29          30        2181          13  0.00%  0.00%  0.00%   0 IOSXE heartbeat
  30           1           9         111  0.00%  0.00%  0.00%   0 Btrace time base
  31           5         182          27  0.00%  0.00%  0.00%   0 DB Lock Manager
  32          16        4356           3  0.00%  0.00%  0.00%   0 GraphIt
  33           0           1           0  0.00%  0.00%  0.00%   0 DB Notification
  34           0           1           0  0.00%  0.00%  0.00%   0 IPC Apps Task
  35           0           1           0  0.00%  0.00%  0.00%   0 ifIndex Receive
  36           4         873           4  0.00%  0.00%  0.00%   0 IPC Event Notifi
  37          49        4259          11  0.00%  0.00%  0.00%   0 IPC Mcast Pendin
  38           0           1           0  0.00%  0.00%  0.00%   0 Platform appsess
  39           2          73          27  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  40           5         873           5  0.00%  0.00%  0.00%   0 IPC Service NonC
  41           0           1           0  0.00%  0.00%  0.00%   0 IPC Zone Manager
  42          38        4259           8  0.00%  0.00%  0.00%   0 IPC Periodic Tim
  43          18        4259           4  0.00%  0.00%  0.00%   0 IPC Deferred Por
  44           0           1           0  0.00%  0.00%  0.00%   0 IPC Process leve
  45           0           1           0  0.00%  0.00%  0.00%   0 IPC Seat Manager
  46           3         250          12  0.00%  0.00%  0.00%   0 IPC Check Queue
  47          0          1          0  0.00%  0.00%  0.00%   0 IPC Seat RX Cont
  48          0          1          0  0.00%  0.00%  0.00%   0 IPC Seat TX Cont
  49         22        437         50  0.00%  0.00%  0.00%   0 IPC Keep Alive M
  50         25        873         28  0.00%  0.00%  0.00%   0 IPC Loadometer
  51          0          1          0  0.00%  0.00%  0.00%   0 IPC Session Deta
  52          0          1          0  0.00%  0.00%  0.00%   0 SENSOR-MGR event
  53          2        437          4  0.00%  0.00%  0.00%   0 Compute SRP rate
```

Overall control plane resources

Control plane memory and CPU utilization on each control processor allows you to keep a tab on the overall control plane resources. You can use the **show platform resources** command to monitor the overall system health and resource usage for the IOS XE platforms. Also, you can use the **show platform software status control-processor brief** command (summary view) or the **show platform software status control-processor** command (detailed view) to view control plane memory and CPU utilization information.

All control processors should show status, Healthy. Other possible status values are Warning and Critical. Warning indicates that the device is operational, but that the operating level should be reviewed. Critical implies that the device is nearing failure.

If you see a Warning or Critical status, take the following actions:

- Reduce the static and dynamic loads on the system by reducing the number of elements in the configuration or by limiting the capacity for dynamic services.
- Reduce the number of routes and adjacencies, limit the number of ACLs and other rules, reduce the number of VLANs, and so on.

The following sections describe the fields in the **show platform software status control-processor** command output.

Load Average

Load average represents the process queue or process contention for CPU resources. For example, on a single-core processor, an instantaneous load of 7 would mean that seven processes are ready to run, one of which is currently running. On a dual-core processor, a load of 7 would mean that seven processes are ready to run, two of which are currently running.

Memory Utilization

Memory utilization is represented by the following fields:

- Total—Total line card memory
- Used—Consumed memory
- Free—Available memory
- Committed—Virtual memory committed to processes

CPU Utilization

CPU utilization is an indication of the percentage of time the CPU is busy, and is represented by the following fields:

- CPU—Allocated processor
- User—Non-Linux kernel processes
- System—Linux kernel process
- Nice—Low-priority processes
- Idle—Percentage of time the CPU was inactive
- IRQ—Interrupts
- SIRQ—System Interrupts
- IOwait—Percentage of time CPU was waiting for I/O

Example: show platform software status control-processor Command

The following are some examples of using the **show platform software status control-processor** command:

```
Router# show platform software status control-processor
RP0: online, statistics updated 3 seconds ago
RP0: online, statistics updated 5 seconds ago
Load Average: healthy
  1-Min: 1.35, status: healthy, under 9.30
  5-Min: 1.06, status: healthy, under 9.30
  15-Min: 1.02, status: healthy, under 9.30
Memory (kb): healthy
  Total: 7768456
  Used: 2572568 (33%), status: healthy
  Free: 5195888 (67%)
  Committed: 3112968 (40%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  3.00, System:  2.40, Nice:  0.00, Idle: 94.60
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU4: CPU Utilization (percentage of time spent)
  User:  7.30, System:  1.70, Nice:  0.00, Idle: 91.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU5: CPU Utilization (percentage of time spent)
  User:  3.30, System:  1.50, Nice:  0.00, Idle: 95.20
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU6: CPU Utilization (percentage of time spent)
  User: 17.91, System: 11.81, Nice:  0.00, Idle: 70.27
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU7: CPU Utilization (percentage of time spent)
  User: 11.91, System: 13.31, Nice:  0.00, Idle: 74.77
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU8: CPU Utilization (percentage of time spent)
  User:  2.70, System:  2.00, Nice:  0.00, Idle: 95.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU9: CPU Utilization (percentage of time spent)
```

```
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU10: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU11: CPU Utilization (percentage of time spent)
  User:  0.00, System:  0.00, Nice:  0.00, Idle:100.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
```

```
Router# show platform software status control-processor brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   1.14   1.07   1.02

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  7768456  2573416 (33%)  5195040 (67%)   3115096 (40%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   2.80   1.80   0.00  95.39   0.00   0.00   0.00
         1   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         2   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         3   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         4   6.80   1.80   0.00  91.39   0.00   0.00   0.00
         5   3.20   1.60   0.00  95.19   0.00   0.00   0.00
         6  16.30  12.60   0.00  71.10   0.00   0.00   0.00
         7  12.40  13.70   0.00  73.90   0.00   0.00   0.00
         8   2.40   2.40   0.00  95.19   0.00   0.00   0.00
         9   0.00   0.00   0.00 100.00   0.00   0.00   0.00
        10   0.00   0.00   0.00 100.00   0.00   0.00   0.00
        11   0.00   0.00   0.00 100.00   0.00   0.00   0.00
```

Monitoring hardware using alarms

Router design and monitoring hardware

The router sends alarm notifications when problems are detected, allowing you to monitor the network remotely. You do not need to use **show** commands to poll devices on a routine basis; however, you can perform onsite monitoring if you choose.

BootFlash disk monitoring

The bootflash disk must have enough free space to store two core dumps. This condition is monitored, and if the bootflash disk is too small to store two core dumps, a syslog alarm is generated, as shown in the following example:

```
Oct  6 14:10:56.292: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota exceeded

[free space is 1429020 kB] - Please clean up files on bootflash.
```

Approaches for monitoring hardware alarms

Viewing the 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 system message log (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 the alarms to be logged. All the 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 are examples of alarm messages that are sent to the console.

Alarms

To view alarms, use the **show facility-alarm status** command. The following example shows a critical alarm for the power supply:

```
Device# show facility-alarm status
System Totals  Critical: 8  Major: 0  Minor: 0

Source                     Time                      Severity      Description [Index]
------                     ------                    --------      -------------------

xcvr container 0/0/0       Sep 11 2025 09:50:51      INFO          Transceiver Missing [0]

xcvr container 0/0/1       Sep 11 2025 09:50:51      INFO          Transceiver Missing [0]

GigabitEthernet0/1/0       Sep 11 2025 09:50:54      CRITICAL      Physical Port Link Down [1]

GigabitEthernet0/1/1       Sep 11 2025 09:50:54      CRITICAL      Physical Port Link Down [1]

GigabitEthernet0/1/2       Sep 11 2025 09:50:54      CRITICAL      Physical Port Link Down [1]

GigabitEthernet0/1/3       Sep 11 2025 09:50:54      CRITICAL      Physical Port Link Down [1]


GigabitEthernet0/1/4       Sep 11 2025 09:50:54      CRITICAL      Physical Port Link Down [1]


GigabitEthernet0/1/5       Sep 11 2025 09:50:54      CRITICAL      Physical Port Link Down [1]


GigabitEthernet0/1/6       Sep 11 2025 09:50:54      CRITICAL      Physical Port Link Down [1]


GigabitEthernet0/1/7       Sep 11 2025 09:50:54      CRITICAL      Physical Port Link Down [1]
```

To view critical alarms, use the **show facility-alarm status critical** command, as shown in the following example:

```
Device# show facility-alarm status critical
System Totals  Critical: 8  Major: 0  Minor: 0

Source                     Time                   Severity      Description [Index]
------                     ------                 --------      -------------------

GigabitEthernet0/1/0       Sep 11 2025 09:50:54   CRITICAL      Physical Port Link Down [1]

GigabitEthernet0/1/1       Sep 11 2025 09:50:54   CRITICAL      Physical Port Link Down [1]

GigabitEthernet0/1/2       Sep 11 2025 09:50:54   CRITICAL      Physical Port Link Down [1]

GigabitEthernet0/1/3       Sep 11 2025 09:50:54   CRITICAL      Physical Port Link Down [1]

GigabitEthernet0/1/4       Sep 11 2025 09:50:54   CRITICAL      Physical Port Link Down [1]

GigabitEthernet0/1/5       Sep 11 2025 09:50:54   CRITICAL      Physical Port Link Down [1]


GigabitEthernet0/1/6       Sep 11 2025 09:50:54   CRITICAL      Physical Port Link Down [1]


GigabitEthernet0/1/7       Sep 11 2025 09:50:54   CRITICAL      Physical Port Link Down [1]
```

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

```
Device# show platform diag

Chassis type: C8161-G2

Slot: 0, C8161-G2
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:31 (02:34:51 ago)
  Software declared up time   : 00:01:03 (02:34:19 ago)
  CPLD version                : 2508050E
  Firmware version            : 17.18(1r)

Sub-slot: 0/0, C8161-2S
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:01:08 (02:34:13 ago)
  Logical insert detect time  : 00:01:08 (02:34:13 ago)

Sub-slot: 0/1, C8161-ES-8
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:01:09 (02:34:13 ago)
  Logical insert detect time  : 00:01:09 (02:34:13 ago)

Sub-slot: 0/2, P-LTEA7-NA
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:14:34 (02:20:48 ago)
  Logical insert detect time  : 00:14:34 (02:20:48 ago)

Slot: R0, C8161-G2
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:31 (02:34:51 ago)
  Software declared up time   : 00:00:31 (02:34:51 ago)
  CPLD version                : 2508050E
  Firmware version            : 17.18(1r)

Slot: F0, C8161-G2
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:31 (02:34:51 ago)
  Software declared up time   : 00:00:59 (02:34:23 ago)
  Hardware ready signal time  : 00:00:55 (02:34:26 ago)
  Packet ready signal time    : 00:01:04 (02:34:18 ago)
  CPLD version                : 2508050E
  Firmware version            : 17.18(1r)

Slot: P0, PWR-12V
  State                       : ok
  Physical insert detect time : 00:00:07 (02:34:26 ago)

Slot: GE-POE, Unknown
  State                       : NA
  Physical insert detect time : 00:00:00 (55y38w 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.

Network management system alerts a network administrator when an alarm is reported through SNMP

The SNMP is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

SNMP provides notification of faults, alarms, and conditions that might affect services. It allows a network administrator to access router information through a network management system (NMS) instead of reviewing logs, polling devices, or reviewing log reports.

To use SNMP to get alarm notification, use the following MIBs:

- ENTITY-MIB, RFC4133(required for the CISCO-ENTITY-ALARM-MIB, ENTITY-STATE-MIB and CISCO-ENTITY-SENSOR-MIB to work)
- CISCO-ENTITY-ALARM-MIB
- ENTITY-STATE-MIB
- CISCO-ENTITY-SENSOR-MIB(for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)

CHAPTER 16

Overview

Security-Enhanced Linux (SELinux) is a solution composed of Linux kernel security module and system utilities to incorporate a strong, flexible Mandatory Access Control (MAC) architecture into Cisco IOS-XE platforms.

SELinux provides an enhanced mechanism to enforce the separation of information, based on confidentiality and integrity requirements, which addresses threats of tampering and bypassing of application security mechanisms and enables the confinement of damage that malicious or flawed applications can cause.

Prerequisites for SELinux

There are no specific prerequisites for this feature.

Restrictions for SELinux

There are no specific restrictions for this feature.

Information about SELinux

SELinux enforces mandatory access control policies that confine user programs and system services to the minimum privilege required to perform their assigned functionality. This reduces or eliminates the ability of these programs and daemons to cause harm when compromised (for example, through buffer overflows or misconfigurations). This is a practical implementation of principle of least privilege by enforcing MAC on Cisco IOS-XE platforms. This confinement mechanism works independently of the traditional Linux access control mechanisms. SELinux provides the capability to define policies to control the access from an application process to any resource object, thereby allowing for the clear definition and confinement of process behavior.

SELinux can operate either in **Permissive mode** or **Enforcing mode** when enabled on a system.

- In Permissive mode, SELinux does not enforce the policy, and only generates system logs for any denials caused by violation of the resource access policy. The operation is not denied, but only logged for resource access policy violation.
- In Enforcing mode, the SELinux policy is enabled and enforced. It denies resource access based on the access policy rules, and generates system logs.

SELinux is enabled in Enforcing mode by default on supported Cisco IOS XE platforms. In the Enforcing mode, any system resource access that does not have the necessary allow policy is treated as a violation, and the operation is denied. The violating operation fails when a denial occurs, and system logs are generated. In Enforcing mode, the solution works in access-violation prevention mode.

Configuring SELinux

The are no additional requirements or configuration steps needed to enable or use the SELinux feature in Enforcing mode.

The following commands are introduced as part of the SELinux feature:

```
set platform software selinux {default | enforcing | permissive}
```

```
platform security selinux {enforcing | permissive}
```

```
show platform software selinux
```

Note These new commands are implemented as **service internal** commands.

Configuring SELinux (EXEC Mode)

Use the **set platform software selinux** command to configure SELinux in EXEC mode.

The following example shows SELinux configuration in EXEC mode:

```
Device# set platform software selinux ?

default  Set SELinux mode to default
enforcing  Set SELinux mode to enforcing
permissive  Set SELinux mode to permissive
```

Configuring SELinux (CONFIG Mode)

Use the **platform security selinux** command to configure SELinux in configuration mode.

The following example shows SELinux configuration in CONFIG mode:

```
Device(config)# platform security selinux

enforcing  Set SELinux policy to Enforcing mode
permissive  Set SELinux policy to Permissive mode

Device(config)# platform security selinux permissive

Device(config)#
*Oct 20 21:52:45.155: %IOSXE-1-PLATFORM: R0/0:
```

```
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!

Device(config)#
```

Examples for SELinux

The following example shows the output for changing the mode from Enforcing to Permissive:

```
“*Oct 20 21:44:03.609: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!”
```

The following example shows the output for changing the mode from Permissive to Enforcing:

```
“*Oct 20 21:44:34.160: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode upgraded to enforcing!”
```

Note If the SELinux mode is changed, this change is considered a system security event, and a system log message is generated.

Syslog message reference

Facility-Severity-Mnemonic	**%SELINUX-1-VIOLATION**
Severity-Meaning	Alert Level Log
Message	N/A
Message Explanation	Resource access was made by the process for which a resource access policy does not exist. The operation was flagged, and resource access was denied. A system log was generated with information that process resource access has been denied.
Component	SELINUX
Recommended Action	Contact Cisco TAC with the following relevant information as attachments: • The exact message as it appears on the console or in the system • Output of the **show tech-support** command (text file) • Archive of Btrace files from the box using the following command: **request platform software trace archive target <URL>** • Output of the **show platform software selinux** command

The following examples demonstrate sample syslog messages:

Example 1:

```
*Nov 14 00:09:04.943: %SELINUX-1-VIOLATION: R0/0: audispd: type=AVC
msg=audit(1699927057.934:129): avc: denied { getattr } for pid=5899 comm="ls"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive=0
```

Example 2:

```
*Nov 14 00:09:04.947: %SELINUX-1-VIOLATION: R0/0: audispd: t type=AVC
msg=audit(1699927198.486:130): avc: denied { write } for pid=6012 comm="echo"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive= 0
```

Verifying SELinux enablement

Use the **show platform software selinux** command to view the SELinux configuration mode:

```
Device# show platform software selinux
=========================================
IOS-XE SELINUX STATUS
=========================================
SElinux Status :    Enabled
Current Mode :      Enforcing
Config file Mode :  Enforcing
```

Troubleshooting SELinux

If there is an instance of an SELinux violation on your device or network, please reach out to Cisco TAC with the following details:

- The message exactly as it appears on the console or in the system log. For example:

  ```
  device#request platform software trace archive target
      flash:selinux_btrace_logs
  ```

- Output of the **show tech-support** command (text file)
- Archive of Btrace files from the box using the following command:

  request platform software trace archive target <URL>

- Output of the **show platform software selinux** command

CHAPTER 17

Packet trace

The Packet trace feature provides three levels of inspection for packets: accounting, summary, and path data. Each level provides a detailed view of packet processing at the cost of some packet processing capability. However, Packet Trace limits inspection to packets that match the debug platform condition statements, and is a viable option even under heavy-traffic situations in customer environments.

The following table explains the three levels of inspection provided by packet trace.

Table 15: Packet trace levels

Packet trace level	Description
Accounting	Packet-Trace accounting provides a count of packets that enter and leave the network processor. Packet-Trace accounting is a lightweight performance activity, and runs continuously until it is disabled.
Summary	At the summary level of packet trace, data is collected for a finite number of packets. Packet-Trace summary tracks the input and output interfaces, the final packet state, and punt, drop, or inject packets, if any. Collecting summary data adds to additional performance compared to normal packet processing, and can help to isolate a troublesome interface.
Path data	The packet-trace path data level provides the greatest level of detail in packet trace. Data is collected for a finite number of packets. Packet-Trace path data captures data, including a conditional debugging ID that is useful to correlate with feature debugs, a timestamp, and also feature-specific path-trace data. Path data also has two optional capabilities: packet copy and Feature Invocation Array (FIA) trace. The packet-copy option enables you to copy input and output packets at various layers of the packet (layer 2, layer 3 or layer 4). The FIA- trace option tracks every feature entry invoked during packet processing and helps you to know what is happening during packet processing. **Note** Collecting path data consumes more packet-processing resources, and the optional capabilities incrementally affect packet performance. Therefore, path-data level should be used in limited capacity or in situations where packet performance change is acceptable.

Usage Guidelines for Configuring Packet Trace

Consider the following best practices while configuring the Packet Trace feature:

- Use of ingress conditions when using the Packet Trace feature is recommended for a more comprehensive view of packets.
- Packet Trace configuration requires data-plane memory. On systems where data-plane memory is constrained, carefully consider how you will select the Packet Trace values. A close approximation of the amount of memory consumed by Packet Trace is provided by the following equation:

memory required = (statistics overhead) + number of packets * (summary size + data size + packet copy size).

When the Packet Trace feature is enabled, a small, fixed amount of memory is allocated for statistics. Similarly, when per-packet data is captured, a small, fixed amount of memory is required for each packet for summary data. However, as shown by the equation, you can significantly influence the amount of memory consumed by the number of packets you select to trace, and whether you collect path data and copies of packets.

Configuring Packet Trace

Perform the following steps to configure the Packet Trace feature.

Note The amount of memory consumed by the Packet Trace feature is affected by the Packet Trace configuration. You should carefully select the size of per-packet path data and copy buffers and the number of packets to be traced in order to avoid interrupting normal services. You can check the current data-plane DRAM memory consumption by using the **show platform hardware qfp active infrastructure exmem statistics** command.

SUMMARY STEPS

1. **enable**
2. **debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]**
3. **debug platform packet-trace {punt |inject|copy|drop|packet|statistics}**
4. **debug platform condition [ipv4 | ipv6] [interface** *interface***][access-list** *access-list -name* | *ipv4-address / subnet-mask* | *ipv6-address / subnet-mask***] [ingress | egress |both]**
5. **debug platform condition start**
6. **debug platform condition stop**
7. **show platform packet-trace {configuration | statistics | summary | packet {all** | *pkt-num***}}**
8. **clear platform condition all**
9. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	**debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]** **Example:** `Router# debug platform packet-trace packets 2048 summary-only`	Collects summary data for a specified number of packets. Captures feature path data by default, and optionally performs FIA trace. *pkt-num*—Specifies the maximum number of packets maintained at a given time. **fia-trace**—Provides detailed level of data capture, including summary data, feature-specific data. Also displays each feature entry visited during packet processing. **summary-only**—Enables the capture of summary data with minimal details. **circular**—Saves the data of the most recently traced packets. *data-size*—Specifies the size of data buffers for storing feature and FIA trace data for each packet in bytes. When very heavy packet processing is performed on packets, users can increase the size of the data buffers if necessary. The default value is 2048.

Step 3	**debug platform packet-trace {punt |inject|copy|drop|packet|statistics}**
	Example:
	`Router# debug platform packet-trace punt`
		Enables tracing of punted packets from data to control plane.

Step 4	**debug platform condition [ipv4 | ipv6] [interface** *interface***][access-list** *access-list -name* | *ipv4-address* / *subnet-mask* | *ipv6-address* / *subnet-mask***] [ingress | egress |both]** **Example:** `Router# debug platform condition interface g0/0/0 ingress`	Specifies the matching criteria for tracing packets. Provides the ability to filter by protocol, IP address and subnet mask, access control list (ACL), interface, and direction.
Step 5	**debug platform condition start** **Example:** `Router# debug platform condition start`	Enables the specified matching criteria and starts packet tracing.

	Command or Action	Purpose
Step 6	**debug platform condition stop** **Example:** `Router# debug platform condition start`	Deactivates the condition and stops packet tracing.

Step 7	**show platform packet-trace {configuration | statistics | summary | packet {all |** *pkt-num***}}**
	Example:
	`Router# show platform packet-trace 14`
		Displays Packet Trace data according to the specified option. See {start cross reference} Table 21-1 {end cross reference} for detailed information about the **show** command options.

Step 8	**clear platform condition all** **Example:** `Router(config)# clear platform condition all`	Removes the configurations provided by the **debug platform condition** and **debug platform packet-trace** commands.
Step 9	**exit** **Example:** `Router# exit`	Exits the privileged EXEC mode.

Display the Packet Trace Information

Use these **show** commands to display Packet Trace information.

Table 16: show Commands

Command	Description
show platform packet-trace configuration	Displays packet trace configuration, including any defaults.
show platform packet-trace statistics	Displays accounting data for all the traced packets.
show platform packet-trace summary	Displays summary data for the number of packets specified.
show platform packet-trace {all | *pkt-num***} [decode]**	Displays the path data for all the packets or the packet specified. The **decode** option attempts to decode the binary packet into a more human- readable form.

Remove Packet Trace data

Use these commands to clear packet-trace data.

Table 17: clear Commands

Command	Description
clear platform packet-trace statistics	Clears the collected packet-trace data and statistics.
clear platform packet-trace configuration	Clears the packet-trace configuration and the statistics.

Example: Configure Packet Trace

This example describes how to configure packet trace and display the results. In this example, incoming packets to Gigabit Ethernet interface 0/0/2 are traced, and FIA-trace data is captured for the first 128 packets. Also, the input packets are copied. The **show platform packet-trace packet 10** command displays the summary data and each feature entry visited during packet processing for packet 10.

```
Router>
enable
Router# debug platform packet-trace packet 128 fia-trace
Router# debug platform packet-trace punt
Router# debug platform condition interface g0/0/2 ingress
Router# debug platform condition start
Router#! ping to UUT
Router# debug platform condition stop
Router# show platform packet-trace packet 10
Packet: 10          CBUG ID: 52
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:1
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 597718358383 ns (06/06/2016 09:00:13.643341 UTC)
    Stop    : 597718409650 ns (06/06/2016 09:00:13.643392 UTC)
Path Trace
  Feature: IPV4
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.64.68.2
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Entry       : 0x8a0177bc - DEBUG_COND_INPUT_PKT
    Lapsed time : 426 ns
  Feature: FIA_TRACE
 --More--                                Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Entry       : 0x8a017788 - IPV4_INPUT_DST_LOOKUP_CONSUME
    Lapsed time : 386 ns
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Entry       : 0x8a01778c - IPV4_INPUT_FOR_US_MARTIAN
    Lapsed time : 13653 ns
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : internal0/0/rp:1
    Entry       : 0x8a017730 - IPV4_INPUT_LOOKUP_PROCESS_EXT
    Lapsed time : 2360 ns
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : internal0/0/rp:1
    Entry       : 0x8a017be0 - IPV4_INPUT_IPOPTIONS_PROCESS_EXT
    Lapsed time : 66 ns
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : internal0/0/rp:1
    Entry       : 0x8a017bfc - IPV4_INPUT_GOTO_OUTPUT_FEATURE_EXT
 --More--                               Lapsed time : 680 ns
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : internal0/0/rp:1
    Entry       : 0x8a017d60 - IPV4_INTERNAL_ARL_SANITY_EXT
    Lapsed time : 320 ns
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : internal0/0/rp:1
    Entry       : 0x8a017a40 - IPV4_VFR_REFRAG_EXT
    Lapsed time : 106 ns
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : internal0/0/rp:1
    Entry       : 0x8a017d2c - IPV4_OUTPUT_DROP_POLICY_EXT
    Lapsed time : 1173 ns
  Feature: FIA_TRACE
    Input       : GigabitEthernet0/0/0
    Output      : internal0/0/rp:1
    Entry       : 0x8a017940 - INTERNAL_TRANSMIT_PKT_EXT
    Lapsed time : 20173 ns
IOSd Path Flow: Packet: 10    CBUG ID: 52
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From CPP
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.64.68.2
    Destination : 224.0.0.102
    Interface   : GigabitEthernet0/0/0
  Feature: UDP
    Pkt Direction: IN
    src         : 10.64.68.2(1985)
    dst         : 224.0.0.102(1985)
    length      : 14
Router# clear platform condition all
Router# exit
```

Example: Using Packet Trace

This example provides a scenario in which packet trace is used to troubleshoot packet drops for a NAT configuration on a Cisco 8100 Series Secure Routers. This example shows how you can effectively utilize the level of detail provided by the Packet Trace feature to gather information about an issue, isolate the issue, and then find a solution.

In this scenario, you can detect that there are issues, but are not sure where to start troubleshooting. You should, therefore, consider accessing the Packet-Trace summary for a number of incoming packets.

```
Router# debug platform condition ingress
Router# debug platform packet-trace packet 2048 summary-only
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Pkt   Input             Output            State  Reason
0     Gi0/0/0           Gi0/0/0           DROP   402 (NoStatsUpdate)
1     internal0/0/rp:0  internal0/0/rp:0  PUNT   21  (RP<->QFP keepalive)
2     internal0/0/recycle:0  Gi0/0/0      FWD
```

The output shows that packets are dropped due to NAT configuration on Gigabit Ethernet interface 0/0/0, which enables you to understand that an issue is occurring on a specific interface. Using this information, you can limit which packets to trace, reduce the number of packets for data capture, and increase the level of inspection.

```
Router# debug platform packet-trace packet 256
Router# debug platform packet-trace punt
Router# debug platform condition interface Gi0/0/0
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Router# show platform packet-trace 15
Packet: 15          CBUG ID: 238
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:1
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 1166288346725 ns (06/06/2016 09:09:42.202734 UTC)
    Stop    : 1166288383210 ns (06/06/2016 09:09:42.202770 UTC)
Path Trace
  Feature: IPV4
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.64.68.3
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985
IOSd Path Flow: Packet: 15    CBUG ID: 238
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From CPP
  Feature: IP
    Pkt Direction: IN
    Source      : 10.64.68.122
    Destination : 10.64.68.255
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.64.68.122
    Destination : 10.64.68.255
    Interface   : GigabitEthernet0/0/0
  Feature: UDP
    Pkt Direction: IN
    src         : 10.64.68.122(1053)
    dst         : 10.64.68.255(1947)
    length      : 48

Router#show platform packet-trace packet 10
Packet: 10          CBUG ID: 10
Summary
```

```
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:0
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 274777907351 ns (01/10/2020 10:56:47.918494 UTC)
    Stop    : 274777922664 ns (01/10/2020 10:56:47.918509 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.78.106.2
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985

IOSd Path Flow: Packet: 10    CBUG ID: 10
  Feature: INFRA
    Pkt Direction: IN
Packet Rcvd From DATAPLANE
 Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.78.106.2
    Destination : 224.0.0.102
    Interface   : GigabitEthernet0/0/0

  Feature: UDP
    Pkt Direction: IN DROP
    Pkt : DROPPED
    UDP: Discarding silently
    src        : 881 10.78.106.2(1985)
    dst         : 224.0.0.102(1985)
    length      : 60

Router#show platform packet-trace packet  12
Packet: 12          CBUG ID: 767
Summary
  Input     : GigabitEthernet3
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 16120990774814 ns (01/20/2020 12:38:02.816435 UTC)
    Stop    : 16120990801840 ns (01/20/2020 12:38:02.816462 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 12.1.1.1
    Destination : 12.1.1.2
    Protocol    : 6 (TCP)
      SrcPort   : 46593
      DstPort   : 23
IOSd Path Flow: Packet: 12    CBUG ID: 767
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 12.1.1.1
    Destination : 12.1.1.2
    Interface   : GigabitEthernet3
  Feature: IP
    Pkt Direction: IN
    FORWARDEDTo transport layer
    Source        : 12.1.1.1
    Destination   : 12.1.1.2
    Interface     : GigabitEthernet3

  Feature: TCP
    Pkt Direction: IN
    tcp0: I NoTCB 12.1.1.1:46593 12.1.1.2:23 seq 1925377975 OPTS 4 SYN  WIN 4128

Router# show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
0     INJ.2                     Gi1                       FWD
1     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
2     INJ.2                     Gi1                       FWD
3     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
4     INJ.2                     Gi1                       FWD
5     INJ.2                     Gi1                       FWD
6     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
7     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
8     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
9     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
10    INJ.2                     Gi1                       FWD
11    INJ.2                     Gi1                       FWD
12    INJ.2                     Gi1                       FWD
13    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
14    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
15    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
16    INJ.2                     Gi1                       FWD
```

The following example displays the packet trace data statistics.

```
Router#show platform packet-trace statistics
Packets Summary
  Matched  3
  Traced   3
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     3
    Count       Code  Cause
    3           56    RP injected for-us control
  Drop     0
  Consume  0

          PKT_DIR_IN
             Dropped       Consumed       Forwarded
INFRA            0             0              0
TCP              0             0              0
UDP              0             0              0
IP               0             0              0
IPV6             0             0              0
ARP              0             0              0

         PKT_DIR_OUT
             Dropped       Consumed       Forwarded
INFRA            0             0              0
TCP              0             0              0
UDP              0             0              0
IP               0             0              0
```

```
IPV6             0             0             0
ARP              0             0             0
```

The following example displays packets that are injected and punted to the forwarding processor from the control plane.

```
Router#debug platform condition ipv4 10.118.74.53/32 both
 Router#Router#debug platform condition start
Router#debug platform packet-trace packet 200
Packet count rounded up from 200 to 256

Router#show platform packet-tracer packet 0
show plat pack pa 0
Packet: 0          CBUG ID: 674
Summary
  Input     : GigabitEthernet1
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 17756544435656 ns (06/29/2020 18:19:17.326313 UTC)
    Stop    : 17756544469451 ns (06/29/2020 18:19:17.326346 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      : <unknown>
    Source      : 10.118.74.53
    Destination : 198.51.100.38
    Protocol    : 17 (UDP)
      SrcPort   : 2640
      DstPort   : 500

IOSd Path Flow: Packet: 0    CBUG ID: 674
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
  Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.118.74.53
    Destination : 198.51.100.38
    Interface   : GigabitEthernet1

  Feature: IP
  Pkt Direction: IN
  FORWARDED To transport layer
    Source        : 10.118.74.53
    Destination   : 198.51.100.38
    Interface     : GigabitEthernet1

  Feature: UDP
  Pkt Direction: IN
  DROPPED
 UDP: Checksum error: dropping
 Source      : 10.118.74.53(2640)
 Destination : 198.51.100.38(500)

Router#show platform packet-tracer packet 2
Packet: 2          CBUG ID: 2

IOSd Path Flow:
  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
OPTS 4 ACK 2346709419 SYN  WIN 4128
```

```
  Feature: TCP
  Pkt Direction: OUT
  FORWARDED
 TCP: Connection is in SYNRCVD state
 ACK         : 2346709419
 SEQ         : 3052140910
 Source      : 198.51.100.38(22)
 Destination : 198.51.100.55(52774)


  Feature: IP
  Pkt Direction: OUTRoute out the generated packet.srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

  Feature: IP
  Pkt Direction: OUTInject and forward successful srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
OPTS 4 ACK 2346709419 SYN  WIN 4128
Summary
  Input     : INJ.2
  Output    : GigabitEthernet1
  State     : FWD
  Timestamp
    Start   : 490928006866 ns (06/29/2020 13:31:30.807879 UTC)
    Stop    : 490928038567 ns (06/29/2020 13:31:30.807911 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : internal0/0/rp:0
    Output      : <unknown>
    Source      : 172.18.124.38
    Destination : 172.18.124.55
    Protocol    : 6 (TCP)
      SrcPort   : 22
      DstPort   : 52774
  Feature: IPSec
    Result    : IPSEC_RESULT_DENY
    Action    : SEND_CLEAR
    SA Handle : 0
    Peer Addr : 55.124.18.172
    Local Addr: 38.124.18.172


Router#
```

CHAPTER 18

Encrypted traffic analytics

Encrypted Traffic Analytics (ET-Analytics) is used to identify malware communications in encrypted traffic. ET-Analytics uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. ET-Analytics uses Cisco NetFlow record fields to detect whether the packet flow has malware, and these NetFlow record fields include IDP (initial data packet) and SPLT (Sequence of Packet Length and Time).

Restrictions for encrypted traffic analytics

ET-Analytics is not supported on management interfaces, VRF-Aware Software Infrastructure (VASI) interface, and internal interfaces.

Information about encrypted traffic analytics

Data Elements for Encrypted Traffic

ET-Analytics uses intraflow metadata to identify malware components, maintaining the integrity of the encrypted traffic without the need for bulk decryption and without compromising on data integrity.

ET-Analytics extracts the following main data elements from the network flow: the sequence of packet lengths and times (SPLT), TLS-specific features, and the initial data packet (IDP). Cisco's Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network. Separate templates can be defined for each of the data elements.

Transport Layer Security (TLS) is a cryptographic protocol that provides privacy for applications. TLS is usually implemented with common protocols such as HTTP for web browsing or Simple Mail Transfer Protocol (SMTP) for email. HTTPS is the use of TLS over HTTP; this protocol is used to secure communication between a web server and client and is supported by most major web servers.

The TLS template is used to report several of the TLS parameters in use for a flow. These parameters help in finding the use of insecure cipher suites, out-of-date protocol version, and so on.

- Sequence of Packet Lengths and Times (SPLT) SPLT contains the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the inter-arrival times of those packets. SPLT can be represented as an array of packet sizes (in bytes) along with an array of times (in milliseconds) indicating the time since the previous packet was observed. The SPLT template is used to report packet size and timing information for a flow, which is useful to analyze encrypted traffic and find malicious flows or perform other classifications.
- Initial Data Packet (IDP) IDP obtains packet data from the first packet of a flow. It allows extraction of data such as an HTTP URL, DNS hostname/address, and other data elements. The TLS handshake is composed of several messages that contain unencrypted metadata used to extract data elements such as cipher suites, TLS versions, and the client's public key length. The IDP template is used to report packet data from the first data packet of a flow. This template allows collectors to perform application classification of a flow (for example, using Snort).

How to configure encrypted traffic analytics

Enabling encrypted traffic analytics on an interface

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**et-analytics**	Enters encrypted traffic analytics configuration mode.
Step 4	**ip flow-record destination** *ip-address port*	Specifies NetFlow collector IP address and port number. A maximum of four exporters is supported.
Step 5	**exit**	Returns to global configuration mode.
Step 6	**interface** *interface-id*	Specifies the interface and port number and enters interface configuration mode.
Step 7	**et-analytics enable**	Enables encrypted traffic analytics on this interface.
Step 8	**end**	Returns to privileged EXEC mode.

Example

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-record destination 192.0.2.1 2055
Device(config-et-analytics)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# et-analytics enable
Device(config-if)# end
```

Applying an ACL in the allowed list

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**et-analytics**	Enters encrypted traffic analytics configuration mode.
Step 4	**whitelist acl** *access-list*	The allowed list specifies the access list traffic. The access list can be a standard, extended, or named ACL.
Step 5	**exit**	Returns to global configuration mode.
Step 6	**ip access-list extended** *access-list*	Specifies a named extended access list and enters extended access list configuration mode.
Step 7	**permit ip** {*ip-address* | **any** | **host** | **object-group**}	Specifies the packets to forward to a source host or source IP address.
Step 8	**end**	Returns to privileged EXEC mode.

Example

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# whitelist acl eta_whitelist
Device(config-et-analytics)# exit
Device(config)# ip access-list extended eta_whitelist
Device(config-ext-nacl)# permit ip host 198.51.100.1 any
Device(config-ext-nacl)# permit ip any host 198.51.100.1
Device(config-ext-nacl)# permit ip host 198.51.200.1 any
Device(config-ext-nacl)# permit ip any host 198.51.200.1
Device(config-ext-nacl)# end
```

Verifying the encrypted traffic analytics configuration

The following **show** commands are used to see the platform encrypted traffic analytics, threat-visibility interfaces, FMAN FP global and interface information, and ET-analytics datapath information. Here are the sample outputs of the **show** commands.

```
Device# show platform hardware qfp active feature et-analytics data interface gigabitEthernet
 2

uidb handle: 0x3fe
Interface Name: GigabitEthernet2
```

```
Device# show platform hardware qfp active feature et-analytics data memory

  ET-Analytics memory information:

   Size of FO            : 3200 bytes
   No. of FO allocs      : 952903
   No. of FO frees       : 952902
```

```
Device# show platform hardware qfp active feature et-analytics data runtime

  ET-Analytics run-time information:

   Feature state         : initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   Flow CFG information  :   !Flow Table Infrastructure information internal to ETA!
       instance ID       : 0x0
       feature ID        : 0x0
       feature object ID : 0x0
       chunk ID          : 0x4
```

```
Device# show platform hardware qfp active feature et-analytics datapath stats export

  ET-Analytics 192.168.1.100:2055 Stats:
    Export statistics:
      Total records exported     : 2967386
      Total packets exported     : 1885447
      Total bytes exported       : 2056906120
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 805813
            responder->initiator : 418799
      Total SPLT records exported:
            initiator->responder : 805813
            responder->initiator : 418799
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 171332
            responder->initiator : 174860
ET-Analytics 172.27.56.99:2055 Stats:
    Export statistics:
      Total records exported     : 2967446
      Total packets exported     : 1885448
      Total bytes exported       : 2056909280
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 805813
            responder->initiator : 418799
      Total SPLT records exported:
            initiator->responder : 805813
            responder->initiator : 418799
   Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 171332
            responder->initiator : 174860
```

```
Device# show platform hardware qfp active feature et-analytics datapath stats flow

  ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 0
      feature object frees  : 0
      flow create requests  : 0
      flow create matching  : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests          : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```

CHAPTER 19

Configure traffic storm control

This topic describes how to configure the Traffic Storm Control feature on a Cisco 8100 Series Secure Routers, and contains the following sections:

Information about traffic storm control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. This feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.

This feature when configured ensures that the rate does not exceed the configured policer rate. When the traffic exceeds the configured rate, packets are dropped to control the traffic.

Prerequisites for traffic storm control

Ensure that you configure a separate storm control policer for each of the unicast, broadcast, and multicast traffic types. It is important to configure traffic storm control policer for each traffic type. For example, multicast traffic will not be controlled traffic if you do not configure a storm control policer for it. If a storm control policer is not configured for multicast traffic, the traffic load may exceed which is the expected behavior and that adds load to the customer network, especially when this traffic is caused by any misconfiguration or a cyberattack.

Limitations of traffic storm control

- Only bandwidth as percentage is used to measure traffic activity.
- Storm control is detected based on interface counter or hardware module reports (depending on the platform).
- Storm control is specific to physical interfaces.

- Storm control is only supported for unicast, broadcast, and multicast ingress traffic.

Configuring traffic storm control

Perform the following steps to configure traffic storm control:

Note Traffic storm control is disabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **storm-control** {**unicast** | **broadcast** | **multicast**} **level** {*level_high*} {*level_low*}
4. **storm-control action** { **shutdown** | **trap**}
5. **exit**

DETAILED STEPS

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	**storm-control** {**unicast** | **broadcast** | **multicast**} **level** {*level_high*} {*level_low*}
	Example:
	• **Unicast control**
	`Router(config-if)#storm-control unicast level 70.00 50.00`
	• **Broadcast Control**
	`Router(config-if)#storm-control broadcast level 70.00 50.00`
	• **Multicast Control**
	`Router(config-if)#storm-control multicast level 70.00 50.00`
		Specifies the interface level unicast, broadcast, or multicast storm control suppression level as a percentage of the total bandwidth. Here, the bandwidth is dependent on the operational speed.
		Unicast: Configures the known and unknown unicast storm control.
		Broadcast: Configures broadcast storm control.
		Multicast: Configures multicast storm control.
		Level: Specifies the threshold levels for broadcast, multicast, or unicast traffic.

	Command or Action	Purpose

Step 4	**storm-control action** { **shutdown** | **trap**}
	Example:
	`Router(config-if)#storm control action trap`
		Specifies the action to take when a storm occurs on a port.
		The traffic is blocked when it exceeds the threshold specified by configuration level, irrespective of the shutdown or SNMP trap being enabled or disabled.
		• **shutdown**: The interface enters err-disable state when traffic exceeds the threshold specified by configuration level.
		• **trap**: The interface sends an SNMP trap event when traffic exceeds the threshold specified by configuration level.
		Note
		You can enable the **shutdown** and **trap** actions simultaneously.

Step 5	**exit**	Exits interface configuration mode and returns the router to global configuration mode.

How to configure traffic storm control

How to configure traffic storm control

```
Router(config)#int gi0/1/0
Router(config-if)#storm-control unicast level 70.00 50.00
Router(config-if)#storm-control broadcast level 70.00 50.00
Router(config-if)#storm-control multicast level 70.00 50.00
Router(config-if)#storm-control action shutdown
Router(config-if)#storm-control action trap
```

CHAPTER 20

Configure bridge domain interfaces

The Cisco 8100 Series Secure Routers support the bridge domain interface (BDI) feature for packaging Layer 2 Ethernet segments into Layer 3 IP address.

Restrictions for bridge domain interfaces

The following are the restrictions pertaining to bridge domain interfaces:

- Only 4096 bridge domain interfaces are supported per system.
- For a bridge domain interface, the maximum transmission unit (MTU) size can be configured between 1500 and 9216 bytes.
- Bridge domain interfaces support only the following features:
  - IPv4 Multicast
  - QoS marking and policing. Shaping and queuing are not supported
  - IPv4 VRF
  - IPv6 unicast forwarding
  - Dynamic routing such as BGP, OSPF, EIGRP, RIP, IS-IS, and STATIC
  - Hot Standby Router Protocol (HSRP) from IOS XE 3.8.0 onwards.
  - Virtual Router Redundancy Protocol (VRRP) from IOS XE 3.8.0 onwards.
  - Flexible NetFlow

Note Flexible NetFlow is supported from Cisco IOS XE 17.18.1a and later releases.

- Bridge domain interfaces do not support the following features:
  - PPP over Ethernet (PPPoE)

- Bidirectional Forwarding Detection (BFD) protocol
- QoS
- Network-Based Application Recognition (NBAR) or Advanced Video Coding (AVC)

Information about bridge domain interface

Bridge domain interface is a logical interface that allows bidirectional flow of traffic between a Layer 2 bridged network and a Layer 3 routed network traffic. Bridge domain interfaces are identified by the same index as the bridge domain. Each bridge domain represents a Layer 2 broadcast domain. Only one bridge domain interface can be associated with a bridge domain.

Bridge domain interface supports the following features:

- IP termination
- Layer 3 VPN termination
- Address Resolution Protocol (ARP), G-ARP, and P-ARP handling
- MAC address assignment

Prior to configuring a bridge domain interface, you must understand the following concepts:

- Ethernet Virtual Circuit Overview
- Bridge Domain Interface Encapsulation
- Assigning a MAC Address
- Support for IP Protocols
- Support for IP Forwarding
- Packet Forwarding
- Bridge Domain Interface Statistics

Ethernet virtual circuit overview

An Ethernet Virtual Circuit (EVC) is an end-to-end representation of a single instance of a Layer 2 service that is offered by a provider. It embodies the different parameters on which the service is being offered. In the Cisco EVC Framework, the bridge domains are made up of one or more Layer 2 interfaces known as service instances. A service instance is the instantiation of an EVC on a given port on a given router. Service instance is associated with a bridge domain based on the configuration.

An incoming frame can be classified as service instance based on the following criteria:

- Single 802.1Q VLAN tag, priority-tagged, or 802.1ad VLAN tag
- Both QinQ (inner and outer) VLAN tags, or both 802.1ad S-VLAN and C-VLAN tags
- Outer 802.1p CoS bits, inner 802.1p CoS bits, or both

- Payload Ethernet type (five choices are supported: IPv4, IPv6, PPPoE-all, PPoE-discovery, and PPPoE-session)

Service instance also supports alternative mapping criteria:

- Untagged—Mapping to all the frames lacking a 802.1Q or 802.1ad header
- Default—Mapping to all the frames

Bridge domain interface encapsulation

Security Group classification includes both Source and Destination Group, which is specified by source SGT and DGT. SGT Based PBR feature provides the PBR route-map match clause for SGT/DGT based packet classification. SGT Based PBR feature supports configuration of unlimited number of tags, but it is recommended to configure the tags based on memory available in the platform.

An EVC provides the ability to employ different encapsulations on each Ethernet flow point (EFP) present in a bridge domain. A BDI egress point may not be aware of the encapsulation of an egress packet because the packet may have egressed from one or more EFPs with different encapsulations.

In a bridge domain, if all the EFPs have different encapsulations, the BDI must be untagged (using the no 802.1Q tag). Encapsulate all the traffic in the bridge domain (popped or pushed) at the EFPs. Configure rewrite at each EFP to enable encapsulation of the traffic on the bridge domain.

In a bridge domain, if all the EFPs have the same encapsulation, configure the encapsulations on the BDI using the encapsulation command. Enabling encapsulation at the BDI ensures effective pushing or popping of tags, thereby eliminating the need for configuring the rewrite command at the EFPs. For more information on configuring the encapsulations on the BDI, see the How to Configure a Bridge Domain Interface.

Assigning a MAC address

All the bridge domain interfaces on the Cisco 8100 Series Secure Routers chassis share a common MAC address. The first bridge domain interface on a bridge domain is allocated a MAC address. Thereafter, the same MAC address is assigned to all the bridge domain interfaces that are created in that bridge domain.

Note You can configure a static MAC address on a bridge domain interface using the **mac-address** command.

Support for IP protocols

Bridge domain interfaces enable the Cisco 8100 Series Secure Routers to act as a Layer 3 endpoint on the Layer 2 bridge domain for the following IP-related protocols:

- ARP
- DHCP
- HTTP
- ICMP
- NTP

- RARP
- SNMP
- TCP
- Telnet
- TFTP
- UDP

Support for IP forwarding

Bridge domain interface supports the following IP forwarding features:

- IPv4 input and output access control lists (ACL)
- IPv4 input and output QoS policies. The operations supported for the input and output service policies on a bridge domain interface are:
  - Classification
  - Marking
  - Policing
- IPv4 L3 VRFs

Packet forwarding

A bridge domain interface provides bridging and forwarding services between the Layer 2 and Layer 3 network infrastructure.

Layer 2 to layer 3

During a packet flow from a Layer 2 network to a Layer 3 network, if the destination MAC address of the incoming packet matches the bridge domain interface MAC address, or if the destination MAC address is a multicast address, the packet or a copy of the packet is forwarded to the bridge domain interface.

Note MAC address learning cannot not be performed on the bridge domain interface.

Layer 3 to layer 2

When a packet arrives at a Layer 3 physical interface of a router, a route lookup action is performed. If route lookup points to a bridge domain interface, then the bridge domain interface adds the layer 2 encapsulation and forwards the frame to the corresponding bridge domain. The byte counters are updated.

During a Layer 2 lookup on a bridge domain to which the bridge domain interface belongs, the bridge domain forwards the packets to the correct service instance based on the destination MAC address.

Link states of a bridge domain and a bridge domain interface

Bridge domain interface acts as a routable IOS interface on Layer 3 and as a port on a bridge domain. Both bridge domain interfaces and bridge domains operate with individual administrative states.

Shutting down a bridge domain interface stops the Layer 3 data service, but does not override or impact the state of the associated bridge domain.

Shutting down a bridge domain stops Layer 2 forwarding across all the associated members including service instances and bridge domain interfaces. The associated service instances influence the operational state of a bridge domain. Bridge domain interface cannot be operational unless one of the associated service instances is up.

Note Because a bridge domain interface is an internal interface, the operational state of bridge domain interface does not affect the bridge domain operational state.

Bridge domain interface initial state

The initial administrative state of a BDI depends on how the bridge domain interface is created. When you create a bridge domain interface at boot time in the startup configuration, the default administrative state for the bridge domain interface is up. It will remain in this state unless the startup configuration includes the shutdown command. This behavior is consistent with all the other interfaces. When you create a bridge domain interface dynamically at command prompt, the default administrative state is down.

Bridge domain interface link state

A BDI maintains a link state that comprises of three states: administratively down, operationally down, and up. The link state of a BDI is derived from two independent inputs: the BDI administrative state set by the corresponding users and the fault indication state from the lower levels of the interface states. It defines a BDI link state based on the state of the two inputs.

Fault Indication State	BDI Admin	
{start emdash} {end emdash}	**Shutdown**	**No Shutdown**
No faults asserted	Admin-down	Up
At least one fault asserted	Admin-down	Operationally-Down

Bridge domain interface statistics

For virtual interfaces, such as the bridge domain interface, protocol counters are periodically queried from the QFP.

When packets flow from a Layer 2 bridge domain network to a Layer 3 routing network through the bridge domain interface, the packets are treated as bridge domain interface input packets and bytes. When packets arrive at a Layer 3 interface and are forwarded through the bridge domain interface to a Layer 2 bridge domain, the packets are treated as output packets and bytes, and the counters are updated accordingly.

A BDI maintains a standard set of Layer 3 packet counters as the case with all Cisco IOS interfaces. Use the show interface command to view the Layer 3 packet counters.

The convention of the counters is relative to the Layer 3 cloud. For example, input refers to the traffic entry to the Layer 3 cloud from the Layer 2 BD, while output refers to the traffic exit from the Layer 3 cloud to the Layer 2 BD.

Use the **show interfaces accounting** command to display the statistics for the BDI status. Use the **show interface** <*if-name*> command to display the overall count of the packets and bytes that are transmitted and received.

Creating or deleting a bridge domain interface

When you define an interface or subinterface for a Cisco IOS router, you name it and specify how it is assigned an IP address. You can create a bridge domain interface before adding a bridge domain to the system. This new bridge domain interface will be activated after the associated bridge domain is configured.

Note When a bridge domain interface is created, a bridge domain is automatically created.

When you create the bridge domain interface and the bridge domain, the system maintains the required associations for mapping the bridge domain-bridge domain interface pair.

The mapping of bridge domain and bridge domain interface is maintained in the system. The bridge domain interface uses the index of the associated bridge domain to show the association.

Bridge domain virtual IP interface

The Virtual IP Interface (VIF) feature helps to associate multiple BDI interfaces with a BD instance. The BD-VIF interface inherits all the existing L3 features of IOS logical IP interface.

Note You must configure every BD-VIF interface with a unique MAC address and it should belong to a different VRF.

The Virtual IP Interface (VIF) feature has the following limitations:

- BD-VIF interface does not support IP multicast.
- Number of BD-VIF interfaces with automatically generated MAC address varies on the basis of platforms.
- BD-VIF Interface does not support MPLS.
- The maximum number of BD-VIF interfaces per bridge-domain and the total number of BD-VIF interface for per system vary based on the type of platforms.

How to configure a bridge domain interface

To configure a bridge domain interface, perform the following steps:

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface BDI** *{interface number}*
4. **encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]*
5. Do one of the following:
6. **match security-group destination tag** *sgt-number*
7. **mac address** *{mac-address}*
8. **no shut**
9. **shut**

DETAILED STEPS

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	**interface BDI** *{interface number}*
	Example:
	`Router(config-if)# interface BDI3`
		Specifies a bridge domain interface.

Step 4	**encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]* **Example:** `Router(config-if)# encapsulation dot1Q 1 second-dot1q 2`	Defines the encapsulation type. The example shows how to define dot1q as the encapsulation type.
Step 5	Do one of the following: **Example:** **ip address** *ip-address mask* **Example:** **Example:** **ipv6 address** *{X:X:X:X::X* **link-local**| *X:X:X:X::X/prefix [***anycast** | **eui-64***]* | **autoconfig** *[***default***]}*	Specifies either the IPv4 or IPv6 address for the bridge domain interface.

	Command or Action	Purpose

	Example:
	`Router(config-if)# ip address 10.2.2.1 255.255.255.0`
	Example:
	Example:
	`Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64`	

Step 6	**match security-group destination tag** *sgt-number* **Example:** `Router(config-route-map)# match security-group destination tag 150`	Configures the value for security-group destination security tag.

Step 7	**mac address** *{mac-address}*
	Example:
	`Router(config-if)# mac-address 1.1.3`
		Specifies the MAC address for the bridge domain interface.

Step 8	**no shut** **Example:** `Router(config-if)# no shut`	Enables the bridge domain interface.
Step 9	**shut** **Example:** `Router(config-if)# shut`	Disables the bridge domain interface.

Example

The following example shows the configuration of a bridge domain interface:

```
Router# configure terminal
Router(config)# interface BD-VIF interface-number
Router(config-if)# encapsulation dot1Q 1 second-dot1q 2
Router(config-if)# ip address ip-address mask
Router(config-if)# mac-address mac-address
Router(config-if)# no shut
Router(config-if)# exit
```

Displaying and verifying bridge domain interface configuration

SUMMARY STEPS

1. **enable**
2. **show interfaces bdi**
3. **show platform software interface fp active name**
4. **show platform hardware qfp active interface if-name**
5. **debug platform hardware qfp feature**
6. **platform trace runtime process forwarding-manager module**
7. **platform trace boottime process forwarding-manager module interfaces**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**show interfaces bdi** **Example:** `Router# show interfaces BDI3`	Displays the configuration summary of the corresponding BDI.
Step 3	**show platform software interface fp active name** **Example:** `Router# show platform software interface fp active name BDI4`	Displays the bridge domain interface configuration in a Forwarding Processor.
Step 4	**show platform hardware qfp active interface if-name** **Example:** `Router# show platform hardware qfp active interface if-name BDI4`	Displays the bridge domain interface configuration in a data path.
Step 5	**debug platform hardware qfp feature** **Example:** `Router# debug platform hardware qfp active feature l2bd client all`	The selected CPP L2BD Client debugging is on.

	Command or Action	Purpose
Step 6	**platform trace runtime process forwarding-manager module** **Example:** `Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module interfaces level info`	Enables the Forwarding Manager Route Processor and Embedded Service Processor trace messages for the Forwarding Manager process.
Step 7	**platform trace boottime process forwarding-manager module interfaces** **Example:** `Router(config)# platform trace boottime slot R0 bay 1 process forwarding-manager forwarding-manager level max`	Enables the Forwarding Manager Route Processor and Embedded Service Processor trace messages for the Route Processor Forwarding Manager process during bootup.

What to do next

For additional information on the commands and the options available with each command, see the Cisco IOS Configuration Fundamentals Command Reference Guide.

Configure bridge domain virtual IP interface

```
enable
configure terminal
[no] interface BD-VIF interface-number
  [ [no] vrf forwarding vrf-name]
  [ [no] mac address mac-address]
  [ [no] ip address ip-address mask]
  [ [no] ipv6 address {X:X:X:X::X link-local| X:X:X:X::X/prefix [anycast | eui-64] |
autoconfig [default]}]

exit
```

To delete BD-VIF interface, use the 'no' form of the command.

Associate VIF interface with a bridge domain

```
enable
configure terminal
bridge-domain bridge-domain number
[no] member BD-VIF interface-number
exit
```

To dissociate the VIF interface, use the 'no' form of the command.

Verify bridge domain virtual IP interface

All existing show commands for interface and IP interface can be used for the BD-VIF interface.

show interface bd-vif *bd-vif-id*

show ip interface bd-vif *bd-vif-id*

show bd-vif interfaces in fman-fp

show pla sof inter fp ac brief | i BD_VIF

Configuration example for bridge domain virtual IP interface

```
Detail sample:

interface Port-channel1
mtu 9000
no ip address
 !Ethernet service endpoint one per neutron network
service instance 1756 ethernet
  description 4e8e5957-649f-477b-9e5b-f1f75b21c03c
  encapsulation dot1q 1756
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1756
!
interface BD-VIF5001
no shutdown
vrf forwarding vrf5001
ip address 10.0.0.1 255.255.255.0
interface BD-VIF5002
no shutdown
vrf forwarding vrf5002
ip address 10.0.0.2 255.255.255.0

bridge-domain 1756
member Port-channel1 service-instance 1756
member bd-vif5001
member bd-vif5002
```

Configuring flexible netflow over a bridge domain virtual IP interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. {**ip** | **ipv6**}**flow monitor** *monitor-name* [**sampler** *sampler-name*] {**input** | **output**}
5. **exit**

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device (config)# interface BD-VIF 100`	Specifies an interface and enters interface configuration mode. Enter the BD-VIF number.

Step 4	{**ip** | **ipv6**}**flow monitor** *monitor-name* [**sampler** *sampler-name*] {**input** | **output**}
	Example:
	`Device(config-if)# ip flow monitor FLOW-MONITOR-1 input`
		Enables a Flexible NetFlow flow monitor for IP traffic that the router is receiving or transmitting on the interface.

Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.

Examples: Flexible netflow over a bridge domain virtual IP interface

The following is a sample output for the **show platform hardware qfp active interface if-name** command showing the QFP information and flow direction for flow monitors. The table below provides the key to the CLI output.

Configuration	Output
ip flow monitor <monitor-name> input	IPV4_INPUT_FNF_FIRST IPV4_INPUT_FNF_FINAL
ip flow monitor <monitor-name> output	IPV4_BDI_OUTPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> input	IPV6_INPUT_FNF_FIRST IPV6_INPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> output	IPV6_BDI_OUTPUT_FNF_FINAL

```
Device# show run interface bd-vif2
Building configuration...

Current configuration: 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
```

```
ipv6 flow monitor test2 output
ipv6 address 2001:DB8::1/32
end

Device# show platform hardware qfp active interface if-name BD-VIF 2
General interface information
  Interface Name: BD-VIF2
  Interface state: VALID
  Platform interface handle: 20
  QFP interface handle: 17
  Rx uidb: 262138
  Tx uidb: 262127
  Channel: 0
Interface Relationships

BGPPA/QPPB interface configuration information
  Ingress: BGPPA/QPPB not configured. flags: 0000
  Egress: BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
ipv6_input enabled.
ipv6_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:
2 GIC FIA state
66 PUNT INJECT DB
70 cpp_l2bd_svr
43 icmp_svr
45 ipfrag_svr
46 ipreass_svr
47 ipv6reass_svr
44 icmp6_svr
58 stile
Protocol 0 - ipv4_input
FIA handle - CP:0x55a7f59df038 DP:0x3fff1000
  IPV4_INPUT_DST_LOOKUP_ISSUE (M)
  IPV4_INPUT_ARL_SANITY (M)
  IPV4_INPUT_SRC_LOOKUP_ISSUE
  IPV4_INPUT_DST_LOOKUP_CONSUME (M)
  IPV4_INPUT_SRC_LOOKUP_CONSUME
  IPV4_INPUT_FOR_US_MARTIAN (M)
  IPV4_INPUT_STILE_LEGACY
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_LOOKUP_PROCESS (M)
  IPV4_INPUT_FNF_FINAL
  IPV4_INPUT_IPOPTIONS_PROCESS (M)
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x55a7f59df0d8 DP:0x3ffeff00
  IPV4_VFR_REFRAG (M)
  IPV4_OUTPUT_SRC_LOOKUP_ISSUE
  IPV4_OUTPUT_L2_REWRITE (M)
  IPV4_OUTPUT_SRC_LOOKUP_CONSUME
  IPV4_OUTPUT_STILE_LEGACY
  IPV4_OUTPUT_FRAG (M)
  IPV4_BDI_OUTPUT_FNF_FINAL.
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
Protocol 6 - ipv6_input
FIA handle - CP:0x55a7f59dee58 DP:0x3fff4300
  IPV6_INPUT_SANITY_CHECK (M)
  IPV6_INPUT_DST_LOOKUP_ISSUE (M)
  IPV6_INPUT_SRC_LOOKUP_ISSUE
  IPV6_INPUT_ARL (M)
  IPV6_INPUT_DST_LOOKUP_CONT (M)
  IPV6_INPUT_SRC_LOOKUP_CONT
  IPV6_INPUT_DST_LOOKUP_CONSUME (M)
  IPV6_INPUT_SRC_LOOKUP_CONSUME
  IPV6_INPUT_STILE_LEGACY
  IPV6_INPUT_FNF_FIRST
  IPV6_INPUT_FOR_US (M)
  IPV6_INPUT_LOOKUP_PROCESS (M)
  IPV6_INPUT_FNF_FINAL
  IPV6_INPUT_LINK_LOCAL_CHECK (M)
  IPV6_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 7 - ipv6_output
FIA handle - CP:0x55a7f59dee08 DP:0x3fff4b80
  IPV6_VFR_REFRAG (M)
  IPV6_OUTPUT_SRC_LOOKUP_ISSUE
  IPV6_OUTPUT_SRC_LOOKUP_CONT
  IPV6_OUTPUT_SRC_LOOKUP_CONSUME
  IPV6_OUTPUT_L2_REWRITE (M)
  IPV6_OUTPUT_STILE_LEGACY
  IPV6_OUTPUT_FRAG (M)
  IPV6_BDI_OUTPUT_FNF_FINAL
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV6_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
□
```

The following is a sample out of the **show flow monitor** [[**name**] [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] command showing the cache output in record format.

```
Device# show flow monitor name FLOW-MONITOR-1 cache format record

Cache type:  Normal
Cache size:  1000
Current entries:  4
High Watermark:  4
Flows added:  101
Flows aged:  97
- Active timeout (1800 secs) 3
- Inactive timeout  (15 secs) 94
- Event aged  0
- Watermark aged  0
- Emergency aged
IPV4 DESTINATION ADDRESS:
198.51.100.1 0
ipv4 source address: 10.10.11.1
trns source port: 25
trns destination port: 25
counter bytes: 72840
counter packets: 1821
IPV4 DESTINATION ADDRESS: 198.51.100.2
ipv4 source address: 10.10.10.2
trns source port: 20
trns destination port: 20
counter bytes: 3913860
counter packets: 7326
IPV4 DESTINATION ADDRESS: 198.51.100.200
```

```
ipv4 source address: 192.168.67.6
trns source port: 0
trns destination port: 3073
counter bytes: 51072
counter packets: 1824


Device# show flow monitor name FLOW-MONITOR-2 cache format record

Cache type:  Normal
Cache size: 1000
Current entries: 2
High Watermark: 3
Flows added: 95
Flows aged: 93
- Active timeout (1800 secs) 0
- Inactive timeout (15 secs) 93
- Event aged 0
- Watermark aged 0
- Emergency aged 0
IPV6 DESTINATION ADDRESS: 2001:DB8:0:ABCD::1
ipv6 source address: 2001:DB8:0:ABCD::2
trns source port: 33572
trns destination port: 23
counter bytes: 19140
counter packets: 349
IPV6 DESTINATION ADDRESS: FF02::9
ipv6 source address: 2001:DB8::A8AA:BBFF:FEBB

trns source port: 521
trns destination port: 521
counter bytes: 92
counter packets: 1
```

The following is a sample out of the **show flow interface** command showing the flow status for an interface.

```
Device# show flow interface BD-VIF2001

Interface GigabitEthernet0/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Input
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction:    Input traffic(ipv6): on

Device# show flow interface BD-VIF2002

Interface GigabitEthernet1/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Output
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction:    Input traffic(ipv6): on
```

The following is a sample output of the **show platform hardware qfp active interface if-name | in FNF** command showing the QFP information and flow direction for flow monitors in Flexible NetFlow configuration. The table below provides the key to the CLI output.

Configuration	Output
ip flow monitor <monitor-name> input	IPV4_INPUT_FNF_FIRST IPV4_INPUT_FNF_FINAL

Configuration	Output
ip flow monitor <monitor-name> output	IPV4_BDI_OUTPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> input	IPV6_INPUT_FNF_FIRST IPV6_INPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> output	IPV6_BDI_OUTPUT_FNF_FINAL

```
Device# show run interface bd-vif2
Building configuration...

Current configuration : 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
ipv6 flow monitor test2 output
ipv6 address 2001::8/64
end
 Device# show platform hardware qfp active interface if-name BD-VIF 2  | in FNF
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_FNF_FINAL
  IPV4_BDI_OUTPUT_FNF_FINAL.
  IPV6_INPUT_FNF_FIRST
  IPV6_INPUT_FNF_FINAL
  IPV6_BDI_OUTPUT_FNF_FINAL
```

The **clear flow monitor name** *monitor-name* [**cache** [**force-export**] | **force-export** | **statistics**] command clears a Flexible NetFlow flow monitor, flow monitor cache, or flow monitor statistics, and can be used to force the export of the data in the flow monitor cache.

For more details on configuring Flexible NetFlow, see the Flexible NetFlow Configuration Guide, Cisco IOS XE 17.

CHAPTER 21

Cisco LTE and 5G on Cisco 8100 Series Secure Routers

This chapter provides an overview of the software features and configuration information for Cisco LTE/5G on the Cisco 8100 Series Secure Routers.

For more information on Cisco LTE/5G SKUs, faceplates, and LED descriptions, see the Cisco 8100 Series Secure Routers Hardware Installation Guide.

Overview of Cisco LTE and 5G

Only the C8151-G2 and C8161-G2 routers support Cisco LTE and 5G using Pluggable Interface Modules (PIMs):

Table 18: Pluggable Modules of the Cisco 8100 Series Secure Routers

Pluggable Interface Modules	Pluggable Interface Modules technology
P-5GS6-R16SA-GL	5G Sub-6 GHz Pluggable Interface Module
P-LTEA7-NA	CAT7 LTE Pluggable for North America
P-LTEA7-JP	CAT7 LTE Advanced PIM for Japan
P-LTEA7-EAL	CAT7 LTE Advanced PIM for EMEA, APAC, LATAM

Cisco LTE/5G supports the following modes:

- **5G** —5G is the next step in the evolution of mobile communications. It is a new global wireless standard after 1G, 2G, 3G, and 4G networks. 5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra low latency, increased availability, massive network capacity, more reliability, and a more uniform user experience to more users.
- **4G LTE** —4G LTE mobile specification provides multi-megabit bandwidth, more efficient radio network, latency reduction, and improved mobility. LTE solutions target new cellular networks. These networks initially support up to 300 Mb/s peak rates in the downlink and up to 50 Mb/s peak rates in the uplink.

The following table describes the Cisco 4G LTE Cat 7 SKUs:

Table 19: Cisco 4G LTE Cat 7 SKUs

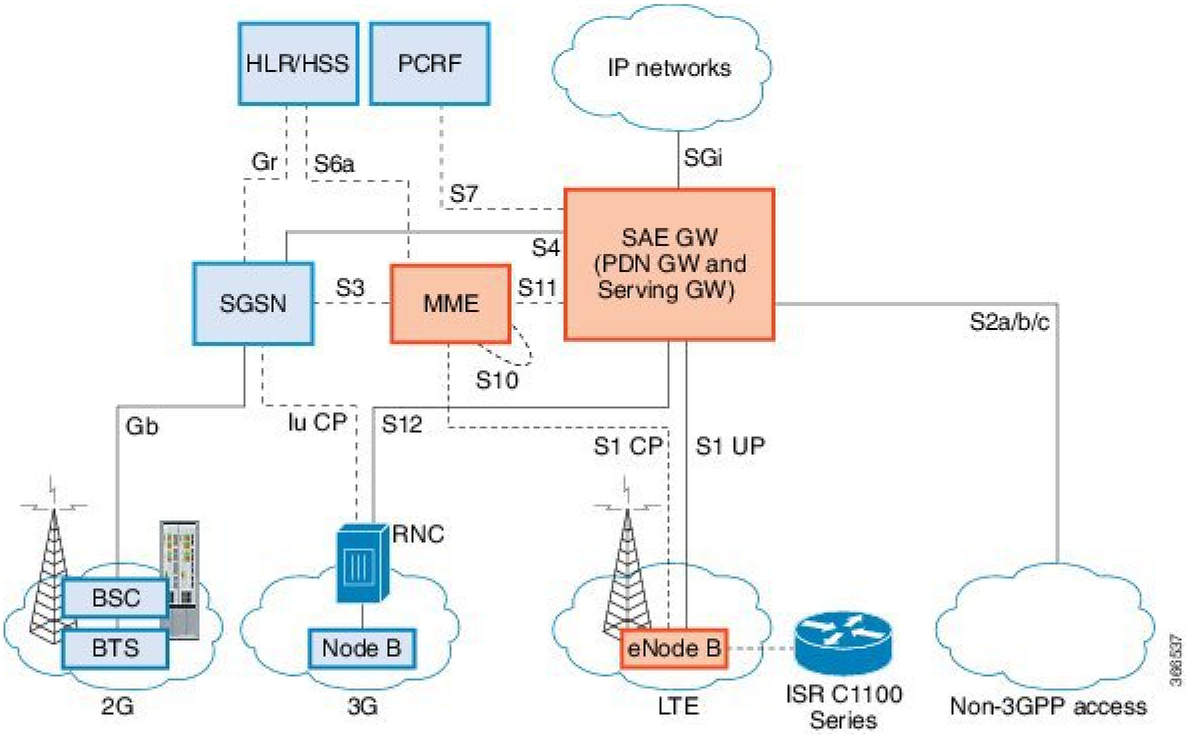
Radio Access Technology (RAT)	Bands
LTE	B2, B4, B5, B7, B12, B13, B14, B25, B26, B41, B42, B43, B48, B66, B71
WCDMA	B2, B4, B5

Table 20: Bands supported for Cisco 5G modems

Radio Access Technology (RAT)	Bands
5GNR Sub-6G	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29, n30, n38, n39, n40, n41, n48, n66, n70, n71, n75, n76, n77, n78, n79
LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B18, B19, B20, B21, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, B71

The following figure explains the 4G LTE packet core network architecture.

Figure 2: 4G LTE Packet Core Network Architecture



Gateways	The Serving Gateway (SGW) routes and forwards user data packets, while also acting as the mobility anchor for the user plane, and is the anchor for mobility between LTE and other 3GPP technologies. The Packet Data Network (PDN) Gateway (PGW) provides connectivity from the User Equipment (UE) to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one PGW for accessing multiple PDNs. The PGW performs policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. Another key role of the PGW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO). The System Architecture Evolution GW (SAE GW) is the entity that covers the PGW and SGW functionality in the Evolved Packet Core (EPC).
RNC	The Radio Network Controller (RNC) is responsible for controlling the Radio Access Network (RAN) that are connected to it. The RNC carries out radio resource management and some of the mobility management functions and is the point where encryption is done before user data is sent to and from the mobile. The RNC connects to the Circuit-Switched Core Network through the Media Gateway (MGW).
BTS	Base Transceiver Station.
BSC	Base Station Controller.
SGSN	Service GPRS Support Node.

Prerequisites for configuring Cisco LTE and 5G

- If the signal is not good at the router, use the Cisco offered antenna accessories and extension cables to place the antenna away from router in a better coverage area.
- You must have LTE and 5G network coverage where your router is physically placed. For a complete list of supported carriers.
- You must subscribe to a service plan with a wireless service provider and obtain a Subscriber Identity Module (SIM) card. Only micro SIM is supported.
- You must install the SIM card before configuring the LTE/5G on Cisco Cisco 8100 Series Secure Routers.
- The standalone antenna that supports GPS capabilities must be installed for the GPS feature to work. See the Cisco 4G Indoor/Outdoor Active GPS Antenna (GPS-ACT-ANTM-SMA) document for installation information.

Restrictions for configuring Cisco LTE and 5G

- Currently, cellular networks support only user initiated bearer establishment.
- Due to the shared nature of wireless communications, the experienced throughput varies depending on the number of active users or congestion in a given network.
- Cellular networks have higher latency compared to wired networks. Latency rates depend on the technology and carrier. Latency also depends on the signal conditions and can be higher because of network congestion.
- CDMA-EVDO, CDMA-1xRTT, and GPRS technology modes are not supported.
- Any restrictions that are part of the terms of service from your carrier.
- SMS—Only one text message up to 160 characters to one recipient at a time is supported. Larger texts are automatically truncated to the proper size before being sent.
- It is strongly recommended that you configure SNMP V3 with authentication/privacy.

Cisco LTE and 5G features

Cisco LTE and 5G supports the following major features:

- Global Positioning System (GPS) and National Marine Electronics Association (NMEA) streaming.
- Short Message Service (SMS)
- SIM lock and unlock capabilities
- Dual SIM
- Auto SIM
- Public Land Mobile Network (PLMN) selection

- IPv6
- Multiple PDN
- LTE Link Recovery

The following sections explains the Cisco LTE/5G features:

4G GPS and NMEA

Active GPS is supported on the SubMiniature version A (SMA) port. Active GPS antenna is supported only in the standalone mode. An Active GPS antenna includes a built-in low-noise Amplifier that provides sufficient gain to overcome coaxial cable losses while providing the proper signal level to the GPS receiver. Active GPS antennae require power from the GPS receiver SMA port to operate. See the Connecting to a server hosting a GPS application, on page 189 for more information.

National Marine Electronics Association (NMEA) streams GPS data either from a LTE and 5G through a virtual COM port and a TCP/IP Ethernet connection to any marine device (such as a Windows-based PC) that runs a commercially available GPS-based application.

The following GPS and NMEA features are supported on the Cisco LTE and 5G:

- GPS standalone mode (satellite-based GPS)
- Cisco IOS CLI display coordinates.
- External application displays router map location
- The Cisco LTE/5G only supports NMEA over IP and uses show commands in the platform

Note Assisted GPS mode is not supported.

For instructions on setting up the GPS antenna, see the Cisco 4G Indoor/Outdoor Active GPS Antenna (GPS-ACT-ANTM-SMA) document.

Connecting to a server hosting a GPS application

You can feed the NMEA data to a remote server that hosts the GPS application. The server can be connected to the router either directly using an Ethernet cable or through a LAN or WAN network. If the application supports serial port, run a serial port emulation program to create a virtual serial port over the LAN or WAN connection.

To connect a Cisco LTE/5G through IP to a PC, perform the following steps:

1. Connect the PC to the router using an Ethernet cable.
2. Ensure that the PC and router can ping.
3. Launch the serial port redirector on the PC.
4. Create a virtual serial port that connects to the NMEA port on the router.
5. Launch **Microsoft Streets & Trips** on your PC.
6. Select the GPS Menu.

7. Click Start Tracking.
8. If you have acquired a location fix from the **show cellular 0/2/0 gps** command output on the router, the current location is plotted on the graph, and a reddish brown dotted cursor with a circle around it is seen on the map.

Dual SIM card

SIM card primary slot is selected when router boots up or when NIM reloads. The default slot is 0. If SIM card is not present in the primary slot, select the alternative slot if SIM card is present.

```
controller cellular 0/2/0
lte sim primary slot <slot#>
```

If the active SIM card loses connectivity to the network a failover to the alternative SIM card slot occurs.

By default the failover timer is two minutes. The failover timer can be set from 1 to 7 minutes.

```
controller cellular 0/2/0
lte failovertimer <3-7>
```

You can also manually switch the SIM slot via the command line interface.

```
cellular 0/2/0 lte sim activate slot <0-1>
```

Auto SIM

The Auto SIM feature detects the SIM and loads the corresponding firmware.

When auto SIM is enabled, it is said to be in auto SIM mode and when disabled, it is known as Manual mode. In auto SIM mode, the modem selects the right carrier firmware from the list of firmware's available. When in manual mode, you can select the firmware manually. Modem resets every time you make a config change from auto SIM enabled to disabled or vice-versa.

Note Auto SIM is always enabled by default.

Enable auto SIM

Auto SIM is enabled by default.

Example: List the firmware when auto SIM is enabled

```
Router# show cellular 0/2/0 firmware
firmware          Idx Carrier      FwVersion      PriVersion   Status
 1   ATT          192.0.2.1        002.035_000  Inactive
 2   GENERIC      192.0.2.2        002.035_000  Active
 3   ROGERS       192.0.2.3        001.012_000  Inactive
 4   SPRINT       192.0.2.4        002.012_000  Inactive
 5   VERIZON      192.0.2.5        002.042_000  Inactive

Firmware Activation mode  =  AUTO
```

Disable auto SIM

SUMMARY STEPS

1. **configure terminal**
2. **controller cellular** *slots / sub-slots / interface*
3. **no lte firmware auto-sim**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**controller cellular** *slots / sub-slots / interface* **Example:** `Router(config)# controller cellular 0/2/0`	Specifies the controller interface.
Step 3	**no lte firmware auto-sim** **Example:** `Router(config-if)# no lte firmware auto-sim`	Disable auto SIM.

Example: List the firmware when auto SIM is disabled

```
Router# show cellular 0/2/0 firmware
 Idx Carrier      FwVersion    PriVersion   Status
 1   ATT          192.0.2.1  002.035_000  Active
 2   GENERIC      192.0.2.2  002.035_000  Inactive
 3   ROGERS       192.0.2.3  001.012_000  Inactive
 4   SPRINT       192.0.2.4  002.012_000  Inactive
 5   VERIZON      192.0.2.5  002.042_000  Inactive


Firmware Activation mode  =  Manual
```

Firmware activation

Note

- To check the carrier firmwares that are available to be switched to, use the **show cellular slots/sub-slots/interface firmware** command.
- To manually switch the carrier firmware, disable the auto SIM.
- For P-5GS6-GL (FN980), use **cellular slots/sub-slots/interface lte mno-activate <1-10>|auto** command.

SUMMARY STEPS

1. **cellular** *slots/sub-slots/interface* **lte** **firmware-activate** *firmware-index*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**cellular** *slots/sub-slots/interface* **lte** **firmware-activate** *firmware-index* **Example:** `Router# cellular 0/2/0 lte firmware-activate 1`	Activates the firmware index. **Note** For the LTE/5G, the *unit* argument identifies the slot, subslot, and the interface separated by slashes (0/2/0).

Using a SIM Card

Cisco LTE or 5G needs an active SIM card provided by a service provider. The SIM cards are usually provided in an unlocked state so that it can be used without a Personal Identification Number (PIN). If the SIM is unlocked, it can be inserted into a LTE or 5G and used without an authorization code.

The SIM can be initially locked with a PIN code (4 to 8 digits s long) defined by the service provider. Contact your service provider for the PIN code.

The SIM-lock feature allows a SIM to be locked or unlocked with a PIN code so that it is used only in an authorized device. Perform the SIM lock and unlock procedures using the Cisco IOS CLI through a console or Telnet/SSH to the router.

After the SIM is locked, it cannot initiate a call unless authentication is done using the same PIN. Authentication is done automatically by Cisco IOS through configuration of the PIN. This mandatory configuration for automatic SIM authentication is done using the Cisco IOS CLI as part of the router startup configuration.

After the Cisco IOS configuration is in place, the router can initiate an LTE connection. The router uses the configured PIN to authenticate prior to the LTE connection. If the Cisco IOS PIN configuration is missing or if the PIN is incorrect, the SIM authentication fails and the connection is not initiated.

If the locked SIM is moved to a different router or to another device, or if the LTE or 5G in which the locked SIM resides is moved to a different LTE or 5G slot in the same router, the router configuration should be changed. The configuration is associated with the cellular controller that is specific to an router LTE or 5G slot number. This will ensure that the SIM card will not be used in any unauthorized device, or, if there are multiple LTE or 5G in a single router, that the appropriate PIN is applied to each LTE or 5G SIM. An authentication command (with the same PIN used to lock the SIM) must be defined on the new device or on the new cellular controller slot to successfully initiate the LTE connection.

The following procedures are used to configure a SIM:

Caution It is very important to use the correct PIN after it is configured. The SIM card will be blocked if the wrong PIN is entered three consecutive times on a locked SIM during authentication or when trying to unlock a locked SIM. You can unblock a blocked SIM card using the PUK code. Contact your service provider for the PUK code. Use the **cellular** <*slot*> **lte sim unblock** <*PUK code*> <*new PIN code*> command to unblock the SIM.

Change the PIN

Ensure to enter the correct PIN, the SIM card gets blocked if the wrong PIN is entered three consecutive times.

SUMMARY STEPS

1. **cellular** *slots subslots interface* **lte sim change-pin** *current-pin new-pin*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**cellular** *slots subslots interface* **lte sim change-pin** *current-pin new-pin* **Example:** `Router# cellular 0/2/0 lte sim lock 1111 1234`	Locks or unlocks the SIM card using a PIN code. **Note** Locks or unlocks the SIM card using a PIN code. *pin*—A code (4 to 8 digits long) provided by your service provider to lock or unlock the SIM card. **Note** SIM should be in locked state when the PIN is being changed.

Locking and unlocking a SIM card using a PIN

Perform this task to lock or unlock a SIM card given by your service provider. Make sure you enter the correct PIN, the SIM card gets blocked if the wrong PIN is entered three consecutive times.

Procedure

	Command or Action	Purpose
Step 1	**cellular** *unit* **lte sim** {**lock** | **unlock**} *pin* **Example:**	Locks or unlocks the SIM card using a PIN code. **Note**

	Command or Action	Purpose
	`Router# cellular 0/2/0 lte sim lock 1111`	*pin*—A code (4 to 8 digits long) provided by your service provider to lock or unlock the SIM card.

Configure CHV1 for unencrypted level 0

Procedure

	Command or Action	Purpose
Step 1	**cellular** *slots subslots interface* **lte sim lte sim authenticate 0 pin** **Example:** `Router# controller cellular 0/0/0`	Enters the cellular controller configuration mode Use either of these commands:**lte sim authenticate 0 pin** or **lte sim authenticate 0 pin slot {0 | 1}**

Configure CHV1 for unencrypted level 7

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode. When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command.

Note After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration. A SIM should be locked for SIM authentication to work.

Procedure

	Command or Action	Purpose
Step 1	**service password-encryption** **Example:** `Router(config)# service password-encryption`	Enables password encryption.
Step 2	*username* **privilege** *var password pin* **Example:** `Router(config)# username SIM privilege 0 password 1111`	**Note** Creates username and password. name - specifies the username.*pin*—A 4 to 8 digits PIN code.
Step 3	**do show run | i name** **Example:**	Shows the username configuration line with the encrypted level 7 PIN for the username created in Step 3 (user “SIM”

	Command or Action	Purpose
	`Router(config)# do show run | i SIM`	in the example shown). Copy the scrambled password for use in Step 6 (as the PIN).
Step 4	*username* **privilege 0** *password* *pin* **Example:** `Router(config)# controller cellular 0/0/0`	Enters the cellular controller configuration mode.

Step 5	**lte sim authenticate 7***pin* `OR`**lte sim authenticate 7 pin slot {0 | 1}**
	Example:
	`Router(config-controller)# lte sim authenticate 7 055A575E70`
		Authenticates the SIM CHV1 code by using the encrypted keyword 7 and the scrambled PIN from Step 4. The PIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call.
		Note
		The slot keyword and its options are available only on platforms that supports Dual-SIM feature.

Step 6	**exit** **Example:** `Router(config-controller)# exit`	(Optional) Exits the cellular controller configuration mode.
Step 7	**no username***name* **Example:** `Router(config-controller)# no username SIM`	(Optional) Removes the username and password created in Step 3.
Step 8	**no service password-encryption***name* **Example:** `Router(config-controller)# no service password-encryption`	(Optional) Removes the username and password created in Step 3.

Verifying the security information of a modem

Perform this task to verify the security information of a modem.

Note For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

Procedure

	Command or Action	Purpose
Step 1	**show cellular** *unit* **security** **Example:**	Shows the security information of the modem, including the SIM lock status.

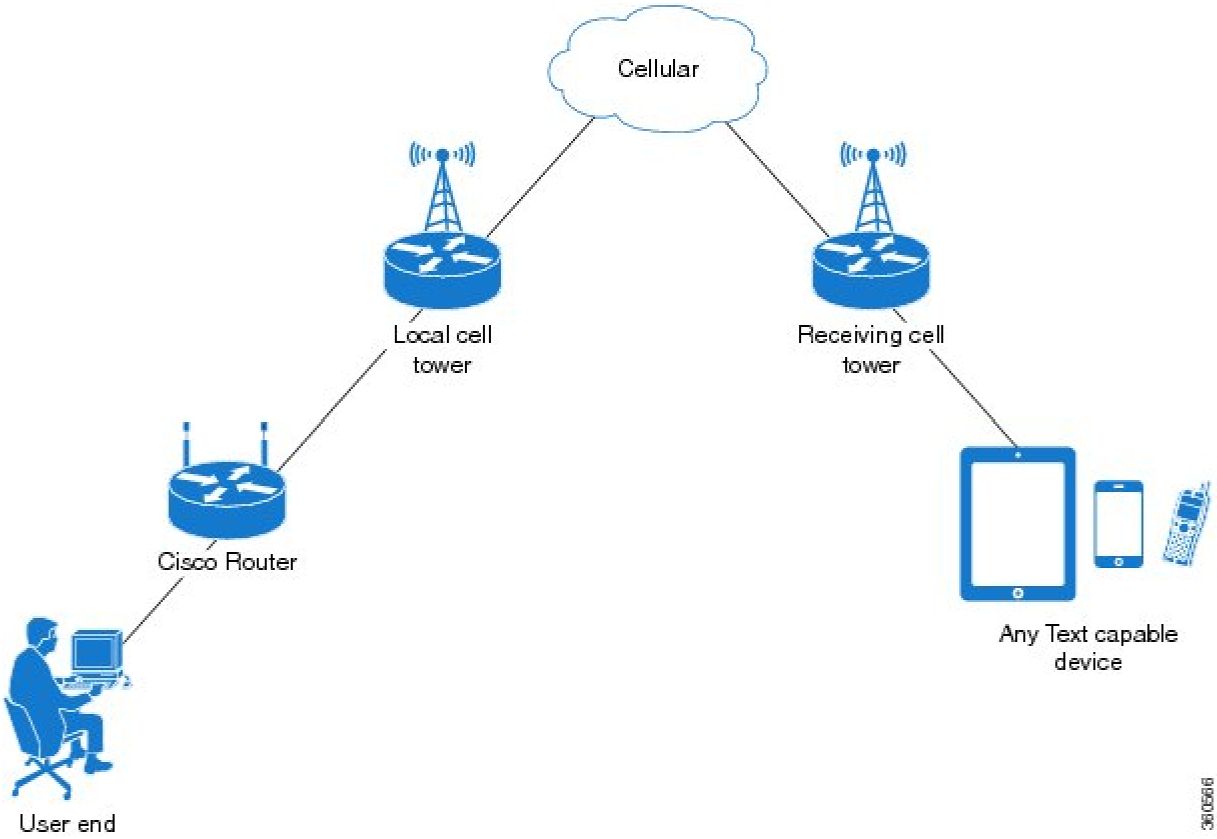
	Command or Action	Purpose
	`Router# show cellular 0/2/0 security`	

Short Message Service capabilities

Cisco LTE/5G support receiving, transmitting, archiving, and deleting of Short Message Service (SMS) messages.

A sending device behind a Cisco LTE/5G transmits an SMS text message over the 4G cellular link through cellular towers until it the message reaches the recipient's router, which then notifies the recipient device, such as a cell phone. The receiving device uses the same process to return a reply to the sending device. The following figure describes the flow from a mobile device to a sending device. For SMS transmission to work, end users must have a text-capable device, and optionally, a text plan. If end users do not have a text plan, standard SMS rates apply to their text transmissions.

Figure 3: SMS Network



Provision data account

One or more modem data profiles can be created to provision a modem on a LTE/5G SKU. An active wireless account with a service provider with one or more (dual) SIM cards must be installed. The modem data profile is pre-configured on the modem.

The following tasks are used to verify the signal strength and service availability of the modem and to create, modify, and delete modem data profiles:

IP multimedia subsystem profiles

IP Multimedia Subsystem (IMS) profiles establish a session, and are a part of the modem configuration and are stored in the modem's NVRAM. An IMS network is an access-independent and standard-based IP connectivity service that enables different types of multimedia services to end users using common Internet-based protocols.

LTE and 5G LEDs

The following table describes the LED behavior in LTE/5G.

Table 21: LTE and 5G LED indicators

LED	Color/Bar and description	
LTE SIM(0) & SIM(1)	Green (Solid)	Modem up, SIM installed and active
	Green Blink	LTE data activity
	Off	Modem not up; or modem up and no SIM
	Amber (Solid)	Modem up, SIM installed but not active
RSSI - Uses Bars for LED Indication	Four Bar	High RSSI >= -69dBm
	Three Bar	Medium RSSI, -89dBm <> -70dBm
	Two Bar	Low RSSI, -99dBm <> -90dBm
	One Bar	RSSI <= -100dBm
	0 or No Bar	No Service
SERVICE - Uses Color Indication	Green(solid)	LTE signal present (RSSI LEDs will be Green)
	Amber(solid)	2G/3G signal present (RSSI LEDs will be Amber)
	No Color	No service detected.
GPS	Green (Solid)	GPS coordinates are obtained.
	Off	GPS is disabled, GPS is enabled without GPS mode and NMEA configuration, or GPS is acquiring

Cisco LTE and 5G features

Cisco LTE and 5G supports the following major features:

- Global Positioning System (GPS) and National Marine Electronics Association (NMEA) streaming.
- Short Message Service (SMS)
- SIM lock and unlock capabilities
- Dual SIM
- Auto SIM
- Public Land Mobile Network (PLMN) selection
- IPv6
- Multiple PDN
- LTE Link Recovery

The following sections explains the Cisco LTE/5G features:

Verifying the cellular modem link recovery configuration

To determine if the cellular modem link recovery is enabled, use the **show controller cellularunit** command. In this example, the cellular modem link recovery feature related information is highlighted.

```
Router# show controller cellular 0/2/0Interface Cellular0/2/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

Cellular Modem Configuration
==============================
Modem is recognized as valid
Power save mode is OFF
manufacture id =  0x00001199     product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status =  NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
---------------------------
SIM 0 is present
SIM 1 is not present
SIM 0 is active SIM

Module Reload Statistics
-------------------------
Soft OIR reloads = 0
Hard OIR reloads = 0
-------------------------

Modem Management Statistics
---------------------------
```

```
Modem resets = 1
Modem timeouts = 0
Link recovery is ON

Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6

Link recovery count is 0
```

When the cellular modem link recovery occurs and modem is power cycled, you can see the %CELLWAN-2-MODEM_DOWN message on the console logs and additionally there is a %CELLWAN-2-LINK_RECOVERY message which indicates that action has been taken by the cellular modem link recovery feature.

Whenever the cellular modem link recovery has occurred, it updates the Modem timeouts counter under the Modem Management Statistics section of the show controller cellular unit command output. Modem parameters at the last timeout section has information that helps to identify the cause of the issue that triggered link recovery

In the following example log, the messages, modem time out counter, and modem parameters at the last time out are highlighted.

*Jul 19 17:15:18.980 PDT: %CELLWAN-2-LINK_RECOVERY: Cellular0/1/0: Cellular Modem has been power cycled

```
Router#show controller Cellular 0/2/0
Interface Cellular0/2/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

Cellular Modem Configuration
==============================
Modem is recognized as valid
Power save mode is OFF
manufacture id =  0x00001199     product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status =  NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
---------------------------
SIM 0 is present
SIM 1 is not present
SIM 0 is active SIM

Module Reload Statistics
-------------------------
Soft OIR reloads = 0
Hard OIR reloads = 0
-------------------------
 Modem Management Statistics
---------------------------
Modem resets = 1
Modem user initiated resets = 0
Modem user initiated power-cycles = 0
Modem timeouts = 1
Modem parameters at the last timeout:
```

```
         LTE first time attach State was No
         Radio Interface Technology Mode was AUTO
         Operating Mode was Online
         RSSI was -0 dBm
         Packet switch domain status was Not Attached
         Registration state(EMM) was Not Registered
         Downlink traffic was not present
Link recovery is ON
Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6
```

Guidelines for Creating, Modifying, or Deleting Modem Data Profiles

Customized profiles (Access Point Name (APN) in mobile networks) can be created and used on Cisco LTE/5G SKU's. Maximum number of profiles that can be created are 16.

Cisco SKU's shipping with specific carrier provisioning file (Can be found in Carrier label under "show cellular <slot> hardware"), default profiles are already populated and can be deployed readily.

In all other cases where profile configurations are not available, separate profiles should be created with required parameters.

You can create multiple profiles on Cisco LTE/5G. The following are the default internet profile numbers for the modems:

Modem	Profile Number
EM7430	Profile 1
EM7455 (Verizon or Sprint)	Both Profile 1 and Profile 3
EM7455 (AT&T or other SP's)	Profile 1

Follow these guidelines when you configure a data profile using EXEC mode or Config mode :

- You do not have to make any profile-related changes if your modem comes with a data profile, for instance, AT&T, Sprint and Verizon.
- If any profile parameter changes are required for a connection type, the changes will likely be carried out in the default profiles.
- To configure different profile types and use them for a different connection, you can create separate profiles with different parameters (for instance, APN names). Note that only one profile is active at a given time.
- Use the **show cellular <unit> profile** command to view the data profile. An asterisk(*) symbol is displayed against the data profile. Double asterisk(**) symbol is displayed against the attach profile.
- The data profile is used to set up a data call. If you want to use a different profile, that profile needs to be made the default one. Use the **lte sim data-profile** *number* command to change the default profile under **controller cellular 0/2/0**.
- Profile 1 is reserved for non-network slicing use only. When using Profile 1, only a single slice is supported on Profile 2, and the data-profile CLI configuration is not required. Profiles 2 and above are designated

for network slicing (NS) functionality. For these profiles, the data-profile CLI must be configured under **controller cellular 0/x/0**. Each data profile from Profile 2 onwards maps to an individual network slice and corresponding cellular interface.

Create, modify, or delete data profiles using EXEC mode

Customized profiles (Access Point Name (APN) in mobile networks) can be created and used on Cisco LTE/5G SKU's. Maximum number of profiles that can be created are 16.

Cisco SKU's shipping with specific carrier provisioning file (can be found in carrier label under **show cellular** *slot* **hardware**, default profiles are already populated and can be deployed readily.

Note For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

Procedure

	Command or Action	Purpose
Step 1	**cellular** *unit* **lte profile** *[***create** | **delete***] profile-number [apn [authentication [username password [bearer-type]]]]* **Example:** `Router# cellular 0/2/0 lte profile create 2 apn.com pap username pwd ipv4`	Creates, modifies, or deletes a modem data profile in the privileged EXEC mode. • The *profile-number* argument specifies the profile number created for the modem. • (Optional) The *apn* argument specifies an Access Point Name (APN). An APN is provided by your service provider. Only a single APN can be specified for a single profile. • (Optional) The *authentication* parameter specifies the authentication type used. Acceptable parameters are **chap**, **none** (no authentication), **pap**, and **pap_chap** (PAP or CHAP authentication). • (Optional) The *username* and *password* arguments are given by a service provider. These are mandatory when an authentication type other than **none** is used. • (Optional) The *PDN* type parameter specifies the type of packet data session established with mobile network using this profile. Acceptable parameters are: **ipv4** **ipv6** and **ipv4v6** (IPv4 and IPv6). The **show cellular** *slot* profile displays configured profile list. **Note** Single asterisk(*) displayed against data profile. Double asterisk(**) displayed against attached profile.

	Command or Action	Purpose
Step 2	**cellular** *unit* **lte profile** [**create** | **delete**] *profile-number [apn [authentication [username password [bearer-type [slice-type [slice-differentiator]]]]]]* **Example:** `Router# cellular 0/2/0 lte profile create 2 apn.com pap username pwd ipv4 eMBB 100`	Creates, modifies, or deletes a modem data profile in the privileged EXEC mode. • The *profile-number* argument specifies the profile number created for the modem. • (Optional) The *apn* argument specifies an Access Point Name (APN). An APN is provided by your service provider. Only a single APN can be specified for a single profile. • (Optional) The *authentication* parameter specifies the authentication type used. Acceptable parameters are **chap**, **none** (no authentication), **pap**, and **pap_chap** (PAP or CHAP authentication). • (Optional) The *username* and *password* arguments are given by a service provider. These are mandatory when an authentication type other than **none** is used. • (Optional) The *PDN* type parameter specifies the type of packet data session established with mobile network using this profile. Acceptable parameters are: **ipv4** **ipv6** and **ipv4v6** (IPv4 and IPv6). The **show cellular** *slot* profile displays configured profile list. **Note** Single asterisk(*) displayed against data profile. Double asterisk(**) displayed against attached profile. **Note** The **slice-type** and **slice-differentiator** options are applicable only for P-5GS6-R16SA-GL. • (Optional) Slice-types are identified by 3GPP-defined values. The valid values for slice type are eMBB, URLLC, and MIoT. • (Optional) Slice-differentiator is an optional value that enables the User Equipment (UE) to use multiple slice instances of the same SST.

Example

```
Router# show cellular 0/2/0 profile
Profile 1 = INACTIVE **
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwims
```

```
Authentication = None

Profile 2 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwadmin
Authentication = None

Profile 3 = ACTIVE*
--------
PDP Type = IPv4v6
PDP address = 192.0.2.1
PDP IPV6 address = 2600:1010:B00E:1E11:192D:3E20:199B:3A70/64  Scope: Global
Access Point Name (APN) = VZWINTERNET
Authentication = None
        Primary DNS address = 192.0.2.2
        Secondary DNS address = 192.0.2.2
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
```

Note If data and attach profile bindings need modification, use the **controller cellular** slot.

```
Router(config-controller)# lte sim data-profile 3 attach-profile 2 slot unit


Router #show cellular 0/2/0 profile
Profile 1 = INACTIVE
--------------------------------------------------
PDP Type = IPv4v6
Access Point Name (APN) = test
Authentication = None

Profile 2 = INACTIVE **
--------
PDP Type = IPv4
Access Point Name (APN) = internet
Authentication = PAP or CHAP
Username =  user@solution.com
Password =  cisco

Profile 3 = INACTIVE*
--------
PDP Type = IPv4v6
Access Point Name (APN) = basic
Authentication = None

  * - Default profile
 ** - LTE attach profile
Configured default profile for active SIM 0 is profile 2.
```

Create, modify, or delete data profiles in configuration mode

Note

- For the LTE/5G NIM, the *unit* argument identifies the router slot, WIC slot, and port separated by slashes (0/1/0).
- The default profile index is 1 and is not allowed to configure the slice type.

Procedure

	Command or Action	Purpose
Step 1	**profile id***id* **apn** *apn name [***authentication** *[username password]***pdn-type** *[pdn type][***slot***slot-number| no-overwrite]]]]* **Example:** `Router(config-controller)# profile id 1 apn apn_internet authentication none pdn-type ipv4 slot 0`	Configures a cellular profile in the configuration mode. • The *id* argument specifies the profile number created for the modem. The maximum number of profiles that can be created for each modem are given as follows: • EM7455 – Up to 16 profiles • EM7430 – Up to 16 profiles • (Optional) The *apn* argument specifies an Access Point Name (APN) in the profile. An APN is provided by your service provider. Only a single APN can be specified in a single profile. • (Optional) The *authentication* parameter specifies the authentication type used. Acceptable parameters are **chap**, **none** (no authentication), **pap**, and **pap_chap** (PAP or CHAP authentication). • (Optional) The *username* and *password* arguments are provided by a service provider. These are mandatory when an authentication type is used other than none. • (Optional) The *PDN-type* parameter specifies the type of packet data session established with mobile network using this profile. Acceptable parameters are: **ipv4**, **ipv6** and **ipv4v6**. • (Optional) The *slot-number* parameter specifies the slot number. By default, the slot-number is the current active slot-number, if not specified. • (Optional) *No-overwrite* action to be taken when a profile already exists in modem for the profile id. If there is a profile already exists in the modem for this profile id and no-overwrite option is specified, this configuration will not overwrite existing profile. Default is *overwrite*.
Step 2	**profile id***id* **apn** *apn name [***authentication** *[username password]***pdn-type** *[pdn type][slice- type][slice-differntiator][***slot***slot-number| no-overwrite]]]]* **Example:** `Router(config-controller)# profile id 1 apn apn_internet authentication none pdn-type ipv4 slice-type eMBB slice-differentiator 100 slot 0`	Configures a cellular profile in the configuration mode. • The *id* argument specifies the profile number created for the modem. The maximum number of profiles that can be created for each modem are given as follows: • EM7455 – Up to 16 profiles • EM7430 – Up to 16 profiles

	Command or Action	Purpose
		• (Optional) The *apn* argument specifies an Access Point Name (APN) in the profile. An APN is provided by your service provider. Only a single APN can be specified in a single profile. • (Optional) The *authentication* parameter specifies the authentication type used. Acceptable parameters are **chap**, **none** (no authentication), **pap**, and **pap_chap** (PAP or CHAP authentication). • (Optional) The *username* and *password* arguments are provided by a service provider. These are mandatory when an authentication type is used other than none. • (Optional) The *PDN-type* parameter specifies the type of packet data session established with mobile network using this profile. Acceptable parameters are: **ipv4**, **ipv6** and **ipv4v6**. • (Optional) The *slot-number* parameter specifies the slot number. By default, the slot-number is the current active slot-number, if not specified. • (Optional) *No-overwrite* action to be taken when a profile already exists in modem for the profile id. If there is a profile already exists in the modem for this profile id and no-overwrite option is specified, this configuration will not overwrite existing profile. Default is *overwrite*. **Note** The **slice-type** and **slice-differentiator** options are applicable only for P-5GS6-R16SA-GL. • (Optional) **Slice-type** is identified by 3GPP-defined values. The valid values for slice type are eMBB, URLLC, and MIoT. • (Optional) **Slice-differentiator** is an optional value that enables the User Equipment (UE) to use multiple slice instances of the same slice-type.

Configuration examples

The following example shows how to change a default profile on LTE/5G:

```
Router(config-controller)# lte sim data-profile 3 attach-profile 1 slot <unit>
```

The following example shows the output of the **show cellular** command for Verizon network service:

```
Router# show cellular 0/2/0 profile
Profile 1 = INACTIVE **
```

```
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwims
Authentication = None

Profile 2 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwadmin
Authentication = None

Profile 3 = ACTIVE*
--------
PDP Type = IPv4v6
PDP address = 192.0.2.1
PDP IPV6 address = 2600:1010:B00E:1E11:192D:3E20:199B:3A70/64  Scope: Global
Access Point Name (APN) = VZWINTERNET
Authentication = None
        Primary DNS address = 192.0.2.2
        Secondary DNS address = 192.0.2.3
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF

Profile 4 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwapp
Authentication = None

Profile 5 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzw800
Authentication = None

Profile 6 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = CISCO.GW4.VZWENTP
Authentication = None

  * - Default profile
 ** - LTE attach profile
```

Configuration example with network slicing

Example Configuration with Network Slicing

```
Router(config-controller)# profile id 2 apn embb authentication none
pdn-type ipv4 slice-type eMBB slice-differentiator 5 slot 0

Router(config-controller)# profile id 3 apn urllc authentication none
pdn-type ipv4 slice-type URLLC slice-differentiator 5 slot 0

Router# show cellular 0/2/0 profile
Profile 1 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = default
Authentication = None

Profile 2 = ACTIVE* **
--------
PDP Type = IPv4
PDP address = 192.168.2.2
IPv4 PDP Connection is successful
Access Point Name (APN) = embb_EMBB000005
Authentication = None
 Primary DNS address = 8.8.8.8
S-NSSAI Slice Type is eMBB
S-NSSAI Slice Differentiator = 5

Profile 3 = ACTIVE
--------
PDP Type = IPv4
PDP address = 192.168.3.2
IPv4 PDP Connection is successful
Access Point Name (APN) = urllc_URLLC000005
Authentication = None
 Primary DNS address = 8.8.8.8
S-NSSAI Slice Type is URLLC
S-NSSAI Slice Differentiator = 5
```

Configuration example under controller cellular

Example Configuration under Controller Cellular

```
Router(config-controller)# profile id 1 apn apn_internet authentication none pdn-type ipv4
 no-overwrite
```

Controller Cellular Running Configuration

```
Router #show running-config controller cellular <slot>
Building configuration...

Current configuration : 330 bytes
!
controller Cellular 0/2/0
profile id 1 apn apn_internet authentication none pdn-type ipv4 no-overwrite
end



 ** This will override exec mode profile configuration
 ** If for a profile ID, configuration CLI exists, exec mode configuration cannot be
performed.
 Router #show cellular <slot> profile 5
Profile 5 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = apn_old
Authentication = None

TSN1#cellular <slot> lte profile create 5 apn_new
 Warning: You are attempting to create Profile 5
 Profile 5 was configured through controller configuration 'profile id <profile #>'
 Please execute command under controller configuration using '[no] profile id <profile #>'
 for profile 5 to create
 Profile 5 NOT written to modem


** As part of this enhancement, any attach and/or data profile changes will immediately
trigger a connection reset and take effect. Below warning message will be displayed.

Warning: You are attempting to modify the data/attach profile.
Connection will be reset
```

Configure radio band selection

This feature allow users to configure and lock down the modem to a specific RF band, or set of bands. The preference can be set to be equal to, or a sub-set of the capability supported by the modem/carrier combination.

The following examples show the controller configuration commands.

:

Procedure

	Command or Action	Purpose

Step 1	**conf t**
	Example:
	`Router# conf t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`	

Step 2	**controllercellular***interface-number* **Example:** `Router(config)# controller cellular 0/2/0`	
Step 3	**lte modem band-selectindicesumts3gindiceslte4gindicesnr5g-nsaindicesnr5g-saindicesslotslot#** **Example:** `Router(config-controller)# lte modem band-select indices umts3g "none" lte4g "all" nr5g-nsa "78" nr5g-sa "78" slot 0`	

Example

```
Router#show cellular 0/3/0 radio ?
  band     Show Radio band settings
  history  Show Radio history in graph format
  |        Output modifiers
  <cr>     <cr>
```

```
Router#show cell 0/3/0 radio band
LTE bands supported by modem:
- Bands 1 2 3 4 5 7 8 12 13 14 17 18 19 20 25 26 28 29 30 32 34 38 39 40 41 42 43 46 48 66
 71.
LTE band Preference settings for the active sim(slot 0):
- Bands 1 2 3 4 5 7 8 12 13 14 17 18 19 20 25 26 28 29 30 32 34 38 39 40 41 42 43 46 48 66
 71.

NR5G NSA bands supported by modem:
- Bands 1 2 3 5 7 8 12 13 14 18 20 25 26 28 29 30 38 40 41 48 66 70 71 75 76 77 78 79.
NR5G NSA band Preference settings for the active sim(slot 0):
- Bands 78

NR5G SA bands supported by modem:
- Bands 1 2 3 5 7 8 12 13 14 18 20 25 26 28 29 30 38 40 41 48 66 70 71 75 76 77 78 79.
NR5G SA band Preference settings for the active sim(slot 0):
- Bands 78.
```

```
3G/GSM bands supported by modem:
Index:
  23 - WCDMA (Europe, Japan, and China) 2100 band
  24 - WCDMA US PCS 1900 band
  26 - WCDMA US 1700 band
  27 - WCDMA US 850 band
  28 - WCDMA Japan 800 band
  50 - WCDMA Europe and Japan 900 band
  61 - WCDMA Japan 850 band
3G/GSM band Preference settings for the active sim(slot 0):
Index: <none>

===========================================


Band index reference list:

For LTE and 5G, indices 1-128 correspond to bands 1-128.

For 3G, indices 1-64 maps to the 3G bands mentioned against each above.
```

Multiple PDN contexts

This feature enables router to connect to multiple (currently two) packet data networks. This allows users to enable different features independently on each PDN. For instance, the first PDN can be used for public Internet access and the second one for VPN connectivity; each PDN has its own set of IP addresses and QoS characteristics.

During the initialization of the router, two cellular interfaces corresponding to the two PDNs are created:

cellular 0/2/0 and cellular 0/2/1

These interfaces can be viewed as two logical interfaces using the same radio resources.

The interface cellular 0/2/0 is referred as the first PDN, and cellular 0/2/1 as the second PDN.

To bring up the two PDNs, configuration needs to be applied on both the cellular interfaces in order to make two simultaneous data calls. The next step is to associate the data-bearer profile with its corresponding cellular interface or PDN. It is sufficient to associate the profile for just the first PDN under the controller cellular configuration. Note that the second PDN assumes a profile that is just one above the profile used for the first PDN. For example, if the first PDN uses profile 1, the second PDN uses profile 2 automatically when the call is initiated for the second one.

After the interesting traffic is routed through these cellular interfaces, data calls are initiated and each interface is assigned its own IP and DNS addresses provided by the cellular network.

Note Both PDNs share radio resources. Therefore, any throughput measurement needs to take into account the aggregate throughput on both PDNs, instead of just one.

Note For Verizon cellular network, the second PDN uses profile #6 automatically, when the call is initiated for the second data connection.

Configuration examples

The following example shows how to configure multiple PDN on Cisco LTE/5G SKU:

```
interface Cellular0/2/0
ip address negotiated
 dialer in-band
 dialer idle-timeout 0
 dialer-group 1
 ipv6 enable
 pulse-time 1
!
interface Cellular0/2/1
ip address negotiated
dialer in-band
dialer idle-timeout 0
dialer-group 1
ipv6 enable
pulse-time 1
! dialer-list 1 protocol ipv6 permit
!

ip route 192.0.2.1 255.255.255.0 Cellular0/2/0
ip route 192.0.2.2 255.255.255.255 Cellular0/2/1
!
```

These show commands can be used to verify the status of the multiple PDN calls:

```
Router#sh cellular 0/2/0 profile
Profile 1 = ACTIVE* **
--------
PDP Type = IPv4v6
PDP address = 192.0.2.1
PDP IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF/64  Scope: Global
Access Point Name (APN) = broadband
Authentication = None
        Primary DNS address = 192.0.2.2
        Secondary DNS address = 192.0.2.3
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF

.
.
.

Profile 16 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = CHAP
Username: ipv4v6
Password: xxxxxx

  * - Default profile
 ** - LTE attach profile

Configured default profile for active SIM 0 is profile 1.

Router# sh cellular 0/2/0 connection
Profile 1, Packet Session Status = ACTIVE
        Cellular0/2/0:
        Data Packets Transmitted = 9 ,  Received = 9
        Data Transmitted = 900 bytes, Received = 900 bytes
        IP address = 192.0.2.1
        IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF/64  Scope: Global
        Primary DNS address = 192.0.2.2
        Secondary DNS address = 192.0.2.3
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
Profile 2, Packet Session Status = ACTIVE
        Cellular0/2/1:
        Data Packets Transmitted = 7 ,  Received = 2
        Data Transmitted = 700 bytes, Received = 176 bytes
        IP address = 192.0.2.4
        IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF/64  Scope: Global
        Primary DNS address = 171.70.168.183
        Secondary DNS address = 192.0.2.5
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
.
.
.
Profile 16, Packet Session Status = INACTIVE

Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.0.2.1       YES manual up                    up
GigabitEthernet0/0/1   unassigned      YES unset  administratively down down
GigabitEthernet0/1/0   unassigned      YES unset  administratively down down
GigabitEthernet0/1/1   unassigned      YES unset  administratively down down
GigabitEthernet0/1/2   unassigned      YES unset  administratively down down
GigabitEthernet0/1/3   unassigned      YES u
nset  administratively down down
GigabitEthernet0/1/4   unassigned      YES unset  administratively down down
GigabitEthernet0/1/5   unassigned      YES unset  administratively down down
GigabitEthernet0/1/6   unassigned      YES unset  administratively down down
GigabitEthernet0/1/7   unassigned      YES unset  administratively down down
Wl0/1/8                unassigned      YES unset  administratively down down
Cellular0/2/0          192.0.2.2      YES IPCP   up                    up
Cellular0/2/1          192.0.2.3    YES IPCP   up                    up
Vlan1                  unassigned      YES manual up                    down

Router#
Router# show ip dns view
DNS View default parameters:
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name:
  Domain search list:
  Domain name-servers:
    192.0.2.1
    2001:4860:4860::8888
    192.0.2.2
    2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
    192.0.2.3
    8.8.8.8
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses: DNS View default parameters: DNS Resolver settings:
Domain lookup is enabled Default domain name: Domain search list: Domain name-servers:
192.0.2.1
192.0.2.2
192.0.2.3
DNS Server settings:
Forwarding of queries is enabled
Forwarder addresses:
Router#
```

Configure a SIM for data calls

Lock and unlock a SIM card using a PIN code

Perform this task to lock or unlock a SIM card given by your service provider.

The SIM card gets blocked if the wrong PIN is entered three consecutive times. Make sure you enter the correct PIN the SIM is configured with. If your SIM card gets blocked, contact your service provider for a PUK code. Using the PUK code, you can unblock the SIM card.

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

Procedure

	Command or Action	Purpose
Step 1	**cellular** *unit* **lte sim** {**lock** | **unlock**} *pin* **Example:** `Router# cellular 0/2/0 lte sim lock 1111`	Locks or unlocks the SIM card using a PIN code. - *pin*—A code (4 to 8 digits long) provided by your carrier to lock or unlock the SIM card.

Change the PIN code

Perform this task to change the PIN code of a SIM.

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

Procedure

	Command or Action	Purpose
Step 1	**cellular** *unit* **lte sim change-pin** *pin new-pin* **Example:** `Router# cellular 0/2/0 lte sim change-pin 1111 1234`	Changes the assigned PIN code. SIM should be in locked state when the PIN is being changed.

Verifying the security information of a modem

Perform this task to verify the security information of a modem.

Note For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

Procedure

	Command or Action	Purpose
Step 1	**show cellular** *unit* **security** **Example:** `Router# show cellular 0/2/0 security`	Shows the security information of the modem, including the SIM lock status.

Configure automatic authentication for a locked SIM

An unencrypted PIN can be configured to activate the Card Holder Verification (CHV1) code that authenticates a modem.

The SIM card gets blocked if the wrong PIN is entered three consecutive times. Make sure you enter the correct PIN the SIM is configured with. If your SIM card gets blocked, contact your service provider for a PUK code.

Follow these procedures when using an unencrypted Level 0 PIN to configure CHV1. For instructions on how to configure CHV1 using an encrypted Level 7 PIN, see the Configure an encrypted PIN for a SIM, on page 214.

A SIM should be locked for SIM authentication to work. To verify the SIM’s status, use the **show cellular** *unit* **security** command.

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**controller cellular** *unit* **Example:** `Router(config)# controller cellular 0/2/0`	Enters the cellular controller configuration mode.
Step 3	**lte sim authenticate 0** *pin*	Authenticates the SIM CHV1 code by using an unencrypted (**0**) keyword and PIN. This PIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call. **Note** This command is valid only when an unencrypted PIN is used. To configure CHV1 code using an encrypted PIN,

	Command or Action	Purpose
		see the Configure an encrypted PIN for a SIM, on page 214.

Configure an encrypted PIN for a SIM

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled Level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode.

Note When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command. After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration.

Note A SIM should be locked for SIM authentication to work. To verify the SIM's status, use the **show cellular** <*unit*> **security** command.

Note For the 4G LTE SKU, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

SUMMARY STEPS

1. **configure terminal**
2. **service password-encryption**
3. **username** *name* **privilege 0 password** *pin*
4. **do show run** | **i** *name*
5. **controller cellular** *unit*
6. **lte sim authenticate** {**0** | **7**} *pin*
7. **exit**
8. **no username** *name*
9. **no service password-encryption**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 2	**service password-encryption** **Example:** `Router(config)# service password-encryption`	Enables password encryption.
Step 3	**username** *name* **privilege 0 password** *pin* **Example:** `Router(config)# username SIM privilege 0 password 1111`	Creates username and password. - *name*—Specifies the username. - *pin*—Specifies the four- to eight-digit PIN code.

Step 4	**do show run | i** *name*
	Example:
	`Router(config)# do show run | i SIM`
		Shows the username configuration line with the encrypted level 7 PIN for the username created in Step 3 (user “SIM” in the example shown).
		Copy the scrambled password for use in Step 6 (as the PIN).

Step 5	**controller cellular** *unit* **Example:** `Router(config)# controller cellular 0/2/0`	Enters the cellular controller configuration mode.
Step 6	**lte sim authenticate** {**0** | **7**} *pin*	Authenticates the SIM CHV1 code by using the encrypted keyword **7** and the scrambled PIN from Step 4. The PIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call.
Step 7	**exit** **Example:** `Router(config-controller)# exit`	(Optional) Exits the cellular controller configuration mode.
Step 8	**no username** *name* **Example:** `Router(config)# no username SIM`	(Optional) Removes the username and password created in Step 3.
Step 9	**no service password-encryption** **Example:** `Router(config)# no service password-encryption`	(Optional) Disables password encryption.

Apply a modem profile in a SIM configuration

SUMMARY STEPS

1. **configure terminal**
2. **controller cellular** *unit*
3. **lte sim data-profile** *number* **attach-profile** *number* **slot** *number*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 2	**controller cellular** *unit* **Example:** `Router(config)# controller cellular 0/2/0`	Enters the cellular controller configuration mode.
Step 3	**lte sim data-profile** *number* **attach-profile** *number* **slot** *number*	Applies the configured profile number to the SIM and its slot number. The default (primary) slot is 0. The **attach profile** is the profile used by the modem to attach to the LTE network. The **data profile** is the profile used to send and receive data over the cellular network. The**slot** is the optional parameter which distinguishes config for SIM 0 or SIM 1.

Data call setup

To set up a data call, use the following procedures:

Configure the cellular interface

To configure the cellular interface, enter the following commands starting in EXEC mode.

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

If a tunnel interface is configured with **ip unnumbered cellular 0/2/0**, it is necessary to configure the actual static IP address under the cellular interface, in place of **ip address negotiated**.

SUMMARY STEPS

1. **configure terminal**

2. **interface cellular** unit
3. **ip address negotiated**
4. **dialer in-band**
5. **dialer-group** group-number
6. **exit**
7. **ip route** *network-number network-mask* {*ip-address* | *interface*} [*administrative distance*] [**name** *name*]
8. **dialer-list** dialer-group **protocol** protocol-name {**permit** | **deny** | **list** *access-list-number* | **access-group**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface cellular** unit **Example:** `Router(config)# interface cellular 0/2/0`	Specifies the cellular interface.
Step 3	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for a particular interface is dynamically obtained.
Step 4	**dialer in-band** **Example:** `Router(config-if)# dialer in-band`	Enables DDR and configures the specified serial interface to use in-band dialing.
Step 5	**dialer-group** group-number **Example:** `Router(config-if)# dialer-group 1`	Specifies the number of the dialer access group to which the specific interface belongs.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Enters the global configuration mode.
Step 7	**ip route** *network-number network-mask* {*ip-address* | *interface*} [*administrative distance*] [**name** *name*] **Example:**	Establishes a floating static route with the configured administrative distance through the specified interface. **Note**

	Command or Action	Purpose
	`Router(config)# ip route 209.165.200.225 255.255.255.224 cellular 0/2/0`	A higher administrative distance should be configured for the route through the backup interface so that it is used only when the primary interface is down.

Step 8	**dialer-list** dialer-group **protocol** protocol-name {**permit** | **deny** | **list** *access-list-number* | **access-group**}
	Example:
	`Router(config)# dialer-list 1 protocol ip list 1`
		Creates a dialer list for traffic of interest and permits access to an entire protocol.

Configure DDR

To configure DDR for the cellular interface, enter the following commands starting in EXEC mode.

Note For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

SUMMARY STEPS

1. **configure terminal**
2. **interface cellular** *unit*
3. **ip address negotiated**
4. **dialer in-band**
5. **ip address negotiated**
6. **dialer idle-timeout** *seconds*
7. dialer-group group-number
8. **exit**
9. dialer-list dialer-group protocol protocol-name {permit | deny | list *access-list-number* | access-group}
10. access-list access-list-number permit *ip*-source-address

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface cellular** *unit* **Example:** `Router(config)# interface cellular 0/2/0`	Specifies the cellular interface.

	Command or Action	Purpose
Step 3	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for a particular interface is dynamically obtained.
Step 4	**dialer in-band** **Example:** `Router(config-if)# dialer in-band`	Enables DDR and configures the specified serial interface to use in-band dialing.
Step 5	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for a particular interface is dynamically obtained.
Step 6	**dialer idle-timeout** *seconds* **Example:** `Router(config-if)# dialer idle-timeout 30`	Specifies the duration of idle time, in seconds, after which a line has no outbound traffic. "0" second means no idle timeout. The default idle timeout is 120 seconds if there is no idle timer specified.
Step 7	dialer-group group-number **Example:** `Router(config-if)# dialer-group 1`	Specifies the number of the dialer access group to which the specific interface belongs.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Enters the global configuration mode.

Step 9	dialer-list dialer-group protocol protocol-name {permit | deny | list *access-list-number* | access-group}
	Example:
	`Router(config)# dialer-list 1 protocol ip list 1`
		Creates a dialer list for traffic of interest and permits access to an entire protocol.

Step 10	access-list access-list-number permit *ip*-source-address **Example:** `Router(config)# access-list 1 permit any`	Defines traffic of interest.

Enable 4G GPS and NMEA data streaming

GPS NMEA data streaming to external NMEA 2.0-compliant GPS plotter applications can be enabled on Cisco LTE/5G.

Note For the LTE/5G, the *unit* argument identifies the router slot, module slot, and the port, and is separated by slashes (0/2/0).

SUMMARY STEPS

1. configure terminal
2. controller cellular *unit*
3. lte gps enable
4. lte gps mode standalone
5. lte gps nmea {ip | udp [*source address*][*destination address*][*destination port*] }
6. test cellular *unit* modem-power-cycle
7. end
8. show cellular *unit* gps
9. show cellular *unit* gps detail

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Router# configure terminal`	Enters the configuration mode.
Step 2	controller cellular *unit* **Example:** `Router(config)# controller cellular 0/2/0`	Enters the controller cellular configuration mode.
Step 3	lte gps enable **Example:** `Router(config-controller)# lte gps enable`	(Optional) GPS is enabled by default. Use this command to enable the GPS feature if GPS has been disabled for any reason.
Step 4	lte gps mode standalone **Example:** `Router(config-controller)# lte gps mode standalone`	Enables the standalone GPS mode.

Step 5	lte gps nmea {ip | udp [*source address*][*destination address*][*destination port*] }
	Example:
	`Router(config-controller)# lte gps nmea ip`
	or
	`Router(config-controller)# lte gps nmea`
		Enables NMEA. Cisco 4G LTE Advanced support only IP NMEA. Therefore, the IP interface and serial interface options are unavailable.

	Command or Action	Purpose
Step 6	test cellular *unit* modem-power-cycle **Example:** `Router# test cellular 0/2/0 modem-power-cycle`	GPS can take effect only after modem power cycle.

Step 7	end
	Example:
	`Router(config-controller)# end`
		Exits the controller configuration mode and returns to the privileged EXEC mode.

Step 8	show cellular *unit* gps
	Example:
	`Router# show cellular 0/2/0 gps`
	
	`GPS Info`
	`-------------`
	`GPS Feature: enabled`
	`GPS Mode Configured: standalone`
	`GPS Port Selected: Dedicated GPS port`
	`GPS Status: GPS coordinates acquired`
	`Last Location Fix Error: Offline [0x0]`
	`Latitude: 38 Deg 11 Min 22.1939 Sec North`
	`Longitude: 96 Deg 40 Min 48.7066 Sec West`
	`Timestamp (GMT): Thu Jun 29 07:13:42 2017`
	
	`Fix type index: 0, Height: 318 m`
	`Satellite Info`
	`----------------`
	`Satellite #3, elevation 62, azimuth 282, SNR 53`
	`.`
	`.`
	`.`
	`Satellite #28, elevation 0, azimuth 0, SNR 0`
	`Router#`
		Displays a summary of the following GPS data:
		• GPS state information (GPS disabled, GPS acquiring, GPS enabled)
		• GPS mode configured (standalone)
		• GPS location and timestamp information
		• GPS satellite information
		• GPS feature (enabled or disabled)
		• GPS port selected (Dedicated GPS and GPS port with voltage-no-bias)

Step 9	show cellular *unit* gps detail
	Example:
	`Router# show cellular 0 gps detail`
	`GPS Info`
	`-------------`
	`GPS Feature: enabled`
	`GPS Mode Configured: standalone`
	`GPS Port Selected: Dedicated GPS port`
	`GPS Status: GPS coordinates acquired`
	`Last Location Fix Error: Offline [0x0]`
	`Latitude: 38 Deg 11 Min 22.1939 Sec North`
	`Longitude: 96 Deg 40 Min 48.7066 Sec West`
	`Timestamp (GMT): Thu Jun 29 07:13:42 2017`
	`Fix type index: 0, Height: 0 m`
	`HDOP: , GPS Mode Used: not configured`
	
	`Satellite Info`
	`----------------`
	`Satellite #3, elevation 0, azimuth 0, SNR 53`
	`.`
	`.`
	`.`
		Displays detailed GPS data.

	Command or Action	Purpose

	`Satellite #9, elevation 0, azimuth 0, SNR 0`
	`Router#`	

Configure 4G SMS messaging

Note For the LTE/5G, the *unit* argument identifies the router slot, module slot, and the port, and is separated by slashes (0/2/0).

SUMMARY STEPS

1. configure terminal
2. controller cellular *unit*
3. lte sms archive path *FTP-URL*
4. cellular *unit* lte sms view { all | *ID* | summary }
5. end
6. show cellular *unit* sms
7. cellular *unit* lte sms send *number*
8. cellular *unit* lte sms delete [all | *id*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Router# configure terminal`	Enters the configuration mode.
Step 2	controller cellular *unit* **Example:** `Router(config)# controller cellular 0/2/0`	Enters the controller cellular configuration mode.

Step 3	lte sms archive path *FTP-URL*
	Example:
	`Router(config-controller)# lte sms archive path ftp://username:password@172.25.211.175/SMS-LTE`
		Specifies an FTP server folder path to send all the incoming and outgoing SMS messages. After the folder path is identified, it is appended automatically with outbox and inbox folders for the path to which SMS messages are sent and received, for example:
		`ftp://172.25.211.175/SMS-LTE/outbox`
		`ftp://172.25.211.175/SMS-LTE/inbox`

Step 4	cellular *unit* lte sms view { all | *ID* | summary } **Example:**	Displays the message contents of incoming texts received by a modem.

	Command or Action	Purpose

	`Router# cellular 0/2/0 lte sms view summary`
	
	`ID FROM YY/MM/DD HR:MN:SC SIZE CONTENT`
	`0 4442235525 12/05/29 10:50:13 137 Your entry last month has...`
	`2 5553337777 13/08/01 10:24:56 5 First`
	`3 5553337777 13/08/01 10:25:02 6 Second`
		• **all**—Displays the message contents of up to 255 incoming text messages received by the modem.
		• *ID*—Displays the message contents for a specified ID (0-255) of an incoming text message.
		• **summary**—Displays a summary of the incoming text messages received by the modem.

Step 5	end
	Example:
	`Router# end`
		Exits the configuration mode and returns to the privileged EXEC mode.

Step 6	show cellular *unit* sms
	Example:
	`Router#  show cellular 0/2/0 sms`
	`Incoming Message Information`
	`----------------------------`
	`SMS stored in modem = 20`
	`SMS archived since booting up = 0`
	`Total SMS deleted since booting up = 0`
	`Storage records allocated = 25`
	`Storage records used = 20`
	`Number of callbacks triggered by SMS = 0`
	`Number of successful archive since booting up = 0`
	`Number of failed archive since booting up = 0`
	
	`Outgoing Message Information`
	`----------------------------`
	`Total SMS sent successfully = 0`
	`Total SMS send failure = 0`
	`Number of outgoing SMS pending = 0`
	`Number of successful archive since booting up = 0`
	`Number of failed archive since booting up = 0`
	`Last Outgoing SMS Status = SUCCESS`
	`Copy-to-SIM Status = 0x0`
	`Send-to-Network Status = 0x0`
	`Report-Outgoing-Message-Number:`
	`Reference Number = 0`
	`Result Code = 0x0`
	`Diag Code = 0x0 0x0 0x0 0x0 0x0`
	
	`SMS Archive URL = ftp://lab:lab@1.3.150.1/outbox`
		Displays all the information in the text messages sent and received. Message information includes text messages sent successfully, received, archived, and messages pending to be sent. LTE-specific information on errors in case of a FAILED attempt may also be displayed.

Step 7	cellular *unit* lte sms send *number* **Example:** `Router# cellular 0/2/0 lte sms send 15554443333 <sms text>`	Enables a user to send a LTE/5G band SMS message to other valid recipients, provided they have a text message plan. The *number* argument is the telephone number of the SMS message recipient. **Note** 10-digit or 11-digit (phone) numbers are the proper numerical format for sending a text. For example, ########## or 1##########. Seven digits are not supported.

	Command or Action	Purpose
Step 8	cellular *unit* lte sms delete [all | *id*] **Example:** `Router# cellular 0/2/0 lte sms delete [ all | id ]`	(Optional) Deletes one message ID or all of the stored messages from memory.

Configure modem DM log collection

Diagnostic Monitor (DM) Log is a modem's feature that captures data transactions between the modem and the network over the radio frequency interface. This feature is a useful tool for troubleshooting 3G and 4G data connectivity or performance issues.

A member of Cisco TAC can help with decoding the DM log files.

To configure DM log collection, enter the following commands, starting in privileged EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**controller cellular** *slot* **Example:** `Router(config)# controller cellular 0/2/0`	Enters cellular controller configuration mode.

Step 3	**lte modem dm-log** {**autoshop** {**link-down** | **timer** *time*} | **enable** | **filesize** *size* | **filter**} **bootflash:***file* | **flash:***file*} **rotation** | **size** *log-size*}
	Example:
	`Router(config-controller)# lte modem dm-log enable`
		Configures DM logging for LTE modem.
		• **autostop**—Automatically stops DM log capturing based on:
		link-down—cellular interface link down event
		timer*timer*—amount of time in minutes
		• **enable**—Starts DM log capturing.
		• **filesize** *size*—Specifies the maximum log file size, in MB for each DM log file before creating another DM log file. Range is from 1 to 64. Default is 20.
		• **filter** *location***:***filename*—Specifies the DM log filter to use from the following locations:
		—bootflash:*file*
		—flash:*file*
		Note

	Command or Action	Purpose
		Bootflash and flash are the only valid locationsto store the DM log filter file. **Note** If the DM log filter file is not specified, the generic filter file, which comes with the router will be used. **Note** The DM log filter file needs to be in .sqf format. • **rotation**—Enables continuous DM log capturing by replacing the oldest DM log files with the latest. • **size** *log-size*—Specifies the maximum total size in MB of all DM log files that can be allowed in the bootflash or flash before modem stops capturing DM log files. If rotation is enabled, the oldest DM files is replaced with the latest DM file to meet this size configuration.

Step 4	**end**
	Example:
	`Router(config-controller)# end`
		Returns to privileged EXEC mode.

Step 5	**show cellular** *unit* **logs dm-log**
	Example:
	`Router# show cellular 0/2/0 logs dm-log`
	`Integrated DM logging is on`
	`output path = Utility Flash`
	`filter = MC74xx generic -`
	`v11026_Generic_GSM_WCDMA_LTE_IP-no-data-packets.sqf`
	`maximum log size = 0`
	`maximum file size = 0`
	`log rotation = disabled`
	
	`33 packets sent to the modem, 4663 bytes, 0 errors`
	`28521 packets received from the modem, 13500758`
	`bytes, 0 input drops`
	`28521 packets stored in utility flash, 13500758`
	`bytes`
	
	`current file size = 13500758`
	`current log size = 13500758`
	`total log size = 13500758`
	`Utility Flash DM log files =  (1) files`
		(Optional) Displays DM log configuration and statistics.

Example

The following example shows how to:

- Specifies the maximum size of all DM log files that can be stored in bootflash or flash to 512 MB

- Specifies the maximum size of each DM log file to 32 MB
- Uses MC7xxx_GPS_Log.sqf DM log filter in the flash
- Enable rotation
- Enables DM log capturing

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log filesize 512
```

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log filesize 32
```

The following example shows how to specify the filter file for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log filter flash:MC7xxx_GPS_Log.sqf
```

The following example shows how to enable DM log rotation for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log rotation
```

The following example shows how to specify the maximum log size for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log enable
```

The following example shows how to enable DM log rotation for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# end
```

The following example shows how to specify the maximum log size for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log size 1024
```

The following example shows how to enable DM log rotation for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# end
```

The following example shows what was configured on the router for DM log feature:

```
Router#show running-config | section controller
controller Cellular 0/2/0
 lte modem dm-log filter flash:MC7xxx_GPS_Log.sqf
 lte modem dm-log size 512
 lte modem dm-log filesize 32
 lte modem dm-log rotation
 lte modem dm-log enable
 lte modem dm-log size 1024
```

The following displays DM log configuration and statistics

```
Router#show cellular 0/2/0 logs dm-log
Integrated DM logging is on
output path = Utility Flash
filter = flash:MC7xxx_GPS_Log.sqf
maximum log size = 536870912
maximum file size = 33554432
log rotation = enabled

32 packets sent to the modem, 3879 bytes, 0 errors
158324 packets received from the modem, 75971279 bytes, 0 input drops
158324 packets stored in utility flash, 75971279 bytes
```

```
current file size = 8863042
current log size = 75971279
total log size = 75971279
Utility Flash DM log files =  (3) files
end
```

The following shows the DM log files created:

```
Router#dir flash:dmlog*
Directory of bootflash:/dmlog*

Directory of bootflash:/

   27  -rw-    33554069   Jun 7 2018 18:08:46 -08:00  dmlog-slot2-20180607-180628.bin
   28  -rw-    33554168   Jun 7 2018 18:11:25 -08:00  dmlog-slot2-20180607-180846.bin
   29  -rw-    14188544   Jun 7 2018 18:12:37 -08:00  dmlog-slot2-20180607-181125.bin
2885718016 bytes total (521891840 bytes free)
lte modem dm-log size 1024
```

The following shows hot to disable/stop DM log capturing:

```
Router(config)#controller cellular 0/2/0
Router(config-controller)#no lte modem dm-log enable
Router(config-controller)#end
```

Enable modem crashdump collection

Modem crashdump collection is useful in debugging firmware crash. To collect crash data, the modem has to be pre-configured so that it will stay in memdump mode after a crash. Memdump mode is a special boot-and-hold mode for the memdump utility to collect crash data.

For earlier releases, the crashdump collection required the PC to be connected to the router using a USB cable or a special RJ45-USB cable on a non-HSPA+7 3G module.

As part of the 3G and 4G serviceability enhancement, the crashdump collection utility is integrated into Cisco IOS.

To enable modem crashdump collection, perform the following steps.

Note The integrated modem crashdump collection feature is supported only on 3G HSPA and LTE/5G based SKUs.

Before you begin

Ensure that the following prerequisites are met before attempting to enable crashdump logging:

- The modem needs to be provisioned for modem crashdump collection. Contact Cisco TAC for details.
- The modem should be in crash state. Run tests that will result in modem firmware crash. A “MODEM_DOWN” message on the router console or syslog is indicative of modem firmware crash.

Note After the modem firmware crashes, the modem is available for crashdump log collection only. Data calls cannot be made.

Procedure

	Command or Action	Purpose

Step 1	test { cell-cwan } *unit* modem-crashdump { on *location* | off }
	Example:
	`Router# test cell-host 0/2/0 modem-crashdump on local_uf`
		Enables or disables modem crashdump collection.
		• **cell-host**
		—Keyword for fixed platform.
		• **cell-cwan**
		— Keyword for LTE on a modular inside platform.
		• *unit*
		—For LTE module, this is the router slot, module slot, and port separated by slashes (for example, 0/2/0). For fixed platform, this is the number 0.
		• **on**
		Enables crashdump log collection.
		• *location*
		—Specifies the destination URL where the modem crashdump logs will be stored.
		• **off**
		—Disables crashdump log collection.

Display modem log error and dump information

As part of the 3G serviceability enhancement, commands strings (**at!err** and **at!gcdump**) can be sent to the modem using Cisco IOS CLI rather than setting up a reverse telnet session to the cellular modem to obtain log error and dump information.

To obtain log error and dump information, perform the following steps.

Note The modem log error and dump collection feature is supported only on 3G SKUs.

Procedure

	Command or Action	Purpose
Step 1	**show cellular** *unit* **log error** **Example:** `Router# show cellular 0/2/0 log error`	Shows modem log error and dump information.

	Command or Action	Purpose
Step 2	**test cellular** *unit* **modem-error-clear** **Example:** `Router# test cellular 0/2/0 modem-error-clear`	(Optional) Clears out the error and dump registers. By default, error and dump registers are not cleared out after a read. This command changes the operation so that registers are cleared once they are read. As a result, the AT command strings are changed to "**at!errclr=–1**" for CDMA and "**at!err=0**" for GSM modems.

Verify the LTE or 5G router information

You can verify the configuration by using the following show commands:

show version

```
Router#show version
Cisco IOS XE Software, Version 17.18.01a
Cisco IOS Software [IOSXE], c81g2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.18.1a, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Wed 13-Aug-25 07:04 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: 17.18(1r)

Router uptime is 2 hours, 39 minutes
Uptime for this control processor is 2 hours, 40 minutes
System returned to ROM by Reload Command
System image file is "bootflash:c81g2be-universalk9.17.18.01a.SPA.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.
```

```
Technology Package License Information:

-----------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
-----------------------------------------------------------------
Smart License  Perpetual    essentials         essentials

The current crypto throughput level is 250000 kbps (Aggregate)


Smart Licensing Status: Smart Licensing Using Policy

cisco C8161-G2 (1RU) processor with 1901039K/6147K bytes of memory.
Processor board ID FGL2924L2AU
Router operating mode: Autonomous
1 Virtual Ethernet interface
10 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
18271231K bytes of flash memory at bootflash:.

Configuration register is 0x2102
```

show platform

```
router# show platform
Chassis type: C8161-G2

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C8161-G2            ok                    02:40:23
 0/0      C8161-2S            ok                    02:39:45
 0/1      C8161-ES-8          ok                    02:39:44
 0/2      P-LTEA7-NA          ok                    02:26:19
R0        C8161-G2            ok, active            02:40:23
F0        C8161-G2            ok, active            02:40:23
P0        PWR-12V             ok                    02:39:58

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         2508050E            17.18(1r)
R0        2508050E            17.18(1r)
F0        2508050E            17.18(1r)
```

show interfaces

```
router#sh interface cellular 0/2/0
Cellular0/2/0 is up, line protocol is up
  Hardware is LTE Advanced CAT-7 pluggable - North America Multimode LTE/DC-HSPA+/HSPA+/HSPA/

  MTU 1500 bytes, BW 50000 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive not supported
  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 abort
   0 packets output, 0 bytes, 0 underruns
   Output 0 broadcasts (0 IP multicasts)
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
   0 carrier transitions
```

Configure cellular modem link recovery

The cellular modem link recovery feature is disabled by default. It is recommended to enable the link recovery feature for improved performance and reliability.

When enabled, the feature monitors specific parameters such as RSSI (Received Signal Strength Indicator), RSRP (Reference Signal Received Power), and RSRQ (Reference Signal Received Quality), one at a time.

These parameters provide information about the strength and quality of the cellular signal.

The modem link recovery feature triggers the modem to reload when any of the configured values (RSSI, RSRP or RSRQ) go beyond the set threshold. Modem link recovery essentially restarts the cellular modem to re-establish a stable connection.

Note This feature does not automatically select the next best carrier network or initiate a SIM switchover based on the RSSI, RSRQ, RSRP values. It only focuses on reloading the modem to resolve potential connectivity problems.

To configure and enable the monitoring parameters for link recovery, perform the **lte modem link-recovery rssi onset-threshold** command for RSSI, **lte modem link-recovery rsrp onset-threshold** for RSRP and **lte modem link-recovery rsrq onset-threshold** for RSRQ.

To disable the link recovery feature, use:

{ lte } modem link-recovery disable | no lte | modem link-recovery disable }

Note The link-recovery feature enables the RSRP (Reference Signal Received Power) and RSRQ (Reference Signal Received Quality) parameters on cellular modems from Cisco IOS XE Dublin 17.11.1a onwards.

To enable or disable the cellular modem link recovery feature (if required) perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **controller cellular** *unit*

3. For LTE modems, RSSI, RSRP (Reference Signal Received Power) and RSRQ (Reference Signal Received Quality) are recommended indicators of signal quality. Perform the **lte modem link-recovery rssi onset-threshold** command for RSSI, **lte modem link-recovery rsrp onset-threshold** for RSRP and **lte modem link-recovery rsrq onset-threshold** for RSRQ. To disable the link recovery feature, use: {**lte**} **modem link-recovery disable | no lte | modem link-recoverydisable**}
4. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**controller cellular** *unit* **Example:** `Router(config)# controller cellular 0/2/0`	Enters cellular controller configuration mode.

Step 3	For LTE modems, RSSI, RSRP (Reference Signal Received Power) and RSRQ (Reference Signal Received Quality) are recommended indicators of signal quality. Perform the **lte modem link-recovery rssi onset-threshold** command for RSSI, **lte modem link-recovery rsrp onset-threshold** for RSRP and **lte modem link-recovery rsrq onset-threshold** for RSRQ. To disable the link recovery feature, use: {**lte**} **modem link-recovery disable | no lte | modem link-recoverydisable**}
	Example:
	`Router(config-controller)# lte modem link-recovery disable`
	`Router(config-controller)# no lte modem link-recovery disable`
	
	`Router#show run | sec controller Cellular 0/2/0`
	`controller Cellular 0/2/0`
	`lte modem link-recovery rssi onset-threshold -110`
	`lte modem link-recovery monitor-timer 20`
	`lte modem link-recovery wait-timer 10`
	`lte modem link-recovery debounce-count 6`
	For the RSSI parameter:
	`Router#configure terminal`
	`Router(config)#controller Cellular 0/2/0`
	`Router(config-controller)#lte modem link-recovery`
		Enables or disables the cellular modem link recovery feature (the cellular modem link recovery feature is disabled by default).
		Further enables the RSSI, RSRQ and RSRP parameters recommended for the link-recovery feature.
		Once we enable link-recovery, the default Cisco recommended values for link-recovery parameters are populated.
		We can change the values of link recovery parameters from the default Cisco recommended values, by using CLI for each parameter like in example.
		Note
		Changing the default recommended Cisco values is not advised as it will impact ideal performance of linkrecovery feature.
		Note
		Only one of the three parameters (RSSI, RSRP, RSRQ) can be configured at a time. If no parameter is explicitly set by the user when link recovery is enabled, the system will fall back to the default value of RSSI.

	Command or Action	Purpose

	`monitor-timer 30`
	`Router(config-controller)#lte modem`
	`link-recovery wait-timer 15`
	`Router(config-controller)#lte modem`
	`link-recovery debounce-count 8`
	`Router(config-controller)#lte modem link-recovery`
	` rssi`
	`onset-threshold -100`
	For the RSRQ parameter:
	`Router#configure terminal`
	`Router(config)#controller`
	`Cellular 0/2/0`
	`Router(config-controller)#lte`
	`modem rsrq onset-threshold -`
	`19`
	For the RSRP parameter:
	`Router#configure terminal`
	`Router(config)#controller`
	`Cellular 0/2/0`
	`Router(config-controller)#lte`
	`modem rsrp onset-threshold -`
	`139`	

Step 4	**end**
	Example:
	`Router(config)# end`
		Exits the configuration mode and returns to the privileged EXEC mode.

Cellular modem link recovery parameters

There are three configurable parameters to adjust the behavior of cellular link recovery. The default values optimized for the best performance of the feature and changing it is not recommended unless advised by Cisco.

The following table explains the link recovery parameters.:

Table 22: Link recovery parameters

Parameter	Description
rssi onset-threshold	This parameter defines the RSSI value below which the link recovery feature triggers additional scrutiny to look for potential issues and take action if needed. The range of this parameter can be set from -90 dBm to -125 dBm. The recommended and default value is -110 dBm.

Parameter	Description
monitor-timer	This parameter determines how often link recovery looks for potential issues. The default value for this parameter is 20 seconds meaning that link recovery feature will be triggered every 20 seconds and look at certain parameters to determine if there is a potential issue. You can configure the monitor-timer range between 20 to 60 seconds. Increasing the monitor timer value above 20 seconds will increase the response time of the feature.
wait-timer and debounce-count	The wait-timer parameter is used in conjunction with the debounce-count parameter to perform more frequent, additional checks, once the link recovery feature has identified a potential issue that needs to be recovered from, with a modem power-cycle. The default value for wait-timer is 10 seconds and the default value for debounce- count is 6. With this setting, once link recovery has identified an inoperative modem state, it performs additional checks every 10 seconds, up to 6 times, to determine if the issue has been resolved without a modem power-cycle. Reducing the debounce-count and the wait-timer makes faster link recovery, while reducing them may increase the time for recovery. The configurable range for wait-timer is 5-60 seconds. The configurable range for debounce-count is 6-20 seconds.

Verifying the cellular modem link recovery configuration

To determine if the cellular modem link recovery is enabled, use the **show controller cellularunit** command. In this example, the cellular modem link recovery feature related information is highlighted.

```
Router# show controller cellular 0/2/0Interface Cellular0/2/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

Cellular Modem Configuration
==============================
Modem is recognized as valid
Power save mode is OFF
manufacture id =  0x00001199     product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status =  NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
---------------------------
SIM 0 is present
SIM 1 is not present
SIM 0 is active SIM

Module Reload Statistics
-------------------------
Soft OIR reloads = 0
Hard OIR reloads = 0
-------------------------

Modem Management Statistics
---------------------------
Modem resets = 1
Modem timeouts = 0
Link recovery is ON

Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6

Link recovery count is 0
```

When the cellular modem link recovery occurs and modem is power cycled, you can see the %CELLWAN-2-MODEM_DOWN message on the console logs and additionally there is a %CELLWAN-2-LINK_RECOVERY message which indicates that action has been taken by the cellular modem link recovery feature.

Whenever the cellular modem link recovery has occurred, it updates the Modem timeouts counter under the Modem Management Statistics section of the show controller cellular unit command output. Modem parameters at the last timeout section has information that helps to identify the cause of the issue that triggered link recovery

In the following example log, the messages, modem time out counter, and modem parameters at the last time out are highlighted.

***Jul 19 17:15:18.980 PDT: %CELLWAN-2-LINK_RECOVERY: Cellular0/1/0: Cellular Modem has been power cycled**

```
Router#show controller Cellular 0/2/0
Interface Cellular0/2/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

Cellular Modem Configuration
==============================
Modem is recognized as valid
Power save mode is OFF
manufacture id =  0x00001199     product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status =  NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
---------------------------
SIM 0 is present
SIM 1 is not present
SIM 0 is active SIM

Module Reload Statistics
-------------------------
```

```
Soft OIR reloads = 0
Hard OIR reloads = 0
-------------------------
 Modem Management Statistics
---------------------------
Modem resets = 1
Modem user initiated resets = 0
Modem user initiated power-cycles = 0
Modem timeouts = 1
Modem parameters at the last timeout:
         LTE first time attach State was No
         Radio Interface Technology Mode was AUTO
         Operating Mode was Online
         RSSI was -0 dBm
         Packet switch domain status was Not Attached
         Registration state(EMM) was Not Registered
         Downlink traffic was not present
Link recovery is ON
Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6
```

Configuration examples for 4G/LTE and 5G serviceability enhancement

Example: Sample output for the show cellular logs dm-log command

The following shows a sample output of the **show cellular logs dm-log** command:

```
Router# show cellular 0/2/0 logs dm-log
Integrated DM logging is on
filter = generic
maximum log size = 67108864
maximum file size = 20971520
log rotation = disabled
7 packets sent to the modem, 3232 bytes, 0 errors
75 packets received from the modem, 57123 bytes, 0 input drops
75 packets stored in file system, 57123 bytes, 0 errors, 0 aborts
2 max rcv queue size
current file size = 57123
current log size = 57123
total log size = 57123
DM log files: (1 files)
```

Example: Sample output for the show cellular logs modem-crashdump command

The following shows a sample output of the **show cellular logs modem-crashdump** command:

```
Router# show cellular 0/2/0 logs modem-crashdump
```

```
Modem crashdump logging: off
Progress = 100%
Last known State = Getting memory chunks
Total consecutive NAKs = 0
Number of retries = 0
Memory Region Info:
1: Full SDRAM [Base:0x0, Length:0x2000000]
2: MDSP RAM A region [Base:0x91000000, Length:0x8000]
3: MDSP RAM B region [Base:0x91200000, Length:0x8000]
4: MDSP RAM C region [Base:0x91400000, Length:0xC000]
5: MDSP Register region [Base:0x91C00000, Length:0x28]
6: ADSP RAM A region [Base:0x70000000, Length:0x10000]
7: ADSP RAM B region [Base:0x70200000, Length:0x10000]
8: ADSP RAM C region [Base:0x70400000, Length:0xC000]
9: ADSP RAM I region [Base:0x70800000, Length:0x18000]
10: CMM Script [Base:0x6A350, Length:0x310]
Router#
```

Configuration examples for Cisco LTE/5G

The following example shows how to configure Cisco LTE/5G:

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

Current configuration : 6256 bytes
!
! Last configuration change at 11:55:04 UTC Thu Sep 11 2025
!
version 17.18
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
!
hostname Router
!
boot-start-marker
boot system bootflash:c81g2be-universalk9.17.18.01a.SPA.bin
! Warning: Booting with bundle mode will be deprecated in the near future. Migration to
install mode is required.
boot-end-marker
!
!
no aaa new-model
!
!
!

Router#show running-config
Building configuration...

Current configuration : 6256 bytes
!
! Last configuration change at 11:55:04 UTC Thu Sep 11 2025
!
version 17.18
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
!
hostname Router
```

```
!
boot-start-marker
boot system bootflash:c81g2be-universalk9.17.18.01a.SPA.bin
! Warning: Booting with bundle mode will be deprecated in the near future. Migration to
install mode is required.
boot-end-marker
!
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-2631722432
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2631722432
 revocation-check none
 rsakeypair TP-self-signed-2631722432
 hash sha512
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha512
!
!
crypto pki certificate chain TP-self-signed-2631722432
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32363331 37323234 3332301E 170D3235 30393131 30393334
  32305A17 0D333530 39313130 39333432 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 36333137
  32323433 32308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100C22A BD9B5FB3 F22B9C03 E2E9CF90 9BF7F7E6 F596A9B5 B1C0117F
  FF0DCFAB 7582906E 18FF4F77 5DC350EF CC09C211 BC0FE3BC 04B9DFB5 E84DDB5C
  997B3DB9 0CB9770C 2E48ED85 2F99BA9D 9F6875DF 63670FAF F62733B8 3286A1F7
  6AB51D18 5D774CA0 43476A66 F35953EB B18A8FB1 F02139E9 90BA9309 14BAF62D
  FF4BDBD7 C2C9D293 8F75412D 8D78DB63 5F861264 7EEAAEEA 067A58FE 8F1C0F06
  C7E5CF52 9E29430E 8A9CA650 F2D98185 C71B6EB9 62783D23 0AC0CFE7 848D67F1
  76AEAA27 86288F31 8E99F8F0 E4BEA406 61EED885 D22A0CDA 8645B49E 11012D40
  0018D148 FFFFB23E D2A16682 C2EF1BA1 8A84FBEC 161DBDE6 4F516810 ECA18902
  921E650E 31630203 010001A3 53305130 1D060355 1D0E0416 0414AF6C 9E98EF87
  6C86D529 2D4693A9 3FB2E815 FEBF301F 0603551D 23041830 168014AF 6C9E98EF
  876C86D5 292D4693 A93FB2E8 15FEBF30 0F060355 1D130101 FF040530 030101FF
  300D0609 2A864886 F70D0101 0D050003 82010100 8BC35481 958BB958 D66B615C
  6902D390 D749BFD8 2CE27737 4002A965 EF141484 8BE093A0 63A8E869 2E447349
  976051BE 81AC192B 7F6AAAF7 122276B9 32F8D5DC 13B401F4 8AE7B9A4 42284EB6
  FFE4EF1A C218F289 7586B0E8 F347B24D 51FAC24E AF9FAF7F F0E54F2C 6CA7D1D7
  BBE42978 DB21EB26 E025E047 30D64CC3 D067AE02 6FD2F8BA 5C64567E 5B5CE4EE
  585E65D5 FA493B6D A2A6D053 DC4EF3C4 78CD81F1 4EB82678 33C7E51C A67D4C1E
  F9341D5A 0A7AD2EE 888BCCC6 41E1C4DC EDC2CD6F 892C9B2A 203D4DFB 4534DC77
  15AFF68F C94BDC6D AAEB55F3 BA563929 22EF95A8 62B3130C 2DE88DBA 62E51430
  EA812136 FEA032A9 D30C6D28 55FC492D E240D125
        quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
!
!
!
!
!
!
!
!
!
diagnostic bootup level minimal
!
license udi pid C8161-G2 sn FGL2924L2AU
memory free low-watermark processor 62736
!
```

```
spanning-tree extend system-id
!
!
!
redundancy
 mode none
!
!
!
!
!
!
controller Cellular 0/2/0
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0/1/4
!
interface GigabitEthernet0/1/5
!
interface GigabitEthernet0/1/6
 switchport
!
interface GigabitEthernet0/1/7
 switchport
!
```

```
interface Cellular0/2/0
 no ip address
!
interface Cellular0/2/1
 no ip address
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
ip forward-protocol udp
ip http server
ip http authentication local
ip http secure-server
!
ip ssh bulk-mode 131072
!
!
!
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
line con 0
 activation-character 13
 stopbits 1
line vty 0 4
 activation-character 13
 login
 transport input ssh
line vty 5 14
 activation-character 13
 login
 transport input ssh
!
!
!
!
!
!
!
end
```

Example: Basic cellular interface configuration Cisco LTE/5G

The following example shows how to configure the cellular interface to be used as a primary and is configured as the default route:

```
Router# show running-config
interface Cellular 0/2/0
```

```
ip address negotiated
dialer in-band
dialer-group 1
ip route 172.22.1.10 255.255.255.255 cellular 0/2/0
dialer-list 1 protocol ip permit
```

Configuration examples for Cisco LTE/5G

The following example shows how to configure Cisco LTE/5G:

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

Current configuration : 6256 bytes
!
! Last configuration change at 11:55:04 UTC Thu Sep 11 2025
!
version 17.18
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
!
hostname Router
!
boot-start-marker
boot system bootflash:c81g2be-universalk9.17.18.01a.SPA.bin
! Warning: Booting with bundle mode will be deprecated in the near future. Migration to
install mode is required.
boot-end-marker
!
!
no aaa new-model
!
!
!

Router#show running-config
Building configuration...

Current configuration : 6256 bytes
!
! Last configuration change at 11:55:04 UTC Thu Sep 11 2025
!
version 17.18
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
!
hostname Router
!
boot-start-marker
boot system bootflash:c81g2be-universalk9.17.18.01a.SPA.bin
! Warning: Booting with bundle mode will be deprecated in the near future. Migration to
install mode is required.
boot-end-marker
!
!
no aaa new-model
!
!
!
!
```

```
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-2631722432
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2631722432
 revocation-check none
 rsakeypair TP-self-signed-2631722432
 hash sha512
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha512
!
!
crypto pki certificate chain TP-self-signed-2631722432
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32363331 37323234 3332301E 170D3235 30393131 30393334
  32305A17 0D333530 39313130 39333432 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 36333137
  32323433 32308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100C22A BD9B5FB3 F22B9C03 E2E9CF90 9BF7F7E6 F596A9B5 B1C0117F
  FF0DCFAB 7582906E 18FF4F77 5DC350EF CC09C211 BC0FE3BC 04B9DFB5 E84DDB5C
  997B3DB9 0CB9770C 2E48ED85 2F99BA9D 9F6875DF 63670FAF F62733B8 3286A1F7
  6AB51D18 5D774CA0 43476A66 F35953EB B18A8FB1 F02139E9 90BA9309 14BAF62D
  FF4BDBD7 C2C9D293 8F75412D 8D78DB63 5F861264 7EEAAEEA 067A58FE 8F1C0F06
  C7E5CF52 9E29430E 8A9CA650 F2D98185 C71B6EB9 62783D23 0AC0CFE7 848D67F1
  76AEAA27 86288F31 8E99F8F0 E4BEA406 61EED885 D22A0CDA 8645B49E 11012D40
  0018D148 FFFFB23E D2A16682 C2EF1BA1 8A84FBEC 161DBDE6 4F516810 ECA18902
  921E650E 31630203 010001A3 53305130 1D060355 1D0E0416 0414AF6C 9E98EF87
  6C86D529 2D4693A9 3FB2E815 FEBF301F 0603551D 23041830 168014AF 6C9E98EF
  876C86D5 292D4693 A93FB2E8 15FEBF30 0F060355 1D130101 FF040530 030101FF
  300D0609 2A864886 F70D0101 0D050003 82010100 8BC35481 958BB958 D66B615C
  6902D390 D749BFD8 2CE27737 4002A965 EF141484 8BE093A0 63A8E869 2E447349
  976051BE 81AC192B 7F6AAAF7 122276B9 32F8D5DC 13B401F4 8AE7B9A4 42284EB6
  FFE4EF1A C218F289 7586B0E8 F347B24D 51FAC24E AF9FAF7F F0E54F2C 6CA7D1D7
  BBE42978 DB21EB26 E025E047 30D64CC3 D067AE02 6FD2F8BA 5C64567E 5B5CE4EE
  585E65D5 FA493B6D A2A6D053 DC4EF3C4 78CD81F1 4EB82678 33C7E51C A67D4C1E
  F9341D5A 0A7AD2EE 888BCCC6 41E1C4DC EDC2CD6F 892C9B2A 203D4DFB 4534DC77
  15AFF68F C94BDC6D AAEB55F3 BA563929 22EF95A8 62B3130C 2DE88DBA 62E51430
  EA812136 FEA032A9 D30C6D28 55FC492D E240D125
        quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
!
!
!
!
!
!
!
!
!
diagnostic bootup level minimal
!
license udi pid C8161-G2 sn FGL2924L2AU
memory free low-watermark processor 62736
!
spanning-tree extend system-id
!
!
!
redundancy
 mode none
!
!
!
!
!
!
controller Cellular 0/2/0
```

```
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0/1/4
!
interface GigabitEthernet0/1/5
!
interface GigabitEthernet0/1/6
 switchport
!
interface GigabitEthernet0/1/7
 switchport
!
interface Cellular0/2/0
 no ip address
!
interface Cellular0/2/1
 no ip address
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
ip forward-protocol udp
ip http server
ip http authentication local
ip http secure-server
!
ip ssh bulk-mode 131072
!
!
!
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
line con 0
 activation-character 13
 stopbits 1
line vty 0 4
 activation-character 13
 login
 transport input ssh
line vty 5 14
 activation-character 13
 login
 transport input ssh
!
!
!
!
!
!
!
end
```

Cellular back-off example

The following example shows how to configure the cellular back-off feature to stop continuous session activation requests back to the router:

```
Router#show cell 0/2/0 all
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
.
.
.
Profile 16, Packet Session Status = INACTIVE
Router#
Router#show cell 0/2/0 c n
Current System Time = Sun Jan 6 0:8:37 1980
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network = 123 456
```

```
Mobile Country Code (MCC) = 123
Mobile Network Code (MNC) = 456
Packet switch domain(PS) state = Attached
LTE Carrier Aggregation state = Deconfigured
Registration state(EMM) = Registered
EMM Sub State = Normal Service
Tracking Area Code (TAC) = 1801
Cell ID = 768001
Network MTU is not Available
Router#
Router#ping 192.0.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.192.187.254, timeout is 2 seconds:

*Dec 20 23:22:28.025: %CELLWAN-6-CELLULAR_BACKOFF_START: Cellular0/2/0: Cellular back-off
has started on PDN 0....
Success rate is 0 percent (0/5)
Router#

Router#ping 192.0.2.2
Type escape sequence to abort.
RouterSending 5, 100-byte ICMP Echos to 192.0.2.2, timeout is 2 seconds
.
.
.
Router#show cell 0/2/0
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
Router Call end mode = 3GPP
Router Session disconnect reason type = 3GPP specification defined(6)
Session disconnect reason = Option unsubscribed(33)
Enforcing cellular interface back-off
Period of back-off = 1 minute(s)
Profile 4, Packet Session Status = INACTIVE
...
Profile 16, Packet Session Status = INACTIVE
Router#
Router#show cell 0/2/0 cn
Sending 5, 100-byte ICMP Echos to 192.0.2.2, timeout is 2 seconds:
Router.....
Success rate is 0 percent (0/5)
Router#
Router#ping 192.0.2.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.5, timeout is 2 seconds:
Router.....
Success rate is 0 percent (0/5)
Router#show cell 0/2/0 cping 192.0.2.6  Type escape sequence to abort.
RouterSending 5, 100-byte ICMP Echos to 192.0.2.6 , timeout is 2 seconds:
Router.....
RouterSuccess rate is 0 percent (0/5)
Router#ping 192.0.2.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.6 , timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#ping 192.0.2.6
Router#sh cell 0/2/0 c
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
RouterCall end mode = 3GPP
RouterSession disconnect reason type = 3GPP specification defined(6)
RouterSession disconnect reason = Option unsubscribed(33)
RouterEnforcing cellular interface back-off
 Period of back-off = 1 minute(s)
Profile 4, Packet Session Status = INACTIVE
...
Profile 16, Packet Session Status = INACTIVE
Profile 4, Packet Session Status = INACTIVE
Profile 5, Packet Session Status = INACTIVE
.
.
.
Profile 16, Packet Session Status = INACTIVE
```

Example: GRE tunnel over cellular interface configuration

The following example shows how to configure the static IP address when a GRE tunnel interface is configured with **ip address unnumbered** *cellular interface*:

Note The GRE tunnel configuration is supported only if the service providers provide a public IP address on the LTE interface.

Note For service providers using a private IP address, the point-to-point static GRE tunnel cannot be set up with a private IP address at one end and a public IP address on the other end.

```
interface Tunnel2
ip unnumbered <internal LAN interface GE0/0 etc.>
tunnel source Cellular0/2/0
tunnel destination a.b.c.d
interface Cellular0/2/0
ip address negotiated
no ip mroute-cache
dialer in-band
dialer-group 1
```

Example: LTE/5G as backup with NAT and IPSec

The following example shows how to configure the LTE/5G on the router as backup with NAT and IPsec:

The receive and transmit speeds cannot be configured. The actual throughput depends on the cellular network service.

For service providers using a private IP address, use the **crypto ipsec transform-set esp** command (that is, esp-aes esp-sha256-hmac...).

```
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool lan-pool
   network 10.4.0.0 255.255.0.0
   dns-server 10.4.0.254
   default-router 10.4.0.254
!
```

```
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key  address a.b.c.d
!
!
crypto ipsec transform-set  ah-sha-hmac esp-3des
!
crypto map gsm1 10 ipsec-isakmp
 set peer a.b.c.d
 set transform-set
 match address 103
!
interface ATM0/2/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0/2/0.1 point-to-point
 backup interface Cellular0/2/0
ip address negotiated
ip mtu 1492
ip nat outside
ip virtual-reassembly
encapsulation ppp
load-interval 30
dialer pool 2
dialer-group 2
ppp authentication chap callin
ppp chap hostname cisco@dsl.com
ppp chap password 0 cisco
ppp ipcp dns request
crypto map gsm1

 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
  pppoe-client dial-pool-number 2
 !
!
interface Cellular0/2/0
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
no ip mroute-cache
 dialer in-band
 dialer idle-timeout 0
dialer-group 1
 crypto map gsm1
!
interface Vlan1
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
ip local policy route-map track-primary-if
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
```

```
!
ip nat inside source route-map nat2cell interface Cellular0/2/0 overload
ip nat inside source route-map nat2dsl overload
!
ip sla 1
 icmp-echo 2.2.2.2 source
 timeout 1000
 frequency 2
ip sla schedule 1 life forever start-time now
access-list 1 permit any
access-list 101 deny ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit icmp any host 2.2.2.2
access-list 103 permit ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
dialer-list 1 protocol ip list 1
dialer-list 2 protocol ip permit
!
!
route-map track-primary-if permit 10
 match ip address 102
!
route-map nat2dsl permit 10
 match ip address 101
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/2/0
!
exec-timeout 0 0
login
 modem InOut
```

Example: SIM configuration

Locking the SIM card

The following example shows how to lock the SIM. The italicized text in this configuration example is used to indicate comments and are not be seen when a normal console output is viewed.

```
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router# !! SIM is in unlocked state.!
Router# cellular 0/2/0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 19:35:28.339: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 19:35:59.967: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router# !! SIM is in locked state.!
```

Unlock the SIM card

The following example shows how to unlock the SIM. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router# !! SIM is in locked state.!
Router# cellular 0/2/0 lte sim unlock 1111
!!!WARNING: SIM will be unlocked with pin=1111(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router# !! SIM is in unlocked state.!
```

Automatic SIM authentication

The following example shows how to configure automatic SIM authentication. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# show cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router# !! SIM is in unlocked state.!Router# cellular 0/2/0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 21:22:34.555: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:23:06.495: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router# !! SIM is in locked state. SIM needs to be in locked state for SIM authentication
to ! work.!Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller cellular 0/2/0
Router(config-controller)# lte sim authenticate 0 1111
CHV1 configured and sent to modem for verification
Router(config-controller)# end
Router#
Apr 26 21:23:50.571: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router# sh cellular 0/2/0 security
```

```
Card Holder Verification (CHV1) = Enabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#!! SIM is now in locked state but it can be used for connectivity since authentication
 is ! good. Authentication can be saved in the router configuration so that when you boot
up ! the router with the same locked SIM, connection can be established with the correct !
 Cisco IOS configuration.!
```

Change the PIN Code

The following example shows how to change the assigned PIN code. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#!! SIM is in unlocked state.!Router#
Router# cellular 0/2/0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 21:58:11.903: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:58:43.775: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#!! SIM is in locked state. SIM needs to be in locked state to change its PIN.!Router#
Router# cellular 0/2/0 lte sim change-pin 1111 0000
!!!WARNING: SIM PIN will be changed from:1111(4) to:0000(4)
Call will be disconnected. If old PIN is entered incorrectly in 3 attempt(s), SIM will be
blocked!!!
Are you sure you want to proceed?[confirm]
Resetting modem, please wait...
CHV1 code change has been completed. Please enter the new PIN in controller configuration
for verfication
Router#
Apr 26 21:59:16.735: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:59:48.387: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#!! SIM stays in locked state, as expected, but with new PIN.!Router# cellular 0/2/0
 lte sim unlock 0000
!!!WARNING: SIM will be unlocked with pin=0000(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Router# show cellular 0/2/0 security
```

```
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#!! Unlock with new PIN is successful. Hence, changing PIN was successful.!
```

Configure an encrypted PIN

The following example shows how to configure automatic SIM authentication using an encrypted PIN. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# service password-encryption
Router(config)# username SIM privilege 0 password 1111
Router(config)# do sh run | i SIM
username SIM privilege 0 password 7 055A575E70.!! Copy the encrypted level 7 PIN. Use this
 scrambled PIN in the SIM authentication ! command.!

Router(config)# controller cellular 0/2/0
Router(config-controller)# lte sim authenticate 7 055A575E70
CHV1 configured and sent to modem for verification
Router(config-controller)# exit
Router(config)# no username SIM
Router(config)# end
May 14 20:20:52.603: %SYS-5-CONFIG_I: Configured from console by console
```

Upgrade the modem firmware

To upgrade the modem firmware, refer Cisco Firmware Upgrade Guide for 4G LTE and 5G Cellular Modems.

Troubleshooting

This section provides the essential information and resources available for troubleshooting the Cisco LTE/5G feature.

Verifying data call setup

To verify the data call setup, follow these steps:

1. After you create a modem data profile using the cellular profile create command and configuring DDR on the cellular interface, send a ping from the router to a host across the wireless network.
2. If the ping fails, debug the failure by using the following debug and show commands:
3. **debug chat**
4. **debug modem**
5. **debug dialer**
6. **show cellular all**

7. **show controller cell***0/2/0*
8. **show interface cellular**
9. **show running-config**
10. **show ip route**
11. **show platform**
12. Save the output from these commands and contact your system administrator.

Check signal strength

If the Received Signal Strength Indication (RSSI) level is very low (for example, if it is less than –110 dBm), follow these steps:

SUMMARY STEPS

1. Check the antenna connection. Make sure the TNC connector is correctly threaded and tightened.
2. If you are using a remote antenna, move the antenna cradle and check if the RSSI has improved.
3. Contact your wireless service provider to verify if there is service availability in your area.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Check the antenna connection. Make sure the TNC connector is correctly threaded and tightened.	
Step 2	If you are using a remote antenna, move the antenna cradle and check if the RSSI has improved.	
Step 3	Contact your wireless service provider to verify if there is service availability in your area.	

Verify service availability

The following is a sample output for the **show cellular all** command for a scenario where the antenna is disconnected and a modem data profile has not been created.

```
Router# show cellular 0/2/0 all
Hardware Information
====================
Modem Firmware Version = SWI9X30C_02.20.03.00
Modem Firmware built = 2016/06/30 10:54:05
Hardware Version = 1.0
Device Model ID: EM7455
International Mobile Subscriber Identity (IMSI) = 123456000031546
International Mobile Equipment Identity (IMEI) = 356129070052334
Integrated Circuit Card ID (ICCID) = 8949001508130031546
```

```
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Modem Online
Current Modem Temperature = 42 deg C
PRI SKU ID = 1102526, PRI version = 002.017_000, Carrier = Generic
OEM PRI version = 002

Profile Information
====================

Profile 1 = ACTIVE* **
--------
PDP Type = IPv4v6
PDP address = 29.29.29.196
PDP IPV6 address = 2001:2678:2680:5FD7:DDE7:70E1:DC07:CCB7/64  Scope: Global
Access Point Name (APN) = broadband
Authentication = None
        Primary DNS address = 8.0.0.8
        Secondary DNS address = 8.8.4.4
        Primary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8888
        Secondary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8844

Profile 2 = ACTIVE
--------
PDP Type = IPv4v6
PDP address = 21.21.21.206
PDP IPV6 address = 2001:567A:567A:1480:5DD6:18D1:BD63:49DA/64  Scope: Global
Access Point Name (APN) = basic
Authentication = None
        Primary DNS address = 171.70.168.183
        Secondary DNS address = 8.8.8.8
        Primary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8888
        Secondary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8844

Profile 3 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mpdn
Authentication = None

Profile 4 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = None

Profile 5 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = cisco.gw4.vzwentp
Authentication = None

Profile 6 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mobility-de1
Authentication = None

Profile 7 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mobility-de2
Authentication = None
```

```
Profile 8 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = None

Profile 9 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mpdndt-qos
Authentication = None

Profile 10 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mobility-de2
Authentication = None

Profile 11 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = None

Profile 12 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = wfqos
Authentication = CHAP
Username: ipv4v6
Password:

Profile 13 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = CHAP
Username: ipv4v6
Password:

Profile 14 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mobility-de2
Authentication = CHAP
Username: ipv4v6
Password:

Profile 15 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = aaaauth
Authentication = CHAP
Username: ipv4v6
Password:

Profile 16 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = CHAP
Username: ipv4v6
Password:
  * - Default profile
 ** - LTE attach profile


Configured default profile for active SIM 0 is profile 1.


Data Connection Information
===========================
Profile 1, Packet Session Status = ACTIVE
        Cellular0/2/0:
        Data Packets Transmitted = 198 ,  Received = 209
        Data Transmitted = 14410 bytes, Received = 24882 bytes
        IP address = 29.29.29.196
        IPV6 address = 2001:2678:2680:5FD7:DDE7:70E1:DC07:CCB7/64  Scope: Global
        Primary DNS address = 8.0.0.8
        Secondary DNS address = 8.8.4.4
        Primary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8888
        Secondary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8844
Profile 2, Packet Session Status = ACTIVE
        Cellular0/2/1:
        Data Packets Transmitted = 12 ,  Received = 13
        Data Transmitted = 1200 bytes, Received = 1144 bytes
        IP address = 21.21.21.206
        IPV6 address = 2001:567A:567A:1480:5DD6:18D1:BD63:49DA/64  Scope: Global
        Primary DNS address = 171.70.168.183
        Secondary DNS address = 8.8.8.8
        Primary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8888
        Secondary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8844
Profile 3, Packet Session Status = INACTIVE
Profile 4, Packet Session Status = INACTIVE
Profile 5, Packet Session Status = INACTIVE
Profile 6, Packet Session Status = INACTIVE
Profile 7, Packet Session Status = INACTIVE
Profile 8, Packet Session Status = INACTIVE
Profile 9, Packet Session Status = INACTIVE
Profile 10, Packet Session Status = INACTIVE
Profile 11, Packet Session Status = INACTIVE
Profile 12, Packet Session Status = INACTIVE
Profile 13, Packet Session Status = INACTIVE
Profile 14, Packet Session Status = INACTIVE
Profile 15, Packet Session Status = INACTIVE
Profile 16, Packet Session Status = INACTIVE

Network Information
===================
Current System Time = Tue Jan 8 23:24:22 1980
 --More--
*Jun 19 06:13:14.665: %IOSXE_OIR-6-INSSPA: SPA inserted in sCurrent Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network = 123 456
Mobile Country Code (MCC) = 123
Mobile Network Code (MNC) = 456
Packet switch domain(PS) state = Attached
LTE Carrier Aggregation state = Deconfigured
Registration state(EMM) = Registered
EMM Sub State = Normal Service
Tracking Area Code (TAC) = 1801
Cell ID = 768001
Network MTU is not Available

Radio Information
```

```
=================
Radio power mode = online
LTE Rx Channel Number =  2000
LTE Tx Channel Number =  20000
LTE Band =  4
LTE Bandwidth = 10 MHz
Current RSSI = -71 dBm
Current RSRP = -95 dBm
Current RSRQ = -7 dB
Current SNR = 26.4  dB
Physical Cell Id = 12
Number of nearby cells = 1
Idx      PCI (Physical Cell Id)
--------------------------------
1              12
Radio Access Technology(RAT) Preference = LTE
Radio Access Technology(RAT) Selected = LTE

Modem Security Information
==========================
Active SIM = 0
SIM switchover attempts = 0
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3

Cellular Firmware List
==========================
 Idx Carrier      FwVersion    PriVersion   Status
 1   ATT          02.20.03.00  002.019_000  Inactive
 2   GENERIC      02.20.03.00  002.017_000  Active
 3   SPRINT       02.20.03.22  002.020_000  Inactive
 4   TELSTRA      02.20.03.00  002.018_000  Inactive
 5   VERIZON      02.20.03.22  002.026_000  Inactive

Firmware Activation mode : AUTO

GPS Information
==========================

GPS Info
-------------
GPS Feature: enabled
GPS Mode Configured: not configured
GPS Status: NMEA Disabled

SMS Information
===============
Incoming Message Information
----------------------------
SMS stored in modem = 0
SMS archived since booting up = 0
Total SMS deleted since booting up = 0
Storage records allocated = 25
Storage records used = 0
Number of callbacks triggered by SMS = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0

Outgoing Message Information
----------------------------
Total SMS sent successfully = 0
Total SMS send failure = 0
```

```
Number of outgoing SMS pending = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0
Last Outgoing SMS Status = SUCCESS
Copy-to-SIM Status =     0x0
Send-to-Network Status = 0x0
Report-Outgoing-Message-Number:
  Reference Number =     0
  Result Code =          0x0
  Diag Code =            0x0 0x0 0x0 0x0 0x0

SMS Archive URL =

Error Information
=================

This command is not supported on 4G modems.


Modem Crashdump Information
===========================
Modem crashdump logging: off
```

Successful call setup

This is a sample output when a call is set up. It shows a received IP address from the network. Call setup is successful and data path is open.

```
debug dialer
debug cellular 0/2/0 messages callcontrol
```

Modem troubleshooting using integrated modem DM logging

The LTE modem dm-log command can be used in controller cellular configuration mode to configure integrated DM logging to monitor traffic on the modem. See the Cisco 3G and 4G Serviceability Enhancement User Guide for more information on configuring Integrated DM Logging parameters.

CHAPTER 22

Configure ethernet switch ports

This chapter contains the following sections:

Configure VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router. A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router.

Example: VLAN configuration

```
Router# configure terminal
 Router(config)# vlan 1
 Router(config)# vlan 2
 Router(config)# interface vlan 1
 Router(config-if)# ip address 192.0.2.1 255.255.255.0
 Router(config-if)# no shut
 Router(config-if)# interface vlan 2
 Router(config-if)# ip address 192.0.2.1 255.255.255.0
 Router(config-if)# no shut
 Router(config-if)# interface gigabitethernet 0/1/0
 Router(config-if)# switchport mode access
 Router(config-if)# switchport access vlan 1
 Router(config-if)# interface gigabitethernet 0/1/1
 Router(config-if)# switchport access vlan 2
 Router(config-if)# exit
```

Configure VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

You should understand the following concepts for configuring VTP.

- VTP domain: A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches or switch stacks under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.

- VTP server: In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP Version 3 should be configured on each switch manually including the VTP server and client. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links.VTP server is the default mode.

- VTP client: A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode.

- VTP transparent: VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode.

- VTP pruning is not supported.

For detailed information on VTP, see the following web link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1046901

Example: Configuring VTP

The following example shows how to configure the switch as a VTP server:

```
Router# configure terminal
Router(config)# vtp mode server
Router(config)# vtp domain Lab_Network
Router(config)# exit
```

The following example shows how to configure the switch as a VTP client:

```
Router# configure terminal
Router(config)# vtp domain Lab_Network
Router(config)# vtp mode client
Router(config)# exit
```

The following example shows how to configure the switch as VTP transparent:

```
Router# configure terminal
Router(config)# vtp mode transparent
Router(config)# exit
```

Configure 802.1x authentication

IEEE 802.1x port-based authentication defines a client-server-based access control and authentication protocol to prevent unauthorized clients from connecting to a LAN through publicly accessible ports.The authentication server authenticates each client connected to a switch port before allowing access to any switch or LAN services. Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic passes through the port.

With IEEE 802.1x authentication, the devices in the network have specific roles:

- Supplicant—Device (workstation) that requests access to the LAN and switch services and responds to requests from the router. The workstation must be running IEEE 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The supplicant is sometimes called the client.)
- Authentication server—Device that performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services. The Network Access Device transparently passes the authentication messages between the supplicant and the authentication server, and the authentication process is carried out between the supplicant and the authentication server. The particular EAP method used will be decided between the supplicant and the authentication server (RADIUS server). RADIUS operates in a client and server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- Authenticator—Router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

Example: Enabling IEEE 802.1x and AAA on a Switch Port

This example shows how to configure Cisco 8100 Series Secure Routers as 802.1x authenticator:

```
Router> enable
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# switchport mode access
Router(config-if)# access-session port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# access-session closed
Router(config-if)# access-session host-mode single-host
Router(config-if)# service-policy type control subscriber interface_policy
Router(config-if)# end
```

Note Cisco 8100 Series Secure Routers switchport do not support the **authentication timer inactivity** command. Due to this, when the MAB client behind the hub is peered, the MAB session is not terminated for prolonged inactivity. mac-move is not supported under this condition.

Instead if you can directly connect to the endpoint or use the dot1x configuration, mac-move works as expected.

dot1x also requires related config like aaa, radius, IBNS(Cisco Identity Based Networking Services) to work together.

Configure spanning tree protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

For detailed configuration information on STP see the following link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4_8PortGENIM.html#pgfId-1079138

Example: Spanning Tree Protocol Configuration

The following example shows configuring spanning-tree port priority of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses the port priority when selecting an interface to put in the forwarding state.

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# spanning-tree vlan 1 port-priority 64
Router(config-if)# end
```

The following example shows how to change the spanning-tree port cost of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state.

```
Router#configure terminal
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# spanning-tree cost 18
Router(config-if)# end
```

The following example shows configuring the bridge priority of VLAN 10 to 33792:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 priority 33792
Router(config)# end
```

The following example shows configuring the hello time for VLAN 10 being configured to 7 seconds. The hello time is the interval between the generation of configuration messages by the root switch.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 hello-time 7
Router(config)# end
```

The following example shows configuring forward delay time. The forward delay is the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 forward-time 21
Router(config)# end
```

The following example shows configuring maximum age interval for the spanning tree. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 max-age 36
Router(config)# end
```

The following example shows the switch being configured as the root bridge for VLAN 10, with a network diameter of 4.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# exit
```

Configure MAC address table manipulation

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address: a source MAC address that the switch learns and then drops when it is not in use. You can use the aging time setting to define how long the switch retains unseen addresses in the table.
- Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port associated with the address and the type (static or dynamic).

See the “Example: MAC Address Table Manipulation” for sample configurations for enabling secure MAC address, creating a statc entry, set the maximum number of secure MAC addresses and set the aging time.

For detailed configuration information on MAC address table manipulation see the following link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1048223

Example: MAC Address Table Manipulation

The following example shows creating a static entry in the MAC address table.

```
Router# configure terminal
Router(config)# mac address-table static 0002.0003.0004 interface GigabitEthernet 0/1/0
vlan 3
Router(config)# end
```

The following example shows setting the aging timer.

```
Router# configure terminal
Router(config)# mac address-table aging-time 300
Router(config)# end
```

Configuring switch port analyzer

Cisco 8100 Series Secure Routers support local SPAN only, and upto one SPAN session. You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source can be monitored by using SPAN; traffic routed to a source cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another source cannot be monitored; however, traffic that is received on the source and routed to another can be monitored.

Example: SPAN Configuration

The following example shows how to configure a SPAN session to monitor bidirectional traffic from a Gigabit Ethernet source interface:

```
Router# configure terminal
Router(config)# monitor session 1 source gigabitethernet 0/1/0
Router(config)# end
```

The following example shows how to configure a gigabit ethernet interface as the destination for a SPAN session:

```
Router# configure terminal
Router(config)# monitor session 1 destination gigabitethernet 0/1/0
Router(config)# end
```

The following example shows how to remove gigabit ethernet as a SPAN source for SPAN session 1:

```
Router# configure terminal
Router(config)# no monitor session 1 source gigabitethernet 0/1/0
Router(config)# end
```

Configuring flex support on layer 2 and layer 3 ports

From Cisco IOS XE Release 17.18.1a, flex support on Layer 2 and Layer 3 ports is enabled on the last two ports of the front-panel Layer 2 switch ports of Cisco 8100 Series Secure Routers. This provides additional Layer 3 WAN port flexibility on the device. The flex ports can be configured as either a Layer 2 port or a Layer 3 port based on the requirement.

Restrictions for flex support on layer 2 and layer 3 ports

- Flex port support is enabled only on Cisco 8100 Series Secure Routers that have four or eight front-panel switch ports.
- The last two ports of the front-panel fixed ports are the flex ports.
- The two internal VLANs are dynamically reserved for two Layer 3 ports to isolate the Layer 3 traffic and separate the forwarding database for MAC filtering.
- Flex Layer 2 and Layer 3 interfaces do not have PoE support because PoE is enabled only on the half lower number interfaces.
- Weighted Round Robin (WRR) bandwidth and Quality of Service (QoS) mapping configuration are global.
- 802.3x TX pause is not supported on flex Layer 2 and Layer 3 ports.
- PLIM QoS is not supported on flex Layer 3 ports.
- All ingress Layer 3 or Switch Virtual Interfaces (SVI) traffic is throttled if flow control is received.

How to configure flex ports

The flex ports are set to Layer 2 interface by default. They can be configured to the Layer 3 port using **no switchport** command and can be returned to the Layer 2 port using **switchport** command. After the interface is converted to Layer 2 or Layer 3, the corresponding Layer 2 or Layer 3 CLIs will be available on that interface.

Configuring flex port to layer 3 port

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no switchport**
5. **ip address** *address mask*
6. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config-if)# interface GigabitEthernet 0/1/6`	Enters configuration mode for the specified interface on the device.
Step 4	**no switchport** **Example:** `Device(config-if)# no switchport`	Converts the port from Layer 2 interface to Layer 3 interface and makes it a routing interface rather than a switch port.
Step 5	**ip address** *address mask* **Example:** `Device(config-if)# ip address 10.10.0.1 255.255.255.0`	Sets the IP address and subnet mask for the specified interface.
Step 6	**exit** **Example:**	Exits configuration mode for the specified interface and returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-if)# exit`	

Configure flex port to layer 2 port

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **switchport**
5. **switchport mode** {**access** \| **dynamic** \| **trunk trunk**
6. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config-if)# interface GigabitEthernet 0/1/6`	Enters configuration mode for the specified interface on the device.
Step 4	**switchport** **Example:** `Device(config-if)# switchport`	Converts the port from Layer 3 interface to Layer 2 interface and makes it a routing interface rather than a switch port.
Step 5	**switchport mode** {**access** | **dynamic** | **trunk trunk** **Example:** `Device(config-if)# switchport mode access`	Configures the operational mode on a Layer 2 interface.
Step 6	**exit** **Example:** `Device(config-if)# exit`	Exits configuration mode for the specified interface and returns to global configuration mode.

Configuration Examples

The following are examples of Layer 2 and Layer 3 port configurations.

Example: Flex Port to Layer 3 Port Configuration

The following example shows how to convert a flex port to a Layer 3 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.0.1 255.255.255.0
Device(config-if)# exit
```

Example: Flex Port to Layer 2 Port Configuration

The following example shows how to convert a flex port to a Layer 2 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# exit
```

Verifying flex port configuration

Use the **show platform hardware subslot** *slot*/*card* **module interface** *type number* **status** command to display information about the platform hardware. If the flex port is configured as Layer 3 port, the output displays the L3_NETWORK. If the flex port is configured as Layer 2 port, the output displays the L2_NETWORK.

The following is a sample Layer 3 port configuration verification output:

```
GE6:
MAC Status: hw_port 7, speed 1000, duplex full, link Up, link_en Enable , fc Enable
L3_NETWORK
```

Configure IGMP snooping

IGMP snooping constrains the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry.

Use the **`[no] ip igmp snooping enable`** command to configure IGMP Snooping on Cisco 8100 Series Secure Routers.

By default, IGMP snooping is globally enabled in Cisco 8100 Series Secure Routers.

When IGMP snooping is enabled on Cisco 8100 Series Secure Routers, and there are no local receivers for multicast traffic in the VLAN, the multicast traffic floods to all ports in the VLAN.

Configure HSRP

Note HSRP is supported only on the SVI interface.

The Hot Standby Router Protocol (HSRP) is Cisco's standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

HSRP uses a priority mechanism to determine which HSRP configured device is to be the default active device. To configure a device as the active device, you assign it a priority that is higher than the priority of all the other HSRP-configured devices. The default priority is 100, so if you configure just one device to have a higher priority, that device will be the default active device. In case of ties, the primary IP addresses are compared, and the higher IP address has priority. If you do not use the standby preempt interface configuration command in the configuration for a router, that router will not become the active router, even if its priority is higher than all other routers.

Example: Configuring HSRP

In this example, Router A is configured to be the active device for group 1 and standby device for group 2. Device B is configured as the active device for group 2 and standby device for group 1.

```
RouterA# configure terminal
RouterA(config)# interface vlan 2
RouterA(config-if)# ip address 10.1.0.21 255.255.0.0
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.0.3
RouterA(config-if)# standby 2 priority 95
RouterA(config-if)# standby 2 preempt
RouterA(config-if)# standby 2 ip 10.1.0.4
RouterA(config-if)# end

RouterB# configure terminal
RouterB(config)# interface vlan 2
RouterB(config-if)# ip address 10.1.0.22 255.255.0.0
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.0.3
RouterB(config-if)# standby 2 priority 110
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 ip 10.1.0.4
```

Configure VRRP

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the primary virtual router, with the other routers acting as backups in case the primary virtual router fails.

An important aspect of the VRRP is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the primary virtual router fails. If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router will function as a primary virtual router. Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming a primary virtual router if the primary virtual router fails. You can configure the priority of each virtual router backup using the vrrp priority command.

By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become primary virtual router. You can disable this preemptive scheme using the no vrrp preempt command. If preemption is disabled, the virtual router backup that is elected to become virtual router primary remains the primary until the original primary virtual router recovers and becomes primary again.

The primary virtual router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the primary virtual router. The VRRP advertisements are encapsulated in IP packets and sent to the IP Version 4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable.

For more information on VRRP, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html

Example: Configuring VRRP

In the following example, Router A and Router B each belong to two VRRP groups, group1 and group 5. In this configuration, each group has the following properties:

Group 1:

- Virtual IP address is 10.1.0.10.
- Router A will become the primary for this group with priority 120.
- Advertising interval is 3 seconds.
- Preemption is enabled.

Group 5:

- Router B will become the primary for this group with priority 200.
- Advertising interval is 30 seconds.
- Preemption is enabled.

```
RouterA(config)# interface vlan 2
RouterA(config-if)# ip address 10.1.0.2 255.0.0.0
RouterA(config-if)# vrrp 1 priority 120
RouterA(config-if)# vrrp 1 authentication cisco
RouterA(config-if)# vrrp 1 timers advertise 3
RouterA(config-if)# vrrp 1 timers learn
RouterA(config-if)# vrrp 1 ip 10.1.0.10
RouterA(config-if)# vrrp 5 priority 100
RouterA(config-if)# vrrp 5 timers advertise 30
RouterA(config-if)# vrrp 5 timers learn
RouterA(config-if)# vrrp 5 ip 10.1.0.50
RouterA(config-if)# no shutdown
RouterA(config-if)# end
RouterB(config)# interface vlan 2
RouterB(config-if)# ip address 10.1.0.1 255.0.0.0
RouterB(config-if)# vrrp 1 priority 100
RouterB(config-if)# vrrp 1 authentication cisco
RouterB(config-if)# vrrp 1 timers advertise 3
RouterB(config-if)# vrrp 1 timers learn
RouterB(config-if)# vrrp 1 ip 10.1.0.10
RouterB(config-if)# vrrp 5 priority 200
RouterB(config-if)# vrrp 5 timers advertise 30
RouterB(config-if)# vrrp 5 timers learn
RouterB(config-if)# vrrp 5 ip 10.1.0.50
RouterB(config-if)# no shutdown
RouterB(config-if)# end
```

CHAPTER 23

Interface configuration

This chapter contains the following sections:

Configuring the interfaces

The following sections describe how to configure interfaces and also provide examples of configuring the router interfaces:

Configuring the interfaces example

The following example shows the **interface gigabitEthernet** command being used to add the interface and set the IP address. **0/0/0** is the slot/subslot/port. The ports are numbered 0 to 3.

```
Router# show running-config interface gigabitEthernet 0/0/0
Building configuration...
Current configuration : 71 bytes
!
interface gigabitEthernet0/0/0
no ip address
negotiation auto
end

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitEthernet 0/0/0
```

Note Several Cisco platforms, NIMs, and SM cards support configuring multiple-rate SFPs on same interface, e.g., 1G SFP or 10G SFP+ on a 10G port.

In a port-channel bundle, all member interfaces should be of same speed, and duplex. It is recommended to use duplex interfaces of the same speed as member interfaces for configuring a port-channel.

For more information about interfaces that support multiple-rate SFPs, see the corresponding datasheets.

Viewing a list of all interfaces: Example

In this example, **show interfaces summary** command is used to display all the interfaces:

```
Router# show interfaces summary
    *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD      RXBS      RXPS
TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------
* GigabitEthernet0/0/0          0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/0/1          0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/0          0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/1          0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/2          0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/3          0         0         0         0         0         0
  0         0         0

  Interface                   IHQ       IQD       OHQ       OQD      RXBS      RXPS
TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------
* GigabitEthernet0/1/4          0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/5          0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/6          0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/7          0         0         0         0         0         0
  0         0         0
* Wl0/1/8                       0         0         0         0         0         0
  0         0         0
* Cellular0/2/0                 0         0         0         0         0         0
  0         0         0
  Cellular0/2/1                 0         0         0         0         0         0
  0         0         0
* Loopback3                     0         0         0         0         0         0
  0         0         0
* Loopback50                    0         0         0         0         0         0
  0         0         0
* Loopback100                   0         0         0         0         0         0
  0         0         0
* Loopback544534                0         0         0         0         0         0
  0         0         0
```

Viewing information about an interface: Example

The following example shows how to display a brief summary of an interface's IP information and status, including the virtual interface bundle information, by using the **show ip interface brief** command:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.1.46    YES NVRAM  up                    up
```

```
GigabitEthernet0/0/1   192.0.2.1      YES NVRAM  up                   up
GigabitEthernet0/1/0   unassigned      YES unset  up                    up
GigabitEthernet0/1/1   unassigned      YES unset  up                    up
GigabitEthernet0/1/2   unassigned      YES unset  up                    up
GigabitEthernet0/1/3   unassigned      YES unset  up                    up
GigabitEthernet0/1/4   unassigned      YES unset  up                    up
GigabitEthernet0/1/5   unassigned      YES unset  up                    up
GigabitEthernet0/1/6   unassigned      YES unset  up                    up
GigabitEthernet0/1/7   unassigned      YES unset  up                    up
Wl0/1/8                unassigned      YES unset  up                    up
Cellular0/2/0          unassigned      YES NVRAM  up                    up
Cellular0/2/1          unassigned      YES NVRAM  administratively down down
Loopback3              unassigned      YES unset  up                    up
Loopback50             192.0.2.2        YES NVRAM  up                    up
Loopback100            unassigned      YES unset  up                    up
Loopback544534         unassigned      YES unset  up                    up
Loopback32432532       unassigned      YES unset  up                    up
Port-channel2          unassigned      YES unset  down                  down
Vlan1                  10.10.10.1      YES NVRAM  up                    up
```

CHAPTER 24

Configure SFP auto-failover

This chapter contains the following sections:

- Enable auto-detect, on page 279

Enable auto-detect

When the media-type is not configured, the auto-detect feature is enabled by default. The auto-detect feature automatically detects the media that is connected and links up. If both the media are connected, whichever media comes up first is linked. By default, the media-type on FPGE ports is set to auto-select. User can overwrite the media-type configuration to either RJ-45 or SFP using the **media-type rj45/sfp** command under the FPGE interface. The media type configuration also falls back to "Auto-select" mode when the **no media-type** command is configured. You can use the **no media-type** command in interface configuration mode to enable the Auto-Detect feature.

Configuring auto-detect

The auto-detect feature is enabled by default on the Front Panel Gige Ports. Auto-failure is enabled by default when auto-select is enabled. To configure the auto-detect, perform these steps:

SUMMARY STEPS

1. **configure terminal**
2. **interface gigabitethernet** {**slot** | **bay**| **port**}
3. **media-type auto-select**
4. **End**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 2	**interface gigabitethernet** {**slot** | **bay**| **port**}
	Example:
	`Router(config)# interface gigabitethernet 0/0/0`
		Enters interface configuration mode.

Step 3	**media-type auto-select** **Example:** `Router(config-if)# media-type auto-select`	Auto-select mode uses whichever connector is attached. The options are: • **rj45**—Uses RJ45 connector. • **sfp**—Uses SFP connector. • **auto-select**
Step 4	**End** **Example:** `Router(config-if)#end`	Exits configuration mode.

The following example shows the default configuration and the show running configuration does not show any media type when the no media-type is selected.

```
Router(config)# show running interface gigabitethernet 0/0/0
Building configuration...

Current configuration : 71 bytes
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
end
```

Configuring the primary and secondary media

When the router receives an indication that the primary media is down, the secondary failover media is enabled. After the switchover, the media does not switch back to primary media when the primary media is restored. You need to use either **shut** or **no shut** command or reload the module to switch the media-type back to primary(preferred) media.

To assign the primary or secondary failover media on the GE-SFP port, perform these steps:

SUMMARY STEPS

1. **configure terminal**
2. **interface gigabitethernet** {**slot** | **bay** | **port**}
3. **media-type rj45 autofailover**
4. **End**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 2	**interface gigabitethernet** {**slot** | **bay** | **port**}
	Example:
	`Router(config)# interface gigabitethernet slot/bay/port`
		Enters interface configuration mode.

Step 3	**media-type rj45 autofailover** **Example:** `Router(config-if)# media-type rj45 autofailover`	Configures the port with rj45 as the primary media for automatic failover.
Step 4	**End** **Example:** `Router(config-if)#end`	Exits configuration mode.

The following example shows the primary configuration.

```
Router(config)# show running interface gigabitethernet 0/0/0
Building configuration...

Current configuration : 102 bytes
!
interface GigabitEthernet0/0/0
 no ip address
 media-type rj45 auto-failover
 negotiation auto
end
```

CHAPTER 25

Configuring cellular IPv6 address

This chapter contains the following sections:

Cellular IPv6 address

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of IPv6 addresses:

- 2001:DB8:FFFF:0000:0000:0000:0001
- 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF

IPv6 addresses commonly contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). The table below lists compressed IPv6 address formats.

An IPv6 address prefix, in the format ipv6-prefix/prefix-length, can be used to represent bit-wise contiguous blocks of the entire address space. The ipv6-prefix must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). For example, 2001:DB8::1/64 is a valid IPv6 prefix.

IPv6 unicast routing

An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.

Cisco 8100 Series Secure Routers support the following address types:

Link-Lock Address

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. An link-local address is automatically configured on the cellular interface when an IPv6 address is enabled.

After the data call is established, the link-local address on the celluar interface is updated with the host generated link-local address that consists of the link-local prefix FF80::/10 (1111 1110 10) and the auto-generated interface identifier from the USB hardware address. The figure below shows the structure of a link-local address.

Global Address

A global IPv6 unicast address is defined by a global routing prefix, a subnet ID, and an interface ID. The routing prefix is obtained from the PGW. The Interface Identifier is automatically generated from the USB hardware address using the interface identifier in the modified EUI-64 format. The USB hardware address changes after the router reloads.

Configuring Cellular IPv6 Address

To configure the cellular IPv6 address, perform these steps:

SUMMARY STEPS

1. **configure terminal**
2. **interface cellular** {**type** | **number**}
3. ip address negotiated
4. load-interval***seconds***
5. dialer in-band
6. dialer idle-timeout ***seconds***
7. dialer string **string**
8. dialer-group**group-number**
9. no peer default ip address
10. ipv6 address autoconfig
11. async mode interactive
12. routing dynamic
13. **dialer-listdialer-groupprotocolprotocol-name** {**permit** |deny|**list** |*access-list-number* | *access-group* }
14. **ipv6 route** *ipv6-prefix/prefix-length 128*
15. **End**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 2	**interface cellular** {**type** | **number**}
	Example:
	`Router(config)# interface cellular 0/1/0`
		Specifies the cellular interface.

	Command or Action	Purpose
Step 3	ip address negotiated **Example:** `Router(config-if)# ipv6 address negotiated`	Specifies that the IP address for a particular interface is dynamically obtained.
Step 4	load-interval***seconds*** **Example:** `Router(config-if)# load-interval 30`	Specifies the length of time for which data is used to compute load statistics.
Step 5	dialer in-band **Example:** `Router(config-if)# dialer in-band`	Enables DDR and configures the specified serial interface to use in-band dialing.
Step 6	dialer idle-timeout ***seconds*** **Example:** `Router(config-if)# dialer idle-timeout 0`	Specifies the dialer idle timeout period.
Step 7	dialer string **string** **Example:** `Router(config-if)# dialer string lte`	Specifies the number or string to dial.
Step 8	dialer-group**group-number** **Example:** `Router(config-if)# dialer-group 1`	Specifies the number of the dialer access group to which the specific interface belongs.
Step 9	no peer default ip address **Example:** `Router(config-if)# no peer default ip address`	Removes the default address from your configuration.
Step 10	ipv6 address autoconfig **Example:** `Router(config-if)# ipv6 address autoconfig`	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.
Step 11	async mode interactive **Example:** `Router(config-if)# async mode interactive`	Please provide the inputs?
Step 12	routing dynamic **Example:** `Router(config-if)#routing dynamic`	Enables the router to pass routing updates to other routers through an interface.
Step 13	**dialer-listdialer-groupprotocolprotocol-name** {**permit** |deny|**list** |*access-list-number* | *access-group* } **Example:**	Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.

	Command or Action	Purpose
	`Router(config)# dialer-list 1 protocol ipv6 permit`	
Step 14	**ipv6 route** *ipv6-prefix/prefix-length 128* **Example:** `Router(config)#ipv6 route 2001:1234:1234::3/128 Cellular0/1/0`	
Step 15	**End** **Example:** `Router(config-if)#end`	Exits to global configuration mode.

Examples

The following example shows the Cellular IPv6 configuration .

```
Router(config)# interface Cellular0/0/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer-group 1
no peer default ip address
ipv6 address autoconfig
async mode interactive
routing dynamic
!
interface Cellular0/1/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer-group 1
no peer default ip address
ipv6 address autoconfig
async mode interactive
routing dynamic

dialer-list 1 protocol ipv6 permit
ipv6 route 2001:1234:1234::/64 Cellular0/1/0
ipv6 route 2001:4321:4321::5/128 Cellular0/1/1
```

CHAPTER 26

Dying gasp through ethernet OAM

Dying Gasp is a final notification, or a signal sent by a device when it is about to lose power. The device sends a signal to alert a peer device, which identifies and responds to the power related issues. The occurrence of an unrecoverable condition like Power Failure triggers Dying Gasp.

Ethernet Operations, Administration, and Maintenance (OAM) is a set of protocols that monitors and manages Ethernet networks. For interfaces where Ethernet OAM is enabled, the device sends a Dying Gasp message using an Ethernet OAM protocol. It supports the generation of the Ethernet OAM Dying Gasp packets to notify the remote peer device that the local device is having a power failure.

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

Note Dying Gasp is only supported on power failure. It is not supported on:

- Reload
- Shutdown

Prerequisites for dying gasp support

- The ethernet OAM is enabled by default on L3 interface.

  The Dying Gasp feature can be disabled using the command:

  ```
  Router(config-if)#ethernet oam mode passive
  ```

  It can be enabled again by using this command:

  ```
  Router (config-if)#ethernet oam mode active
  ```

- Ethernet OAM is sent out only when there is power loss.

Restrictions for dying gasp support

- Cisco 8100 Series Secure Routers power failure dying gasp only support sending out Ethernet OAM packets.
- Dying Gasp feature is not supported during a power loss, while a signal is initiated using jumbo frames with 10M of WAN line.
- Cisco 8100 Series Secure Routers support dying gasp on WAN front GE interfaces.

Information about dying gasp through ethernet OAM

Dying Gasp

One of the OAM features as defined by IEEE 802.3ah is Remote Failure Indication, which helps in detecting faults in Ethernet connectivity that are caused by slowly deteriorating quality. Ethernet OAM provides a mechanism for an OAM entity to convey these failure conditions to its peer via specific flags in the OAM PDU. One of the failure condition method to communicate is Dying Gasp, which indicates that an unrecoverable condition has occurred. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously.

How to configure dying gasp ethernet OAM

Dying gasp notification on the peer router

```
001689: *May 30 14:16:47.746 IST: %ETHERNET_OAM-6-RFI: The client on interface Gi0/0/0 has
 received a remote failure indication from its remote peer(failure reason = remote client
power failure action = )
```

Configuring OAMPDU

With the new Dying Gasp feature in the Cisco 8100 Series Secure Routers, you can configure the **Code** field value in the OAMPDU frame. The allowed values to be configured are:

- **Information**: Indicates the OAM package is transferring local or remote information data. 0x00 stands for Information OAMPDU.
- **Organization specific**: Indicates that this is reserved for vendors. Each vendor can use this code to carry customized data. 0xFE stands for organization specific OAMPDU which is the default type set for OAMPDU.

Configuring information OAMPDU

```
Router# enable
 Router# configure terminal
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ethernet oam dying-gasp type information
Router(config-if)# exit
Router(config)# exit
Router#show ethernet oam status interface GigabitEthernet0/0/0
GigabitEthernet0/0/0
General
-------
  Admin state:           enabled
  Mode:                  passive
  Type:                  information
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1000 ms
… …
```

Configuring organization specific OAMPDU

```
Router# enable
 Router# configure terminal
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ethernet oam dying-gasp type organization
Router (config-if)# exit
Router(config)# exit
Router# show ethernet oam status interface GigabitEthernet0/0/0
GigabitEthernet0/0/0
General
-------
  Admin state:           enabled
  Mode:                  passive
  Type:                  organization
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1000 ms
```

CHAPTER 27

Tamper detection

The Tamper Detection feature is designed to enhance the physical security by identifying unauthorized access to the device's internal components. Each device is shipped from the factory with its cover screwed tightly. If the cover is subsequently opened, the hardware records these open or close events in a tamper-proof memory. This recording occurs whether the system is powered on or off. Upon boot-up, the IOS software reads these recorded events and compares them against previously known event indices. If discrepancies are found, the software generates a syslog message, alerting the user to a potential tamper event.

Note The ability to send the alarm depends on the the WAN interface (Ethernet or LTE connectivity) being available at the time of the occurrence of the tamper detection.

Tamper detection capabilities and event logging

The tamper detection hardware operates independently of the software configuration, continuously recording cover open or close events. These events are stored in two dedicated memory sections:

1. **System fully powered off**:
   - When the system is powered off, a battery powers the hardware to record events.
   - Only the *first* cover open event between the last power-off and the next power-on is recorded, even if multiple open/close events occur during this period.
   - This section can log up to 250 events (2KB). If the log capacity is reached, it will roll over, and a rollover flag will be set.
2. **System partially or fully powered up**:
   - When system power is available, the hardware records all cover open or close events.
   - This section can log up to 506 events (4KB). Similar to the power-off section, the log will roll over if full, and a rollover flag will be set.

Restrictions of tamper detection

- During a fully powered-off state, only the *first* cover open event is recorded. Subsequent open or close events during the same power-off cycle are not logged.
- Each event log section has a finite capacity (250 for power-off, 506 for power-on). Once full, the logs roll over, potentially overwriting older events, though a rollover flag indicates this.

How to configure tamper detection

Tamper detection is enabled by default, meaning the hardware continuously records events. The software configuration primarily controls whether syslog notifications are displayed during boot-up when new tamper events are detected.

To prevent the system from displaying syslog messages related to tamper events during boot-up, you can disable the feature's notification capability. This does not stop the hardware from recording events.

Router(config)# no platform tamper-detection

When this command is configured, users will not see the tamper event messages during boot-up, even if new events have occurred.

Procedure

Step 1 request consent-token generate-challenge tamper-auth auth-timeout <timeout value in minutes>

Generates a challenge for consent token.

Step 2 request consent-token accept-response tamper-auth <response_string>

Accept the response with the generated challenge.

Step 3 request platform hardware tamper-detection event-mark

Post successful execution, the system confirms that the tamper event has been marked and terminate the authentication session.

Examples

Dumping event logs

A `show` command is available to dump all or a specified number of recent tamper events from either the power-on or power-off log sections. This command is accessible regardless of whether tamper detection notifications are enabled or disabled.

Example 1: Showing the last 4 power-on tamper events

```
Router# show platform tamper-detection event power-on lastx 4

Current Time: 2025/02/11 08:22:07    Rollover Status: No    Rollover Count: 0
------------------------------------------------------------------------------------------
Tamper event index   |   Tamper event timestamp   |   Tamper events description
------------------------------------------------------------------------------------------

    #6               2023/08/01 10:33:21          Chassis is opened
    #5               2023/08/01 10:33:15          Chassis is closed
    #4               2023/08/01 10:33:15          Chassis is opened
    #3               2023/08/01 10:33:15          Chassis is closed
```

The output includes the event index, timestamp, and a description of the event (Chassis is opened/closed).

Example 2: Showing power-on events with log rollover

```
Router# show platform tamper-detection event power-on lastx 2

Current Time: 2023/10/01 15:28:56    Rollover Status: Yes    Rollover Count: 5
------------------------------------------------------------------------------------------
Tamper event index   |   Tamper event timestamp   |   Tamper events description
------------------------------------------------------------------------------------------

    #2627            2023/08/12 08:44:40          Chassis is closed
    #2626            2023/08/12 08:41:27          Chassis is opened
```

In this example, "Rollover Status: Yes" and "Rollover Count: 5" indicate that the event log has rolled over 5 times, meaning older events have been overwritten.

Consent token authentication example

The `event-mark` command requires consent token authentication for security. Below is an example of the workflow:

```
Router# request consent-token generate-challenge tamper-auth auth-timeout 60
[illegible]
Router#
*Feb 11 08:48:39.682: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation
attempt: Tamper-auth 0).

8PP2B# request consent-token accept-response tamper-auth
61+O/gAAAQYBAAQAAAUBAgAEAAAAAAMBYlNVOHNvRmlIUDFiUEp4OU5yTVEwUCtK
SkMrNUp3MnpNMWlJcC9ibEJjakQxcFJaWGxtNDNkWGJVYnZ2bVpiRFUNCjV2ckt3
eDV4ajEabnVtUURNTFdxeExLb0IwMHhkMkRRdEQyUWJ2TlR5L0V4V1JNRjdDQ0VT
YjRKREFrVnBaMGkNCm43ZHlyMWsrTGpGV1FaeGkvc2lnUVgyOHR4ZEx6VHVsckxk
b3pGK3FnRmZCeWNhR3lmU3VwT0ZKcFU2T0ZGVWANCllhY01ZWXZ3aTF0WUZKaE1n
d1BBTVkxbFE4b3JoSXVNVTU5S1RhZ0YxNmw0V0tBK3dEbVpHc2F0Sk5ubDIrL3gN
CjdndmljMFNCNXR2aXR2YVNyVTNtaVFnWkM3MnNLdHhMb3R5Zi9nNVVwcWVkUFJR
K21aVXhlUysyakdFS1pNbmoNCnIrNkpIQnpXZ05lMm05SUpnUGhTVHc9PQoBYk9O
NCtGSi95Ym1LeVpHRmNBY28xQjZlUVBrcSswY3lWU0lsZkgyVGw1dFNHM0NjWHk4
bnpCa0xIYTN2NGZJMjQNClZ5aE96MldTZDRBMUk1bHFVVmtyekI3aHJqRjJsaUQ1
anRQOU1XcEVaMkR3eVMxcmh0bmhHNG1HRFFiQmFXVlENCmJXbVBQUkFiQ2xobG1a
L2RDUTdhMkxIVXA0RDI0RTJPWmtsdGlXeVpnT3dBVHZQUndXVWxmTm9HSlNxN3U4
a0QNClZBM2pqTW5MdHJXRzFkTkhZemg4UjM3Uy82SDVXY1dJOWpZMGlkS2NqRDVC
TzUzK21xYTdLNVU2T3ppaE5FZFcNCjQvRlk1OStldWs2d0kyeDZTdWE1V2dZKy8w
UnIzL3B4RTJjTDg5NUVvejYwWlNnaFc4d25LYU1RMEM0cWFlc1kNCmNYanc3alZm
ekpZY0dkTkpXK280a0E9PQ==

% Consent token authorization success

Router#
*Feb 11 08:49:29.826: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success:
 Tamper-auth 0).
```

```
Router# request platform hardware tamper-detection event-mark
% Tamper-event marked successfully...terminating the tamper auth session
% Consent token authorization termination success

8PP2B#
*Feb 11 08:49:54.788: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication:
 Tamper-auth 0).
```

CHAPTER 28

Cisco Umbrella integration

The Cisco Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the Cisco 8100 Series Secure Routers. The security administrator configures policies on the Cisco Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN). Cisco 8100 Series Secure Routers acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Cisco Umbrella portal.

Prerequisites for Cisco Umbrella integration

Before you configure the Cisco Umbrella Integration feature on the Cisco 8100 Series Secure Routers, ensure that the following are met:

- The Cisco 8100 Series Secure Routers has a security K9 license to enable Cisco Umbrella Integration.
- Cisco Umbrella subscription license is available.
- The DNS traffic passed through the Cisco 8100 Series Secure Routers.
- Communication for device registration to the Cisco Umbrella server is through HTTPS. This requires a root certificate to be installed on the router. To download this certificate directly from a link instead of pasting it in, you can find the certificate here: https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt

Restrictions for Cisco Umbrella integration

- If an application or host uses IP address directly instead of DNS to query domain names, policy enforcement is not applied.
- When the client is connected to a web proxy, the DNS query does not pass through the Cisco device. In this case, the connector does not detect any DNS request and the connection to the web server bypasses any policy from the Cisco Umbrella portal.
- When the Cisco Umbrella Integration policy blocks a DNS query, the client is redirected to a Cisco Umbrella block page. HTTPS servers provide these block pages and the IP address range of these block pages is defined by the Cisco Umbrella portal.
- User authentication and identity is not supported in this release.
- The type A, AAAA, and TXT queries are the only records that are redirected. Other types of query bypasses the connector. Cisco Umbrella Connector maintains a list of IP address that is known for malicious traffic. When the Cisco Umbrella roaming client detects the destination of packets to those addresses, it forwards those addresses to Cisco Umbrella cloud for further inspection.
- Only the IPv4 address of the host is conveyed in the EDNS option.
- A maximum of 64 local domains can be configured, and the allowed domain name length is 100 characters.

Cloud-based security service using cisco Umbrella integration

The Cisco Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through Cisco 8100 Series Secure Routers. When a host initiates the traffic and sends a DNS query, the Cisco Umbrella Connector in Cisco 8100 Series Secure Routers intercepts and inspects the DNS query. If the DNS query is for a local domain, it forwards the query without changing the DNS packet to the DNS server in the enterprise network. If it is for an external domain, it adds an Extended DNS (EDNS) record to the query and sends it to Cisco Umbrella Resolver. An EDNS record includes the device identifier information, organization ID and client IP. Based on this information, Cisco Umbrella Cloud applies different policies to the DNS query.

Encrypting the DNS packet

The DNS packet sent from the Cisco 8100 Series Secure Routers to Cisco Umbrella Integration server must be encrypted if the EDNS information in the packet contains information such as user IDs, internal network IP addresses, and so on. When the DNS response is sent back from the DNS server, Cisco 8100 Series Secure Routers decrypts the packet and forwards it to the host.

You can encrypt DNS packets only when the DNScrypt feature is enabled on the Cisco 8100 Series Secure Routers.

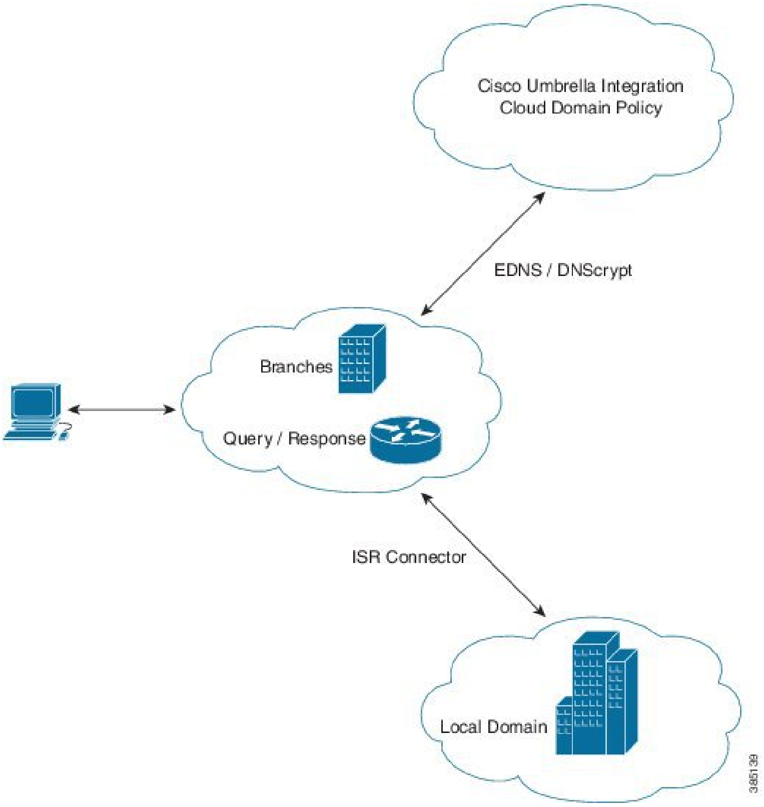
Cisco 8100 Series Secure Routers uses the following Anycast recursive Cisco Umbrella Integration servers:

- 208.67.222.222
- 208.67.220.220

- 2620:119:53::53
- 2620:119:35::35

The Figure 1 describes the Cisco Umbrella Integration topology.

Figure 4: Cisco Umbrella Integration Topology



Benefits of Cisco Umbrella integration

Cisco Umbrella integration provides security and policy enforcement at DNS level. It enables the administrator to split the DNS traffic and directly send some of the desired DNS traffic to a specific DNS server (DNS server located within the enterprise network). This helps the administrator to bypass the Cisco Umbrella integration.

How to configure Cisco Umbrella connector

Configure the Cisco Umbrella connector

To configure Cisco Umbrella connector, perform these steps:

SUMMARY STEPS

1. Get the API token from the Cisco Umbrella registration server.
2. Have the root certificate establish the HTTPS connection with the Cisco Umbrella registration server. Import the root certificate of DigiCert given below into the device using the **crypto pki trustpool import terminal** command.
3. Verify that the PEM import is successful. A message is displayed after importing the certificate.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Get the API token from the Cisco Umbrella registration server.	
Step 2	Have the root certificate establish the HTTPS connection with the Cisco Umbrella registration server. Import the root certificate of DigiCert given below into the device using the **crypto pki trustpool import terminal** command.	-----BEGIN CERTIFICATE----- MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3 d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83 nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f /ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0 /RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6 Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1 oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl 5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA 8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC 2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0 j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz -----END CERTIFICATE-----
Step 3	Verify that the PEM import is successful. A message is displayed after importing the certificate.	

Example

This is the sample configuration:

```
enable
configure terminal
parameter-map type umbrella global
 token AABBA59A0BDE1485C912AFE472952641001EEECC

exit
```

Register the Cisco Umbrella tag

1. Configure the umbrella parameter map as shown in the previous section.
2. Configure **umbrella out** on the WAN interface:

   ```
   interface gigabitEthernet 0/0/0
    umbrella out
   ```

3. Configure **umbrella in** on the LAN interface:

   ```
   interface vlan20
    umbrella in mydevice_tag
   ```

Note For Cisco Cisco 8100 Series Secure Routers, the length of the hostname and umbrella tag should not exceed 49 characters.

4. After you configure **umbrella in** with a tag using the **umbrella in mydevice_tag** command, the Cisco 8100 Series Secure Routers registers the tag to the Cisco Umbrella portal.
5. The Cisco 8100 Series Secure Routers initiates the registration process by resolving *api.opendns.com*. You need to have a name server (*ip name-server x.x.x.x*) and domain lookup (*ip domain-lookup*) configured on Cisco 8100 Series Secure Routers to successfully resolve the FQDN.

Note You should configure the **umbrella out** command before you configure **opendns in** command. Registration is successful only when the port 443 is in *open* state and allows the traffic to pass through the existing firewall.

Configure Cisco 8100 Series Secure Router as a pass-through server

You can identify the traffic to be bypassed using domain names. In the Cisco 8100 Series Secure Routers, you can define these domains in the form of regular expressions. If the DNS query that is intercepted by the Cisco 8100 Series Secure Routers matches one of the configured regular expressions, then the query is bypassed to the specified DNS server without redirecting to the Cisco Umbrella cloud. This sample configuration shows how to define a regex parameter-map with a desired domain name and regular expressions:

```
Device# configure terminal
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.fisco.com
Device(config)# pattern .*engineering.fisco.*

Attach the regex param-map with the umbrella global configuration as shown below:

Device(config)# parameter-map type umbrella global
Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF
Device(config-profile)# local-domain dns_bypass
```

Clear command

clear platform hardware qfp active feature umbrella datapath stats

The **clear platform hardware qfp active feature umbrella datapath stats** command clears the Umbrella connector statistics in datapath.

```
Device# clear platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats Cleared
```

Troubleshoot the Cisco Umbrella integration

Troubleshoot issues that are related to enabling Cisco Umbrella integration feature using these commands:

- **debug umbrella device-registration**
- **debug umbrella config**
- **debug umbrella dnscrypt**

Depending on the OS, run either of these two commands from the client device:

- The **nslookup -type=txt debug.umbrella.com** command from the command prompt of the Windows machine
- The **nslookup -type=txt debug.umbrella.com** command from the terminal window or shell of the Linux machine

```
nslookup -type=txt debug.opendns.com 192.0.2.1
Server:         192.0.2.2
Address:        192.0.2.3

Non-authoritative answer:
debug.opendns.com       text = "server r6.mum1"
debug.opendns.com       text = "device 010A826AAABB6C3D"
debug.opendns.com       text = "organization id 1892929"
debug.opendns.com       text = "remoteip 172.16.0.1"
debug.opendns.com       text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com       text = "originid 119211936"
debug.opendns.com       text = "orgid 1892929"
debug.opendns.com       text = "orgflags 3"
debug.opendns.com       text = "actype 0"
debug.opendns.com       text = "bundle 365396"
debug.opendns.com       text = "source 172.31.255.254:36914"
debug.opendns.com       text = "dnscrypt enabled (713156774457306E)"
```

When you deploy the Cisco Umbrella Integration feature:

- If you use the multiple EDNS options, DNS packets containing EDNS (DNSSEC) will not pass through the device. For assistance, contact Cisco Technical Support.
- If the WAN interface is down for more than 30 minutes, the device may reload with an exception. Disable the DNScrypt to stop this exception. For assistance, contact Cisco Technical Support .

Configuration examples

This example shows how to enable Cisco Umbrella integration on Cisco 8100 Series Secure Routers:

Deploy the Cisco Umbrella integration using Cisco prime CLI templates

You can use the Cisco Prime CLI templates to provision the Cisco Umbrella Integration deployment. The Cisco Prime CLI templates make provisioning Cisco Umbrella Integration deployment simple.

Note The Cisco Prime CLI templates is supported only on Cisco Prime version 3.1 or later.

To use the Cisco Prime CLI templates to provision the Cisco Umbrella Integration deployment, perform these steps:

Procedure

Step 1 Download the Cisco Prime templates corresponding to the Cisco IOS XE version running on your system.

Step 2 Unzip the file, if it is a zipped version.

Step 3 From Cisco Prime Web UI, choose **Configuration** > **Templates** > **Features and Technologies**, and then select **CLI Templates** (User Defined).

Step 4 Click **Import**.

Step 5 Select the folder where you want to import the templates and click Select Templates and choose the templates that you just downloaded.

Step 6 The following Cisco Umbrella Integration templates are available:

- Umbrella—Use this template to provision Umbrella Connector on Cisco 8100 Series Secure Routers.
- Umbrella Cleanup—Use this template to remove previously configured Umbrella Connector on Cisco 8100 Series Secure Routers.

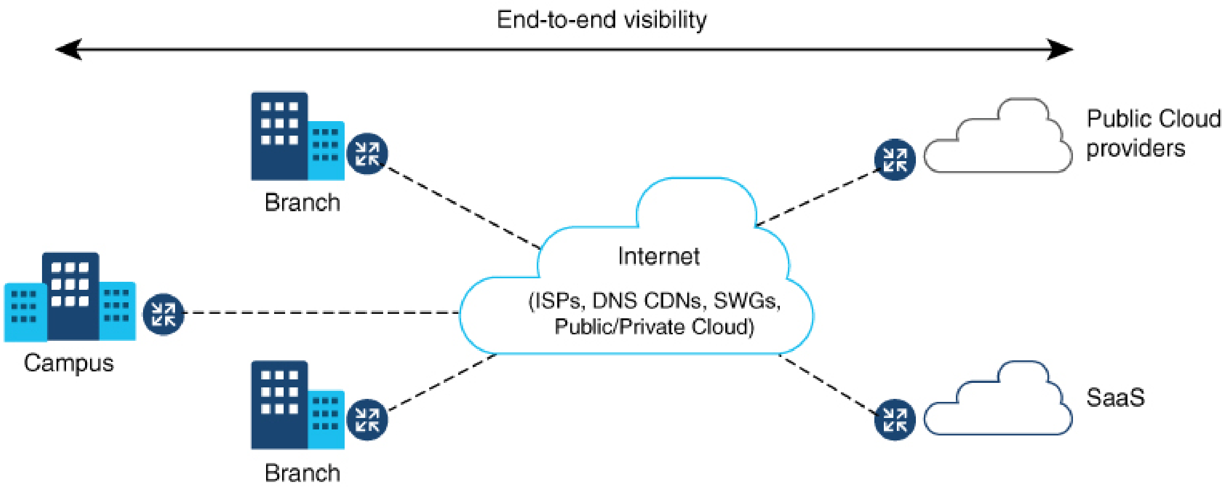
CHAPTER 29

Cisco ThousandEyes enterprise agent application hosting

Cisco ThousandEyes is a network intelligence platform that allows you to use its agents to run a variety of tests from its agents to monitor the network and application performance. This application enables you to view end-to-end paths across networks and services that impact your business. Cisco ThousandEyes application actively monitors the network traffic paths across internal, external, and internet networks in real time, and helps to analyse the network performance. Also, isco ThousandEyes application provides application availability insights that are enriched with routing and device data for a multidimensional view of digital experience.

From Cisco IOS XE Release 17.18.1a, you can use application-hosting capabilities to deploy the Cisco ThousandEyes Enterprise Agent as a container application on Cisco 8100 Series Secure Routers. This agent application runs as a docker image using Cisco IOx docker-type option. For more information on how to configure Cisco ThousandEyes in controller mode, see Cisco SD-WAN Systems and Interfaces Configuration Guide.

Figure 5: Network View through ThousandEyes Application



- Troubleshoot the Cisco ThousandEyes application, on page 309

Supported platforms and system requirements

The following table lists the supported platforms and system requirements.

Platforms	Bootflash	DRAM
Cisco 8100 Series Secure Routers		
C8151-G2	16GB (usable 13.1GB	8GB
C8161-G2	16GB (usable 13.1GB	8GB

Workflow to Install and Run the Cisco ThousandEyes Application

To install and run the Cisco ThousandEyes image on the device, perform these steps:

- Create a new account on the Cisco ThousandEyes portal.
- Download the Cisco ThousandEyes application package from the software downloads page and ensure to use the agent version 4.2.2.
- Copy the image on the device.
- Install and launch the image.
- Connect the agent to the controller.

Note For the supported platforms ordered with Cisco IOS XE 17.8.1 software, the Cisco ThousandEyes application package will be available on the bootflash of the device.

Workflow to host the Cisco ThousandEyes application

To install and launch the application, perform these steps:

Before you begin

Create a new account on the Cisco ThousandEyes portal and generate the token. The Cisco ThousandEyes agent application uses this token to authenticate and check into the correct Cisco ThousandEyes account. you see a message stating that your token is invalid and you want to troubleshoot the issue, see #unique_351.

Note If you configure the correct token and Domain Name Server (DNS) information, the device is discovered automatically.

Procedure

Step 1 Enable Cisco IOX application environment on the device.

- Use the following commands for non-SD-WAN (autonomous mode) images:

  ```
  config terminal
   iox
  end
  write
  ```

- Use the following commands for SD-WAN (controller mode) images:

```
config-transaction
iox
commit
```

Step 2 If the IOx command is accepted, wait for a few seconds and check whether the IOx process is up and running by using the **show iox** command. The output must display that the show IOxman process is running.

```
Device #show iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF) 1.11.0.0     : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Not Supported
Libvirtd 1.3.4                 : Running
```

Step 3 Ensure that the ThousandEyes application LXC tarball is available in the device *bootflash:*.

Step 4 Create a virtual port group interface to enable the traffic path to the Cisco ThousandEyes application:

```
interface VirtualPortGroup 0
          ip address 192.168.35.1 255.255.255.0
        exit
```

Step 5 Configure the app-hosting application with the generated token:

```
app-hosting appid te
          app-vnic gateway1 virtualportgroup 0 guest-interface 0
          guest-ipaddress 192.168.35.2 netmask 255.255.255.0
          app-default-gateway 192.168.35.1 guest-interface 0
          app-resource docker
                   prepend-pkg-opts  Required to get the default run-time options from package.yaml

                   run-opts 1 "--hostname thousandeyes"
             run-opts 2 "-e TEAGENT_ACCOUNT_TOKEN=<ThousandEyes token>"
        run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e TEAGENT_PROXY_LOCATION=proxy.something.other:80"

          name-server0 75.75.75.75  ISP’s DNS server
        end

app-hosting appid te
 app-resource docker
  prepend-pkg-opts
  run-opts 2 “--hostname
```

Note

You can use the proxy configuration only if the Cisco ThousandEyes agent does not have an internet access without a proxy. Also, the hostname is optional. If you do not provide the hostname during the installation, the device hostname is used as the Cisco ThousandEyes agent hostname. The device hostname is displayed on the Cisco ThousandEyes portal. The DNS name server information is optional. If the Cisco ThousandEyes agent uses a private IP address, ensure that you establish a connection to the device through NAT.

Step 6 Configure the **start** command to run the application automatically when the application is installed on the device using the **install** command:

```
app-hosting appid te
         start
```

Step 7 Convert the device to app-heavy mode and reload the device using the following commands:

```
Device(config)#platform resource app-heavy
Please reboot to activate this template

Device(config)#end
Device#wr mem
Building configuration...
[OK]
Device#

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

Step 8 Install the ThousandEyes application:

```
app-hosting install appid <appid> package [bootflash: | harddisk: | https:]
```

Select a location to install the ThousandEyes application from these options:

```
Device# app-hosting install appid te package ?
           bootflash:  Package path
           harddisk:   Package path
           https:      Package path
```

Step 9 Check if the application is up and running:

```
Device#show app-hosting list
 App id                                   State
---------------------------------------------------------
  te                                       RUNNING
```

Note

If any of these steps fail, use the **show logging** command and check the IOx error message. If the error message is about insufficient disk space, clean the storage media (bootflash or hard disk) to free up the space. Use the **show app-hosting resource** command to check the CPU and disk memory.

Download and copy the image to the device

To download and copy the image to bootflash, perform these steps:

Procedure

Step 1 Check if the Cisco ThousandEyes image is precopied to *bootflash:/<directory name>*.

Step 2 If the image is not available in the device directory, perform these steps:

a) If the device has a direct access to internet, use the *https:*. option in the **application install** command. This option downloads the image from the Cisco ThousandEyes software downloads page into *bootflash:/apps* and installs the application.

```
Device# app-hosting install appid <appid string> package [bootflash: | flash | http | https://
| ftp | ] URL to image location hosted on ThousandEyes portal

Device# app-hosting install appid te1000 package
https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar

Installing package
'https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar'
 for 'te1000'.

Use 'show app-hosting list' for progress.
*Jun 29 23:43:29.244: %IOSXE-6-PLATFORM: R0/0: IOx:  App verification successful
*Jun 29 23:45:00.449: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install succeeded: te1000
installed successfully Current state is DEPLOYED
*Jun 29 23:45:01.801: %IOSXE-6-PLATFORM: R0/0: IOx:  App verification successful
*Jun 29 23:45:51.054: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succeeded: te1000 started
 successfully Current state is RUNNING

Device#show app-hosting detail appid te1000  ( Details of Application)
App id                 : te1000
Owner                  : iox
State                  : RUNNING
Application
  Type                 : docker
  Name                 : ThousandEyes Enterprise Agent
  Version              : 4.0
  Author               : ThousandEyes <support@thousandeyes.com>
  Path                 : bootflash:thousandeyes-enterprise-agent-4.0-22.cisco.tar
Resource reservation
  Memory               : 500 MB
  Disk                 : 1 MB
  CPU                  : 1500 units
  CPU-percent          : 70 %
```

b) If the device has a proxy server, copy the image manually to *bootflash:/apps*.

c) Download the Cisco ThousandEyes application package from the software downloads page and ensure that you use the agent version 4.0.2.

d) Create an application directory in the *bootflash:* to copy the image:

```
Device# mkdir bootflash:apps
Create directory filename [apps]?
Created dir bootflash:/apps
```

e) Copy the Cisco ThousandEyes image to the *bootflash:apps* directory.

f) Validate the image using the **verify** command:

```
verify /md5 bootflash:apps/<file name>
```

Connect the Cisco ThousandEyes Agent with the controller

Before you begin

Ensure that you have an Internet connection before you connect the agent with the controller.

Procedure

After the Cisco ThousandEyes application is up and running, the agent (ThousandEyes-agent) process connects to the controller that is running on the cloud environment.

Note
If you have issues related to connectivity, the application logs the relevant error messages in the application-specific logs (*/var/logs*).

Modify the agent parameters

To modify the agent parameters, perform these actions:

Procedure

Step 1 Stop the application using the **app-hosting stop appid appid** command.

Step 2 Deactivate the application using the **app-hosting deactivate appid appid** command.

Step 3 Make the required changes to app-hosting configuration.

Step 4 Activate the application using the **app-hosting activate appid appid** command.

Step 5 Start the application using the **app-hosting start appid appid** command.

Uninstall the application

To uninstall the application, perform these steps:

Procedure

Step 1 Stop the application using the **app-hosting stop appid te** command.

Step 2 Check if the application is in active state using the **show app-hosting list** command.

Step 3 Deactivate the application using the **app-hosting deactivate appid te** command.

Step 4 Ensure that the application is not in active state. Use the **show app-hosting list** command to check status of the application.

Step 5 Uninstall the application using the **app-hosting uninstall appid te** command.

Step 6 After the uninstallation process is complete, use the **show app-hosting list** command to check if the application is uninstalled successfully.

Troubleshoot the Cisco ThousandEyes application

To troubleshoot the Cisco ThousandEyes application, perform these steps:

1. Connect to Cisco ThousandEyes agent application using the **app-hosting connect appid appid session /bin/bash** command.
2. Verify the configuration applied to the application at the following path */etc/te-agent.cfg*.
3. View the logs at the following path */var/log/agent/te-agent.log*. You can use these logs to troubleshoot the configuration.

Check the ThousandEyes application status

When the Cisco ThousandEyes application is in running state, it is registered on the ThousandEyes portal. If the application does not show up in a few minutes after the agent is in running state, check the following using the **app-hosting connect appid thousandeyes_enterprise_agent session** command:

```
Device#app-hosting connect appid thousandeyes_enterprise_agent session
Device# cat /var/log/agent/te-agent.log
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.AptPackageInterface] {} Initialized APT
 package interface
2021-02-04 08:59:29.642 INFO  [e4736a40] [te.agent.main] {} Agent version 1.103.0 starting.
  Max core size is 0 and max open files is 1024
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.db] {} Vacuuming database
2021-02-04 08:59:29.643 INFO  [e4736a40] [te.agent.db] {} Found version 0, expected version
 50
2021-02-04 08:59:29.672 INFO  [e4708700] [te.probe.ServerTaskExecutor] {} ProbeTaskExecutor
 started with 2 threads.
2021-02-04 08:59:29.673 INFO  [e2f05700] [te.probe.ProbeTaskExecutor.bandwidth] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO  [e2704700] [te.probe.ProbeTaskExecutor.realtime] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO  [e1f03700] [te.probe.ProbeTaskExecutor.throughput] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.agent.DnssecTaskProceessor] {} Agent is not
running bind
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
 session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
 session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
 session
2021-02-04 08:59:29.674 INFO  [e4736a40] [te.agent.main] {} Agent starting up
2021-02-04 08:59:29.675 INFO  [e4736a40] [te.agent.main] {} No agent id found, attempting
to obtain one
2021-02-04 08:59:29.675 INFO  [e4736a40] [te.agent.ClusterMasterAdapter] {} Attempting to
get agent id from sc1.thousandeyes.com
2021-02-04 08:59:29.679 ERROR [e4736a40] [te.agent.main] {} Error calling create_agent:
Curl error - Couldn't resolve host name
2021-02-04 08:59:29.680 INFO  [e4736a40] [te.agent.main] {} Sleeping for 30 seconds
Note :
```

Note Check the DNS server connection. If the Cisco ThousandEyes agent is assigned to a private IP address, check the NAT configuration.

CHAPTER 30

Small form-factor pluggables

Small Form-Factor Pluggables (SFPs) that are not Cisco certified are called third-party SFPs. Cisco approved means the SFPs have undergone rigorous testing with Cisco products and the SFPs are guaranteed to have 100% compatibility.

Note Cisco does not provide any kind of support for the third-party SFPs because they are not validated by Cisco.

Configuring third-party SFPs

Third-party SFPs are manufactured by companies that are not on the Cisco-approved Vendor List (AVL). Currently, Cisco 8100 Series Secure Routers support only Cisco-approved SFPs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**service unsupported-transceiver** **Example:** `Router(config)# service unsupported-transceiver`	Enables third-party SFP support.
Step 3	**interface type** *slot subslot port number* **Example:** `Router(config-if)# interface ethernet 0/3/0`	Selects an interface to configure.
Step 4	**media-type sfp** **Example:** `Router(config-if)#media-type sfp`	Changes media type to SFP.

	Command or Action	Purpose
Step 5	**speed** *value* **Example:** `Router# speed 100`	Configures the speed of the interface. **Note** For 100BASE SFPs, configure the speed to 100 Mbps only. Similarly, for 1000BASE SFPs, configure the speed to 1000 Mbps only.
Step 6	**shutdown** **Example:** `Router(config)# shutdown`	Disables the interface, changing its state from administratively UP to administratively DOWN.
Step 7	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface, changing its state from administratively DOWN to administratively UP.
Step 8	**exit** **Example:** `Router(config-if)#exit`	Exits the configuration mode and returns the global configuration mode.

Examples

This example shows how to configure a third-party SFP on Cisco 8100 Series Secure Routers:

```
Router# configure terminal
Router(config)# interface ethernet 0/3/0
Router(config-if)# service unsupported-transceiver
Router(config)# interface ethernet 0/3/0
Router(config-if)# media-type sfp
Router(config-if)# speed 100
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

CHAPTER 31

Online insertion and removal

Online insertion and removal (OIR) enables you to replace faulty modules without affecting system operation. There is only soft OIR,which is done via CLI.

OIR allows you to insert and remove hardware components, such as network modules, PIM, while the system is powered on and operational. This involves a process where the specific module needs to be shut down before physical removal, without shutting down the entire system.

Soft OIR procedures

The following describes the soft OIR procedures:

```
Router#hw-module subslot 0/0 start
*Sep 11 12:38:46.023: %IOSXE_OIR-6-SOFT_STARTSPA: SPA(C8161-2S) restarted in subslot 0/0
*Sep 11 12:38:51.365: %SPA_OIR-6-ONLINECARD: SPA (C8161-2S) online in subslot 0/0
```

```
Router#hw-module subslot 0/0 stop
Proceed with stop of module? [confirm]
Router#
*Sep 11 12:38:01.505: %SPA_OIR-6-OFFLINECARD: SPA (C8161-2S) offline in subslot 0/0
*Sep 11 12:38:01.505: %IOSXE_OIR-6-SOFT_STOPSPA: SPA(C8161-2S) stopped in subslot 0/0,
interfaces disabled
```

```
Router#hw-module subslot 0/0 reload
Proceed with reload of module? [confirm]
Router#
*Sep 11 12:40:18.301: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(C8161-2S) reloaded on subslot 0/0
*Sep 11 12:40:18.302: %SPA_OIR-6-OFFLINECARD: SPA (C8161-2S) offline in subslot 0/0
*Sep 11 12:40:29.127: %SPA_OIR-6-ONLINECARD: SPA (C8161-2S) online in subslot 0/0
```

Manage OIR for pluggable LTE modules

To replace a faulty pluggable module, or to swap a module when the system is in operation, use the following CLI:

hw-module subslot <*subslot*> **stop**

Wait for the module to power off and then remove the module. Insert another pluggable LTE module into the slot, which is automatically detected, powers-up, and is authenticated.

```
Router#hw-module subslot 0/2 stop
Proceed with stop of module? [confirm]
Router#
*Sep 11 12:38:01.505: %SPA_OIR-6-OFFLINECARD: SPA (C8161-2S) offline in subslot 0/2
*Sep 11 12:38:01.505: %IOSXE_OIR-6-SOFT_STOPSPA: SPA(C8161-2S) stopped in subslot 0/2,
interfaces disabled
```

CHAPTER 32

Security group tagging

Each security group in a Cisco TrustSec domain is assigned a unique 16 bit tag called the Security Group Tag (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is in turn propagated between network hops allowing any intermediary devices (switches, routers) to enforce polices based on the identity tag.

Cisco TrustSec-capable devices have built-in hardware capabilities than can send and receive packets with SGT embedded in the MAC (L3) layer. This feature is called Layer 3 (L3)-SGT Imposition. It allows ethernet interfaces on the device to be enabled for L3-SGT imposition so that the device can insert an SGT in the packet to be carried to its next hop ethernet neighbor. SGT-over-Ethernet is a method of hop-by-hop propagation of SGT embedded in clear-text (unencrypted) ethernet packets. The inline identity propagation is scalable, provides near line-rate performance and avoids control plane overhead.

The Cisco TrustSec with SGT Exchange Protocol V4 (SXPv4) feature supports Cisco TrustSec metadata-based L3-SGT. When a packet enters a Cisco TrustSec-enabled interface, the IP-SGT mapping database (with dynamic entries built by SXP and/or static entries built by configuration commands) is analyzed to learn the SGT corresponding to the source IP address of the packet, which is then inserted into the packet and carried throughout the network within the Cisco TrustSec header.

As the tag represents the group of the source, the tag is also referred to as the Source Group Tag (SGT). At the egress edge of the network, the group assigned to the packet's destination becomes known. At this point, access control can be applied. With Cisco TrustSec, access control policies are defined between the security groups and are referred to as Security Group Access Control Lists (SGACL). From the view of any given packet, SGACL is simply being sourced from a security group and destined for another security group.

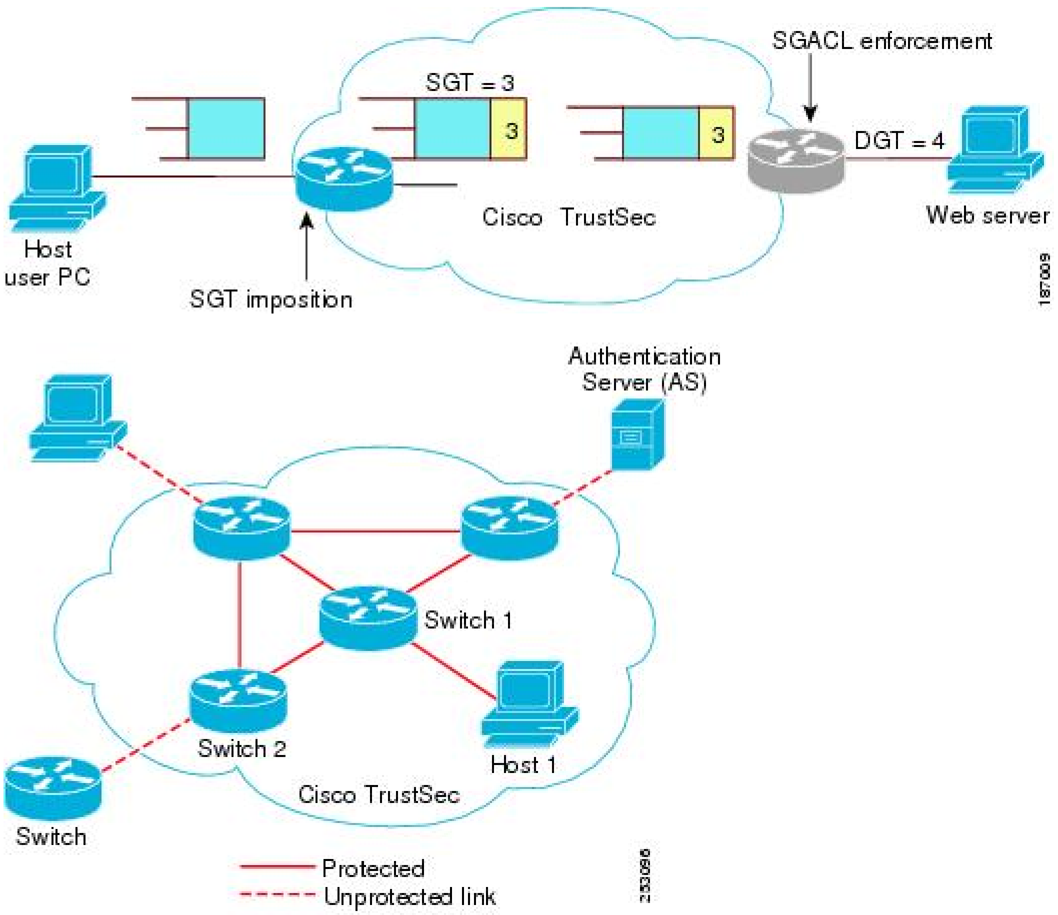
The SGT tag received in a packet from a trusted interface is propagated to the network, and is also be used for Identity firewall classification. When IPsec support is added, the received SGT tag is shared with IPSec for SGT tagging.

A network device at the ingress of Cisco TrustSec cloud needs to determine the SGT of the packet entering the Cisco TrustSec cloud so that it can tag the packet with that SGT when it forwards it into the Cisco TrustSec cloud. The SGT of a packet can be determined with these methods:

- SGT field on Cisco TrustSec header: If a packet is coming from a trusted peer device, it is assumed that the Cisco TrustSec header carries the correct SGT field. This situation applies to a network that is not the first network device in the Cisco TrustSec cloud for the packet.
- SGT lookup based on source IP address: In some cases, the administrator may manually configure a policy to decide the SGT of a packet based upon the source IP address. An IP address to SGT table can also be populated by the SXP protocol.

The following figures explains the topologies:

Figure 6: Cisco TrustSec Network



Limitations for security group tag

The following are the limitations of the Cisco TrustSec feature:

- SGT and SGACL enforcement on switchport are not supported.
- Dynamic SGT and SGACL for ipv6 is not supported.
- The **cts manual** command is not support on SVI interface, while they are supported on on-board L3 interface.

Configure security group tagging for dynamic SGT and SGACL

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aa new-model`	Enables AAA..
Step 4	**aaa authentication dot1x***{default | listname}* **group***group-name* **Example:** `Device(config)# aaa authentication dot1x default group ise`	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.
Step 5	**aaa authorization network***{default | listname}***group** *group-name* **Example:** `Device(config)# aaa authentication network default group coa-ise`	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.
Step 6	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 7	**dot1x system-auth-control** **Example:**	Globally enables 802.1X port-based authentication.

	Command or Action	Purpose
	`Device(config)# dot1x system-auth-control`	
Step 8	**aaa group server radius {radius | tacacs+}***group-name* **Example:** `Device(config)# aaa group server radius coa-ise`	Defines the AAA server group with a group name. Example: Device(config)# aaa group server radius group1 • All members of a group must be the same type, that is, RADIUS or TACACS+. This command puts the device in server group RADIUS configuration mode.
Step 9	**radius server** *server-name* **Example:** `Device(config)# radius server cts`	Specifies the name for the RADIUS server.
Step 10	**server** *ip-address***[auth-port***port-number***[acct-port***port-number* **Example:** `Device(config-sg-radius)# address ipv4 %{ise.ip} auth-port 1812 acct-port 1813`	Specifies the name for the RADIUS server.
Step 11	**pac key** *encyrption-key* **Example:** `Device(config-sg-radius)# pac key 0 cisco123`	Specifies the PAC encryption key (overrides the default). • The encryption-key can be **0** (specifies that an unencrypted keys follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.
Step 12	**policy-map type control subscriber***control-policy-name* **Example:** `Device(config)# policy-map type control subscriber simple_dot1x`	Defines a control policy for subscriber sessions.
Step 13	**event** *event-name***[match-all | match-first]** **Example:** `Device(config-event-control-policymap)# event session-started match-all`	Specifies the type of event that triggers actions in a control policy if conditions are met. • match-all is the default behavior.
Step 14	**priority-number class {control-class-name | always}[do-all | do-until-failure | do-until-success]** **Example:**	Associates a control class with one or more actions in a control policy. • A named control class must first be configured before specifying it with the control-class-name argument..

	Command or Action	Purpose
	`Device(config-event-control-policymap)# 10 class always do-until-failur`	• do-until-failure is the default behavior.

Step 15	**action-number authenticate using {dot1x | mab | webauth}aaa {authc-list authc-list-name | authz-list authz-list-name]} [merge] [parameter-map map-name] [priority priority-number] [replace | replace-all] [retries number {retry-time seconds}**
	Example:
	`Device(config-event-control-policymap)# 10 authenticate using dot1x`
		Optional) Initiates the authentication of a subscriber session using the specified method.

Step 16	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet0/1`	Enter the interface to be added to the VLAN.
Step 17	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 22`	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094
Step 18	**switchport access mode** **Example:** `Device(config-if)# switchport mode access`	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094
Step 19	**access-session closed** **Example:** `Device(config-if)# access-session closed`	The **access-session closed** command closes access to a port, preventing clients or devices from gaining network access before authentication is performed.

Step 20	**access-session port-control {auto | force-authorized | force-unauthorized }**
	Example:
	`Device(config-if)# access-session port-control auto`
		Sets the authorization state of a port.

	Command or Action	Purpose
Step 21	**policy-map type control subscriber***control-policy-name* **Example:** `Device(config-if)# policy-map type control subscriber simple_coa`	Defines a control policy for subscriber sessions.
Step 22	**dot1x pae [supplicant | authenticator | both]** **Example:** `Device(config-if)# dot1x pae authenticator`	[authenticator | Sets the Port Access Entity (PAE) type. • supplicant—The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator. • authenticator-—The interface acts only as an authenticator and does not respond to any messages meant for a supplicant. • both—The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages.

Step 23	**end**
	Example:
	`Device(config-if)# end`
		Exits Cisco TrustSec manual interface configuration mode and enters privileged EXEC mode.

Configure SGT tagging

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode. aaa authorization network cts-list group

	Command or Action	Purpose
Step 3	**aaa authorization network***{default | lcts-list}* **group***group-name* **Example:** `Device(config)# aaa authorization network cts-list group coa-ise`	Configures the device to use RADIUS authorization for all network-related service requests.
Step 4	**cts authorization list***mlist* **Example:** `Device(config)# cts authorization list cts-list`	Specifies a Cisco TrustSec AAA server group. Non-seed devices will obtain the server list from the authenticator.

Step 5	**cts sgt** *{sgt_number}*
	Example:
	`Device(config)# cts sgt 4`
		Enables Cisco TrustSec.

Step 6	**interface** *interface-id***VLAN***VLAN-id* **Example:** `Device(config)# interface Vlan32`	Enter the interface to be added to the VLAN.

Step 7	**cts role-based {sgt-map |sgt }**
	Example:
	`Device(config-if)# cts role-based sgt-map sgt`
		Enables Cisco TrustSec SGACL policy enforcement on routed interfaces..

Step 8	**cts role-based enforcement** **Example:** `Device(configif)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on the VLAN or VLAN list.
Step 9	**ip access-list role-based** *rbacl-name* **Example:** `Device(configif)# ip access-list role-based sgacl1`	Creates a Role-based ACL and enters Role-based ACL configuration mode.
Step 10	**access-list permit icmp** **Example:** `Device(config-rb-acl)# 10 permit icmp`	

	Command or Action	Purpose
Step 11	**ipv6 access-list role-based** *rbacl-name* **Example:** `Device(configif-rb-acl)# ipv6 access-list role-based v6_acl`	Creates a Role-based ACL and enters Role-based ACL configuration mode.
Step 12	**sequence 10 permit icmp echo-reply** *ip-address* **Example:** `Device(configif-rb-acl)# sequence 10 permit icmp echo-reply`	
Step 13	**exit** **Example:** `Device(configif-rb-acl)# exit`	
Step 14	**cts role-based monitor enable** *from {sgt_num} to {dgt_num}***[ipv4 | ipv6]** **Example:** `Device(configif)# cts role-based monitor enable from 4 to 32 sgacl1`	Enables monitor mode for IPv4/IPv6 Role Based Access Control List (RBACL) (Security cts role-based monitor permissions from {sgt_num} to {dgt_num} [ipv4 | ipv6] Step 4 Group Tag (SGT)- Destination Group Tag (DGT) pair).
Step 15	**cts role-based permissions** *from {sgt_num} to {dgt_num}***[ipv4 | ipv6]** **Example:** `Device(configif)# cts role-based permissions from 4 to 32 ipv6 v6_acl`	Enables role-base permissions mode for IPv4/IPv6 Role Based Access Control List (RBACL) (Security cts role-based monitor permissions from {sgt_num} to {dgt_num} [ipv4 | ipv6] Step 4 Group Tag (SGT)- Destination Group Tag (DGT) pair).

Step 16	**end**
	Example:
	`Device(config-if)# end`
		Exits Cisco TrustSec manual interface configuration mode and enters privileged EXEC mode.

Static security group tagging and security group ACL

This example shows how to enable an interface on the device for L3-SGT tagging or imposition and defines whether the interface is trusted for Cisco TrustSec.

```
Device# configure terminal
Device(config)# cts authorization list cts-list
Device(config)#cts sgt 4
Device(config)#interface Vlan32
Device(config-if)#ip address 192.168.32.2 255.255.255.0
Device(config-if)#ipv6 address 2001:DB8::1
Device(config-if)#cts role-based sgt-map sgt 32
Device(config-if)#cts role-based enforcement
Device(config-if)#ip access-list role-based sgacl1
Device(config-rb-acl#10 permit icmp
Device(config-rb-acl)#exit
Device(config)#ipv6 access-list role-based v6_acl
Device(config-rb-acl)#sequence 10 permit icmp echo-reply
Device(config-rb-acl)#cts role-based permissions from 4 to 32 sgacl1
Device(config-rb-acl)#cts role-based permissions from 4 to 32 ipv6 v6_acl
```

Dynamic security group tagging and security group ACL

This example shows how to enable an interface on the device for L3-SGT tagging or imposition and defines whether the interface is trusted for Cisco TrustSec.

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)#aaa authentication dot1x default group coa-ise
Device(config)#aaa authorization network default group coa-ise
Device(config)#dot1x system-auth-control
Device(config)#aaa group server radius coa-ise
Device(config)#server name coa
Device(config)#radius server coa
Device(config-sg-radius)#address ipv4 %{ise.ip} auth-port 1812 acct-port 1813
Device(config-sg-radius)#pac key 0 cisco123
Device(config-sg-radius)#exit
Device(config)#policy-map type control subscriber simple_coa
Device(config)#event session-started match-all
Device(config)#10 class always do-until-failure
Device(config)#10 authenticate using dot1x
Device(config)#interface gigabitethernet0/1
Device(config-if)#switchport access vlan 22
Device(config-if)#switchport mode access
Device(config-if)#access-session closed
Device(config-if)#access-session port-control auto
Device(config-if)#dot1x pae authenticator
Device(config-if)#service-policy type control subscriber simple_coa
```

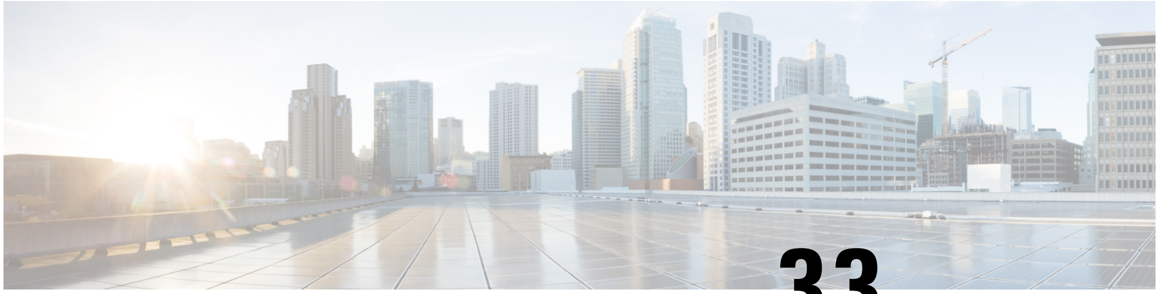
Note The Dynamic Security Group Tagging and Security Group ACL are configured on ISE server, after the 802.1x client is authenticated by ISE server. Subsequently, the corresponding SGT and SGACL will be downloaded from ISE and applied to the client.

Troubleshoot the security group tagging configuration

You can use the following commands to troubleshoot the Cisco TrustSec configuration:

- **debug cts all**

- **debug rbm bindings debug**
- **debug condition interface <intf-name>**
- deb cts authorization events verbose
- **debug radius**



CHAPTER 33

System messages

This chapter contains the following sections:

Information about process management

You can access system messages by logging in to the console through Telnet protocol and monitoring your system components remotely from any workstation that supports the Telnet protocol.

Starting and monitoring software is referred to as process management. The process management infrastructure for a router is platform independent, and error messages are consistent across platforms running on Cisco IOS XE. You do not have to be directly involved in process management, but we recommend that you read the system messages that refer to process failures and other issues.

How to find error message details

To show further details about a process management or a syslog error message, enter the error message into the Error Message Decoder tool at: https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi.

For example, enter the message `%PMAN-0-PROCESS_NOTIFICATION` into the tool to view an explanation of the error message and the recommended action to be taken.

The following are examples of the description and the recommended action displayed by the Error Message Decoder tool for some of the error messages.

Error Message: `%PMAN-0-PROCESS_NOTIFICATION : The process lifecycle notification component failed because [chars]`	
Explanation	**Recommended action**

The process lifecycle notification component failed, preventing proper detection of a process start and stop. This problem is likely the result of a software defect in the software subpackage.	Note the time of the message and investigate the kernel error message logs to learn more about the problem and see if it is correctable. If the problem cannot be corrected or the logs are not helpful, copy the error message exactly as it appears on the console along with the output of the **show tech-support** command and provide the gathered information to a Cisco technical support representative.

Error Message: `%PMAN-0-PROCFAILCRIT A critical process [chars] has failed (rc [dec])`

Explanation	**Recommended action**
A process important to the functioning of the router has failed.	Note the time of the message and investigate the error message logs to learn more about the problem. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAILOPT An optional process [chars] has failed (rc [dec])`

Explanation	**Recommended action**

A process that does not affect the forwarding of traffic has failed.	Note the time of the message and investigate the kernel error message logs to learn more about the problem. Although traffic will still be forwarded after receiving this message, certain functions on the router may be disabled because of this message and the error should be investigated. If the logs are not helpful or indicate a problem you cannot correct, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAIL The process [chars] has failed (rc [dec])`

Explanation	**Recommended action**
The process has failed as the result of an error.	This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAIL_IGNORE [chars] process exits and failures are being ignored due to debug settings. Normal router functionality will be affected. Critical router functions like RP switchover, router reload, FRU resets, etc. may not function properly.`

Explanation	Recommended action
A process failure is being ignored due to the user-configured debug settings.	If this behavior is desired and the debug settings are set according to a user's preference, no action is needed. If the appearance of this message is viewed as a problem, change the debug settings. The router is not expected to behave normally with this debug setting. Functionalities such as SSO switchover, router reloads, FRU resets, and so on will be affected. This setting should only be used in a debug scenario. It is not normal to run the router with this setting.

Error Message: `%PMAN-3-PROCHOLDDOWN The process [chars] has been helddown (rc [dec])`

Explanation	Recommended action
The process was restarted too many times with repeated failures and has been placed in the hold-down state.	This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-RELOAD_RP_SB_NOT_READY : Reloading: [chars]`

Explanation	Recommended action
The route processor is being reloaded because there is no ready standby instance.	Ensure that the reload is not due to an error condition.

Error Message: `%PMAN-3-RELOAD_RP : Reloading: [chars]`

Explanation	Recommended action

The RP is being reloaded.	Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-3-RELOAD_SYSTEM : Reloading: [chars]`

Explanation	Recommended action
The system is being reloaded.	Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-3-PROC_BAD_EXECUTABLE : Bad executable or permission problem with process [chars]`

Explanation	Recommended action
The executable file used for the process is bad or has permission problem.	Ensure that the named executable is replaced with the correct executable.

Error Message: `%PMAN-3-PROC_BAD_COMMAND:Non-existent executable or bad library used for process <process name>`

Explanation	Recommended action
The executable file used for the process is missing, or a dependent library is bad.	Ensure that the named executable is present and the dependent libraries are good.

Error Message: `%PMAN-3-PROC_EMPTY_EXEC_FILE : Empty executable used for process [chars]`

Explanation	Recommended action
The executable file used for the process is empty.	Ensure that the named executable is non-zero in size.

Error Message: `%PMAN-5-EXITACTION : Process manager is exiting: [chars]`

Explanation	Recommended action
The process manager is exiting.	Ensure that the process manager is not exiting due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-6-PROCSHUT : The process [chars] has shutdown`

Explanation	Recommended action
The process has gracefully shut down.	No user action is necessary. This message is provided for informational purposes only.

Error Message: `%PMAN-6-PROCSTART : The process [chars] has started`

Explanation	Recommended action

The process has launched and is operating properly.	No user action is necessary. This message is provided for informational purposes only.

Error Message: `%PMAN-6-PROCSTATELESS : The process [chars] is restarting stateless`

Explanation	Recommended action
The process has requested a stateless restart.	No user action is necessary. This message is provided for informational purposes only.

CHAPTER 34

Troubleshooting

This section describes the troubleshooting scenarios.

Before troubleshooting a software problem, you must connect a terminal or PC to the router by using the light-blue console port. With a connected terminal or PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface (Ethernet, ADSL, or telephone) by using Telnet. The Telnet option assumes that the interface is up and running.

Before contacting Cisco or your reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number
- Date you received the hardware
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem

show interfaces troubleshooting command

Use the **show interface** command to display the status of all physical ports (Ethernet, Fast Ethernet, and ATM) and logical interfaces on the router. Table 23: show interfaces Command Output Description , on page 332describes messages in the command output.

The following example shows how to view the status of Ethernet or Fast Ethernet Interfaces:

```
Router# show interfaces ethernet 0 **similar output for show interfaces fastethernet 0
command **
Ethernet0 is up, line protocol is up
Hardware is PQUICC Ethernet, address is 0000.Oc13.a4db
(bia0010.9181.1281)
Internet address is 192.0.2.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
 reliability 255/255., txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
```

The following example shows how to view the status of ATM Interfaces:

```
Router# show interfaces atm 0
ATM0 is up, line protocol is up
  Hardware is PQUICC_SAR (with Alcatel ADSL Module)
  Internet address is 192.0.2.1/8
  MTU 1500 bytes, sub MTU 1500, BW 640 Kbit, DLY 80 usec,
     reliability 40/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5, PVC mode
  10 maximum active VCs, 1 current VCCs
  VC idle disconnect time:300 seconds
  Last input 01:16:31, output 01:16:31, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:Per VC Queueing
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     512 packets input, 59780 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 1024 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     426 packets output, 46282 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to view the status of Dialer Interfaces:

```
Router# show interfaces dialer 1
Dialer 1 is up, line protocol is up
 Hardware is Dialer interface
 Internet address is 10.0.0.1/24
 MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec, reliability
  255/255. txload 1/255, rxload 1/255
 Encapsulation PPP, loopback not set
 Keepalive set (10 sec)
DTR is pulsed for 5 seconds on reset
LCP Closed
```

The table below describes possible command output for the **show interfaces** command.

Table 23: show interfaces Command Output Description

Output	Cause
For ATM Interfaces	The ATM line is up and operating correctly.
ATM 0 is up, line protocol is up	

Output	Cause
ATM 0 is down, line protocol is down	- The ATM interface has been disabled with the shutdown command. or - The ATM line is down, possibly because the ADSL cable is disconnected or because the wrong type of cable is connected to the ATM port.
ATM 0.*n* is up, line protocol is up	The specified ATM subinterface is up and operating correctly.
ATM 0.*n* is administratively down, line protocol is down	The specified ATM subinterface has been disabled with the shutdown command.
ATM 0.*n* is down, line protocol is down	The specified ATM subinterface is down, possibly because the ATM line has been disconnected (by the service provider).
For Ethernet/Fast Ethernet Interfaces	
Ethernet/Fast Ethernet *n* is up, line protocol is up	The specified Ethernet/Fast Ethernet interface is connected to the network and operating correctly.
Ethernet/Fast Ethernet *n* is up, line protocol is down	The specified Ethernet/Fast Ethernet interface has been correctly configured and enabled, but the Ethernet cable might be disconnected from the LAN.
Ethernet/Fast Ethernet *n* is administratively down, line protocol is down	The specified Ethernet/Fast Ethernet interface has been disabled with the **shutdown** command, and the interface is disconnected.
For Dialer Interfaces	
Dialer *n* is up, line protocol is up	The specified dialer interface is up and operating correctly.
Dialer *n* is down, line protocol is down	- This is a standard message and may not indicate anything is actually wrong with the configuration. or - If you are having problems with the specified dialer interface, this can mean it is not operating, possibly because the interface has been brought down with the **shutdown** command, or the ADSL cable is disconnected.

ATM troubleshooting commands

Use the following commands to troubleshoot your ATM interface:

ping atm interface command

Use the **ping atm interface** command to determine whether a particular PVC is in use. The PVC does not need to be configured on the router to use this command. The below example shows the use of this command to determine whether PVC 8/35 is in use.

The following example shows how to determine if a PVC is in use:

```
Router# ping atm interface atm 0 8 35 seg-loopback

Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/148/148 ms
```

This command sends five OAM F5 loopback packets to the DSLAM (segment OAM packets). If the PVC is configured at the DSLAM, the ping is successful.

To test whether the PVC is being used at the aggregator, enter the following command:

```
Router# ping atm interface atm 0 8 35 end-loopback

Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 400/401/404 ms
```

This command sends end-to-end OAM F5 packets, which are echoed back by the aggregator.

show atm interface command

To display ATM-specific information about an ATM interface, use the **show atm interface atm 0 command from** privileged EXEC mode.

The following example shows how to view information about an ATM interface:

```
Router# show atm interface atm 0
Interface ATM0:
AAL enabled: AAL5 , Maximum VCs:11, Current VCCs:0
Maximum Transmit Channels:0
Max. Datagram Size:1528
PLIM Type:INVALID - 640Kbps, Framing is INVALID,
DS3 lbo:short, TX clocking:LINE
0 input, 0 output, 0 IN fast, 0 OUT fast
Avail bw = 640
Config. is ACTIVE
```

The table below describes some of the fields shown in the command output.

Table 24: show atm interface command output description

Field	Description
ATM interface	Interface number.
AAL enabled	Type of AAL enabled.
Maximum VCs	Maximum number of virtual connections this interface supports.

Field	Description
Current VCCs	Number of active virtual channel connections (VCCs).
Maximum Transmit Channels	Maximum number of transmit channels.
Max Datagram Size	Configured maximum number of bytes in the largest datagram.
PLIM Type	Physical layer interface module (PLIM) type.

debug atm commands

Use the **debug** commands to troubleshoot configuration problems that you might be having on your network. The **debug** commands provide extensive, informative displays to help you interpret any possible problems.

Guidelines for using debug commands

Read the following guidelines before using debug commands to ensure appropriate results.

- All debug commands are entered in privileged EXEC mode.
- To view debugging messages on a console, enter the **logging console debug** command.
- Most **debug** commands take no arguments.
- To disable debugging, enter the **undebug all** command.
- To use **debug** commands during a Telnet session on your router, enter the **terminal monitor** command.

Caution Debugging is assigned a high priority in your router CPU process, and it can render your router unusable. For this reason, use **debug** commands only to troubleshoot specific problems. The best time to use debug commands is during periods of low network traffic so that other activity on the network is not adversely affected.

You can find additional information and documentation about the **debug** commands in the Cisco IOS Debug Command Reference.

debug atm errors command

Use the **debug atm errors** command to display ATM errors. The **no** form of this command disables debugging output.

The following example shows how to view the ATM errors:

```
Router# debug atm errors
ATM errors debugging is on
Router#
01:32:02:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:04:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:06:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:08:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:10:ATM(ATM0.2):VC(3) Bad SAP received 4500
```

debug atm events command

Use the **debug atm events** command to display events that occur on the ATM interface processor and to diagnose problems in an ATM network. This command provides an overall picture of the stability of the network. The **no** form of this command disables debugging output.

If the interface is successfully communicating with the Digital Subscriber Line Access Multiplexer (DSLAM) at the telephone company, the modem state is 0x10. If the interface is not communicating with the DSLAM, the modem state is 0x8. Note that the modem state does not transition to 0x10.

The following example shows how to view the ATM interface processor events-success:

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:02: DSL: 2: Modem state = 0x10
00:03:05: DSL: 3: Modem state = 0x10
00:03:07: DSL: 4: Modem state = 0x10
00:03:09: DSL: Received response: 0x24
00:03:09: DSL: Showtime!
00:03:09: DSL: Sent command 0x11
00:03:09: DSL: Received response: 0x61
00:03:09: DSL: Read firmware revision 0x1A04
00:03:09: DSL: Sent command 0x31
00:03:09: DSL: Received response: 0x12
00:03:09: DSL: operation mode 0x0001
00:03:09: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_SHOWTIME]
```

The following example shows how to view the ATM interface processor events—failure:

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
```

debug atm packet command

Use the **debug atm packet** command to display all process-level ATM packets for both outbound and inbound packets. The output reports information online when a packet is received or a transmission is attempted. The **no** form of this command disables debugging output.

Caution Because the **debug atm packet** command generates a significant amount of output for every packet processed, use it only when network traffic is low, so that other system activities are not adversely affected.

The command syntax is:

debug atm **packet** [**interface atm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

no debug atm **packet** [**interface atm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

where the keywords are defined as follows:

interface atm *number* (Optional) ATM interface or subinterface number.

vcd *vcd-number* (Optional) Number of the virtual circuit designator (VCD).

vc *vpi/vci number* VPI/VCI value of the ATM PVC.

The below example shows sample output for the **debug atm packet** command.

```
Router# debug atm packet
Router#
01:23:48:ATM0(O):
VCD:0x1 VPI:0x1 VCI:0x64 DM:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FF01 9F80 0E00 0010 0E00 0001 0800 A103 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
01:23:48:ATM0(I):
VCD:0x1 VPI:0x1 VCI:0x64 Type:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FE01 A080 0E00 0001 0E00 0010 0000 A903 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
```

The table below describes some of the fields shown in the **debug atm packet** command output.

Table 25: debug atm packet command output description

Field	Description
ATM0	Interface that is generating the packet.
(O)	Output packet. (I) would mean receive packet.
VCD: 0x*n*	Virtual circuit associated with this packet, where *n* is some value.
VPI: 0x*n*	Virtual path identifier for this packet, where *n* is some value.
DM: 0x*n*	Descriptor mode bits, where *n* is some value.

Field	Description
Length: *n*	Total length of the packet (in bytes) including the ATM headers.

System report

System reports or crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to crash. It is necessary to collect critical crash information quickly and reliably and bundle it in a way that it can be identified with a specific crash occurrence. System reports are generated and saved into the '/core' directory, either on harddisk: or flash: filesystem. The system does not generate reports in case of a reload.

In case of a system crash, the following details are collected:

1. Full process core
   - IOSd core file and IOS crashinfo file if there was an IOSd process crash
2. Tracelogs
3. System process information
4. Bootup logs
5. Certain types of /proc information

This report is generated before the router goes down to rommon/bootloader. The information is stored in separate files which are then archived and compressed into the tar.gz bundle. This makes it convenient to get a crash snapshot in one place, and can be then moved off the box for analysis.

Device hostname, the ID of the module that generated the system report and its creation timestamp are embedded in the file name:

```
<hostname>_<moduleID>-system-report_<timestamp>.tar.gz
```

Example:

Router1_RP_0-system-report_20210204-163559-UTC

A device with hostname Router1 experienced an unexpected reload of RP0 module and the system-report was generated on 4th February 2021 at 4:39:59 PM UTC.

```
├── bootflash/
│   └── pd_info/
│       ├── dmesg_output-20210204-163538-UTC.log
│       ├── filesystems-20210204-163538-UTC.log
│       ├── memaudit-20210204-163538-UTC.log
│       ├── proc_cpuinfo-20210204-163538-UTC.log
│       ├── proc_diskstats-20210204-163538-UTC.log
│       ├── proc_interrupts-20210204-163538-UTC.log
│       ├── proc_oom_stats-20210204-163538-UTC.log
│       ├── proc_softirqs-20210204-163538-UTC.log
│       ├── system_report_trigger.log
│       └── top_output-20210204-163538-UTC.log
├── harddisk/
│   ├── core/
│   │   └── Router1_RP_0_hman_17716_20210212-123836-UTC.core.gz
│   └── tracelogs/
├── tmp/
│   ├── fp/
│   │   └── trace/
│   ├── maroon_stats/
│   ├── rp/
│   │   └── trace/
│   └── Router1_RP_0-bootuplog-20210204-163559-UTC.log
└── var/
    └── log/
        └── audit/
            └── audit.log
```

Recovering a lost password

To recover a lost enable or lost enable-secret password, refer to the following sections:

1. Change the Configuration Register
2. Reset the Router
3. Reset the Password and Save your Changes (for lost enable secret passwords only)
4. Reset the Configuration Register Value.

Note Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

Tip See the “Hot Tips” section on Cisco.com for additional information on replacing enable secret passwords.

Change the configuration register

To change a configuration register, follow these steps:

SUMMARY STEPS

1. Connect an ASCII terminal or a PC running a terminal emulation program to the CONSOLE port on the Fthe router.
2. Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1 stop bit.
3. At the privileged EXEC prompt (r*outer_name* #), enter the **show version** command to display the existing configuration register value (shown in bold at the bottom of this output example):

4. Record the setting of the configuration register.
5. To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the **config-register 0x01** command from privileged EXEC mode.

DETAILED STEPS

Procedure

Step 1 Connect an ASCII terminal or a PC running a terminal emulation program to the CONSOLE port on the Fthe router.

Step 2 Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1 stop bit.

Step 3 At the privileged EXEC prompt (r*outer_name* #), enter the **show version** command to display the existing configuration register value (shown in bold at the bottom of this output example):

Example:

```
Router# show version
.
.
.



Suite License Information for Module:'esg'

--------------------------------------------------------------------------------
Suite                 Suite Current         Type           Suite Next reboot
--------------------------------------------------------------------------------
FoundationSuiteK9     None                  None           None
securityk9
appxk9


Technology Package License Information:

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
appxk9           None             None             None
securityk9       None             None             None
ipbase           ipbasek9         None             ipbasek9

cisco C1111-8PLTELAWN (1RU) processor with 1464345K/6147K bytes of memory.
Processor board ID FGL212392WT
8 Virtual Ethernet interfaces
11 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
6762495K bytes of flash memory at bootflash:.
7855044K bytes of USB flash at usb0:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x2100

Router#
```

Step 4 Record the setting of the configuration register.

Step 5 To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the **config-register 0x01** command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

Reset the Router

To reset the router, follow these steps:

SUMMARY STEPS

1. If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.
2. Press break. The terminal displays the following prompt:
3. Enter **confreg 0x142** to reset the configuration register:
4. Initialize the router by entering the **reset** command:
5. Enter **no** in response to the prompts until the following message is displayed:
6. Press **Return**. The following prompt appears:
7. Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:
8. Enter the **show startup-config** command to display an enable password in the configuration file:

DETAILED STEPS

Procedure

Step 1 If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.

Note
Some terminal keyboards have a key labeled *Break* . If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.

Step 2 Press break. The terminal displays the following prompt:

Example:

```
rommon 2>
```

Step 3 Enter **confreg 0x142** to reset the configuration register:

Example:

```
rommon 2> confreg 0x142
```

Step 4 Initialize the router by entering the **reset** command:

Example:

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

Example:

```
--- System Configuration Dialog ---
```

Step 5 Enter **no** in response to the prompts until the following message is displayed:

Example:

```
Press RETURN to get started!
```

Step 6 Press **Return**. The following prompt appears:

Example:

```
Router>
```

Step 7 Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:

Example:

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

Example:

```
Router#
```

Step 8 Enter the **show startup-config** command to display an enable password in the configuration file:

Example:

```
Router# show startup-config
```

What to do next

If you are recovering an enable password, do not perform the steps in the Reset the Password and Save Your Changes section. Instead, complete the password recovery process by performing the steps in the Reset the Configuration Register Value section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the Reset the Password and Save Your Changes section.

Reset the router

To reset the router, follow these steps:

SUMMARY STEPS

1. If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.
2. Press break. The terminal displays the following prompt:
3. Enter **confreg 0x142** to reset the configuration register:
4. Initialize the router by entering the **reset** command:
5. Enter **no** in response to the prompts until the following message is displayed:
6. Press **Return**. The following prompt appears:
7. Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:
8. Enter the **show startup-config** command to display an enable password in the configuration file:

DETAILED STEPS

Procedure

Step 1 If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.

Note
Some terminal keyboards have a key labeled *Break* . If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.

Step 2 Press break. The terminal displays the following prompt:

Example:

```
rommon 2>
```

Step 3 Enter **confreg 0x142** to reset the configuration register:

Example:

```
rommon 2> confreg 0x142
```

Step 4 Initialize the router by entering the **reset** command:

Example:

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

Example:

```
--- System Configuration Dialog ---
```

Step 5 Enter **no** in response to the prompts until the following message is displayed:

Example:

```
Press RETURN to get started!
```

Step 6 Press **Return**. The following prompt appears:

Example:

```
Router>
```

Step 7 Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:

Example:

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

Example:

```
Router#
```

Step 8 Enter the **show startup-config** command to display an enable password in the configuration file:

Example:

```
Router# show startup-config
```

What to do next

If you are recovering an enable password, do not perform the steps in the Reset the Password and Save Your Changes section. Instead, complete the password recovery process by performing the steps in the Reset the Configuration Register Value section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the Reset the Password and Save Your Changes section.

Reset the password and save your changes

To reset your password and save the changes, follow these steps:

SUMMARY STEPS

1. Enter the **configure terminal** command to enter global configuration mode:
2. Enter the **enable secret** command to reset the enable secret password in the router:
3. Enter **exit** to exit global configuration mode:
4. Save your configuration changes:

DETAILED STEPS

Procedure

Step 1 Enter the **configure terminal** command to enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter the **enable secret** command to reset the enable secret password in the router:

Example:

```
Router(config)# enable secret
password
```

Step 3 Enter **exit** to exit global configuration mode:

Example:

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

Step 4 Save your configuration changes:

Example:

```
Router# copy running-config startup-config
```

Reset the configuration register value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

SUMMARY STEPS

1. Enter the **configure terminal** command to enter global configuration mode:
2. Enter the **configure register** command and the original configuration register value that you recorded.
3. Enter **exit** to exit configuration mode:
4. Reboot the router, and enter the recovered password.

DETAILED STEPS

Procedure

Step 1 Enter the **configure terminal** command to enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter the **configure register** command and the original configuration register value that you recorded.

Example:

```
Router(config)# config-reg
value
```

Step 3 Enter **exit** to exit configuration mode:

Example:

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

Note
To return to the configuration being used before you recovered the lost enable password, do not save the configuration changes before rebooting the router.

Step 4 Reboot the router, and enter the recovered password.

INDEX