Cisco 8300 Series Secure Routers Software Configuration Guide

First Published: 2025-07-31

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

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 19

CHAPTER 20

APPENDIX A

Preface

This section briefly describes the objectives of this document and provides links to additional information on related products and services:

Objectives

This guide provides an overview of the Cisco 8300 Series Secure Routers and explains how to configure the various features on these routers.

Important Information on Features and Commands

For more information about Cisco IOS XE software, including features available on the router (described in configuration guides), see the Cisco IOS XE 17 Software Documentation set.

To verify support for specific features, use Cisco Feature Navigator. For more information about this, see Cisco Feature Navigator, on page 36.

To find reference information for a specific Cisco IOS XE command, see the Cisco IOS Master Command List, All Releases.

Related Documentation

- Hardware Installation Guide for the Cisco 8300 Series Secure Routers
- Release Notes for the Cisco 8300 Series Secure Routers

Commands

Cisco IOS XE commands are identical in look, feel, and usage to Cisco IOS commands on most platforms. To find reference information for a specific Cisco IOS XE command, see the Cisco IOS Master Command List, All Releases document.

Features

The router runs Cisco IOS XE software which is used on multiple platforms. To verify support for specific features, use the Cisco Feature Navigator tool. For more information, see Cisco Feature Navigator, on page 36.

Document Conventions

This documentation uses the following conventions:

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

Command syntax descriptions use the following conventions:

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

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

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

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS XE software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

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

Note Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

Obtaining Documentation and Submitting a Service Request

- 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 discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- 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 1

Overview

This chapter includes information about Cisco 8300 Series Secure Routers and describes the autonomous mode and controller mode. It contains the following sections:

Cisco 8300 Series Secure Routers

Cisco 8300 Series Secure Routers deliver secure networking simplified. Powered by the all-new secure networking processor and the unified Cisco secure networking platform, the Cisco 8300 Series Secure Routers deliver robust, platform-level security, advanced performance engineering thorough routing and SD-WAN, and on-premises, infrastructure-as-code, or cloud management flexibility that enables businesses to seamlessly scale and grow. Each class of secure routers is designed to deliver risk reduction, enhanced reliability, and future readiness.

Cisco 8300 Series Secure Routers are engineered for large branch locations and provide scalable, high-throughput connectivity with embedded platform-level security. With hardware-native assurance, post-quantum cryptography, and unified infrastructure as code, the Cisco 8300 Series enables large branches to support bandwidth-intensive applications and evolving threat landscapes with confidence.

This document is a summary of software functionality that is specific to the Cisco 8300 Series Secure Routers. You can access the Cisco IOS XE and Cisco IOS XE SD-WAN functionality through Autonomous and Controller execution modes, respectively. The Autonomous mode is the default mode for the device and includes the Cisco IOS XE functionality. To access Cisco IOS XE SD-WAN functionality switch to the Controller mode. You can use the existing Plug and Play workflow to determine the mode of the device.

You can use the universalk9 image to deploy both Cisco IOS XE SD-WAN and Cisco IOS XE on Cisco IOS XE platforms. The Cisco IOS XE 17.15.3 helps in seamless upgrades of both the SD-WAN and non-SDWAN features and deployments.

Switch between controller and autonomous modes using Cisco CLI

Use the **controller-mode** command in Privileged EXEC mode to switch between controller and autonomous modes.

The **controller-mode disable** command switches the device to autonomous mode.

```
Device# controller-mode disable
```

The **controller-mode enable** command switches the device to controller mode.

```
Device# controller-mode enable
```

Note When the device mode is switched from autonomous to controller, the startup configuration and the information in NVRAM (certificates), are erased. This action is same as the **write erase**.

When the device mode is switched from controller to autonomous, all Yang-based configuration is preserved and can be reused if you switch back to controller mode. If you want to switch the mode from controller to autonomous, ensue that the configuration on the device is set to auto-boot.

Switch between controller and autonomous modes using bootstrap configuration files

To switch modes, use the **controller-mode enable** command to switch from autonomous to controller mode and **controller-mode disable** command to switch from controller mode to autonomous mode. After the device boots up, the configuration present in the configuration file is applied.

After the device boots up in controller mode, the configuration present in the configuration file is applied.

For more information on how to use a single universalk9 image to deploy Cisco IOS XE SD-WAN and Cisco IOS XE functionality on all the supported devices, see the Install and Deploy Cisco IOS XE and Cisco IOS XE SD-WAN Functionality on Edge Platforms guide.

The Cisco 8300 Series Secure Routers models are:

- C8375-E-G2

Supported modules and features on Cisco 8300 Series Secure Routers

The table provides the supported modules and features on Cisco 8300 Series Secure Routers.

Table 1: Supported Modules and Features on Cisco 8300 Series Secure Routers

Features	C8375-E-G2
Service Plane Applications (UTD, AppQoE, and TcpOpt)	Yes
CPU Core	16 Core
CPU Memory	16G OR 32G
Backplane Support	10G

CHAPTER 2

Basic platform configuration

This section includes information about some basic platform configuration in Autonomous mode, and contains these sections:

Default configuration

When you boot up the device in autonomous mode, the device looks for a default file name-the PID of the device. For example, the Cisco 8300 Series Secure Routers look for a file named C8375-E-G2.cfg. The device looks for this file before finding the standard files-router-confg or the ciscortr.cfg.

The device looks for the C8375-E-G2.cfg file in the bootflash. If the file is not found in the bootflash, the device then looks for the standard files-router-confg and ciscortr.cfg. If none of the files are found, the device 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
Current configuration : 6621 bytes
!
! Last configuration change at 06:24:36 UTC Fri Feb 7 2025 by admin
!
version 17.15
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
!
hostname router
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no logging console
no aaa new-model
!
no ip domain lookup
!
!
!
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
!
subscriber templating
!
!
!
crypto pki trustpoint TP-self-signed-2220840378
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2220840378
 revocation-check none
 rsakeypair TP-self-signed-2220840378
 hash sha512
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha512
!
!
crypto pki certificate chain TP-self-signed-2220840378
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
  31312F30 2D060355 04030C26 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32323230 38343033 3738301E 170D3235 30313039 30393132
  31315A17 0D333530 31303930 39313231 315A3031 312F302D 06035504 030C2649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 32323038
  34303337 38308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 01008F2E D295CE5D 6DFDC027 4E7B4410 CD546B85 C14F0844 A4A08A47
  3621C3A8 4AF11F97 9489AD4B 00E1C57F AEAD53CE B08B684A 9018E660 8BCFABCE
  B1DCD79D 86E78BF4 DF278EF3 6C86539E 97217942 05C48B9A CBB057FB FFB2B225
  5A626C11 091376D8 A81E66B2 36ECE937 B44451F5 49D9CBB7 4D674A87 6532F4A7
  0A047D14 481A98A7 15574BE5 BFFFB4B1 F397C982 FECED50C 59605382 39B317F2
  3183C1B4 B83F62CF 3A9D6EE8 A1A34C61 86AD6B15 5474FD41 3151540D 5E387FC8
  B169558A E0DF905E F1187E78 AB59BD67 A38E97D9 79AAF825 E6D2B3A6 CF9239D6
  8B5F7E7D D4645263 F6006E12 FF69C3AF 7B769A2E F7F099AE 03A336EA 294A0423
  748E52EF 99330203 010001A3 53305130 1D060355 1D0E0416 04149FE1 4E1985FF
  AB1E7167 F6A67B35 5F3353E3 5B88301F 0603551D 23041830 1680149F E14E1985
  FFAB1E71 67F6A67B 355F3353 E35B8830 0F060355 1D130101 FF040530 030101FF
  300D0609 2A864886 F70D0101 0D050003 82010100 4F0CF81D C9E72E8B 2D5BC14A
  862DF349 42772862 46777631 3F402A07 DCD34CF7 5ED43C42 3C1839BB B68B0677
  C0C66B83 E97A0980 A54E5444 F0473525 C592D1C0 4D6C101A DA4BCDA0 D9C36EE1
CAD752AB AA37B084 A6C5F926 ED264D20 F6EF4940 F1103FAF 7122F428 0A5221F4
  DFB69177 BD7F5E67 DF662F1A F7888526 8867A938 C7F0B75B C34CDAFB 4AA2386B
  10ECE4FD 348D2028 E66E2FF1 FB6B0089 3D68FB71 E993D055 47CC0AA9 F08586E3
  319C0C26 86082E0A E4A9D4DA 99727580 6BEA0CF3 E530CD60 BBC627C5 16D8B483
  A96D47F4 B4746157 0DD2829E 7FC7E087 BE22D84B 09EDD9D7 A2D09897 247397B5
  AB6BBA3C E37BEDA0 053DE14A 748502E1 510197E4
        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 C8375-E-G2 sn FDO2833M01A
memory free low-watermark processor 63953
!
spanning-tree extend system-id
!
!
username admin privilege 15 password 0 admin
!
redundancy
 mode none
!
```

```
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface TwoGigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface TwoGigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface TwoGigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface TwoGigabitEthernet0/0/3
 no ip address
 shutdown
 negotiation auto
!
interface TenGigabitEthernet0/0/4
 no ip address
 shutdown
!
interface TenGigabitEthernet0/0/5
 no ip address
 shutdown
!
interface TwoGigabitEthernet0/1/0
!
interface TwoGigabitEthernet0/1/1
!
interface TwoGigabitEthernet0/1/2
!
interface TwoGigabitEthernet0/1/3
!
interface TwoGigabitEthernet0/1/4
!
interface TwoGigabitEthernet0/1/5
!
interface TwoGigabitEthernet0/1/6
 switchport
!
interface TwoGigabitEthernet0/1/7
 switchport
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 10.79.58.164 255.255.255.0
 negotiation auto
!
interface Vlan1
 no ip address
!
```

```
ip forward-protocol nd
ip tftp source-interface GigabitEthernet0
ip http server
ip http authentication local
ip http secure-server
ip route 64.104.134.61 255.255.255.255 10.79.58.1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.79.58.1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 64.104.134.61
ip ssh bulk-mode 131072
!
snmp-server community public RW
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 login local
 transport input telnet
line vty 5 10
 privilege level 15
 login local
 transport input telnet
line vty 11 14
 login
 transport input ssh
!
!
!
!
!
!
!
end
```

Configuring global parameters

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

SUMMARY STEPS

1. **configure terminal**
2. **hostname** *name*
3. **enable secret** *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 device 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 device.
Step 3	**enable secret** *password* **Example:** `Router(config)# enable secret cr1ny5ho`	Specifies an encrypted password to prevent unauthorized access to the device.
Step 4	**no ip domain-lookup** **Example:** `Router(config)# no ip domain-lookup`	Disables the device 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 TwoGigabitEthernet** *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 TwoGigabitEthernet** *slot/bay/port* **Example:** `Router(config)# interface TwoGigabitEthernet 0/0/1`	Enters the configuration mode for a Gigabit Ethernet interface on the device.
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 Gigabit Ethernet 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 Gigabit Ethernet 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 Gigabit Ethernet interface and changes its state from administratively down to administratively up.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the Gigabit Ethernet interface and returns to privileged EXEC 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 10.108.1.1 255.255.255.0`	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.

Example

Verifying Loopback Interface Configuration

This configuration example shows the loopback interface configured on the Gigabit Ethernet interface with an IP address of 203.0.113.1/32, 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 203.0.113.1 255.255.255.255 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
```

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

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 203.0.113.1/32
  MTU 1514 bytes, BW 8000000 Kbit/sec, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (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 output buffer failures, 0 output buffers swapped out
```

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

```
Router# ping  203.0.113.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Configuring module interfaces

For detailed information about configuring service modules, see "Service Modules" in the "Service Module Management" section of the Cisco Service Module Configuration Guide.

Dynamic allocation of cores

Dynamic core allocations on the Cisco 8300 Series Secure Routers provide flexibility for users to leverage the CPU cores for different services and/or CEF/IPSec performances. The Cisco 8300 Series Secure Routers are equipped with a minimum of 16 CPU cores and have the flexibility to allocate cores into the service plane from the data plane. The core allocation is based on the customer configuration of the different services available on these platforms.

From Cisco IOS XE Release 17.15.3 onwards, you can use the **platform resource { service-plane-heavy | data-plane-heavy }** command to adjust the cores across service plane and data plane.

```
Router(config)# platform resource { service-plane-heavy | data-plane-heavy }
```

Following are the list of Cisco 8300 Series Secure Routers that support changing the core allocations dynamically:

- C8375-E-G2

Show command output for C8375-E-G2

This show command output shows the CPU cores allocaton for the data plane for C8375-E-G2:

Note By default, when a device boots up, the mode is service-plane-heavy.

```
Router# show platform software cpu alloc

CPU alloc information:
  Control plane cpu alloc: 0
  Data plane cpu alloc: 0-15
  Service plane cpu alloc: 0
  Slow control plane cpu alloc:
  Template used: CLI-data_plane_heavy
```

Note In the example, the maximum data plane core allocation is 15.

This show command output shows the CPU cores allocaton for the service plane for C8375-E-G2:

```
Router# show platform software cpu alloc
CPU alloc information:
  Control plane cpu alloc: 0
  Data plane cpu alloc: 0,7-15
  Service plane cpu alloc: 1-6
  Slow control plane cpu alloc:
 Template used: default-service_plane_heavy
```

The show command output shows the PPE status for C8375-E-G2:

```
Router# show platform hardware qfp active datapath infrastructure sw-cio

Credits Usage:

                                                              ID      Port  Wght  Global
WRKR0  WRKR1  WRKR2  WRKR3  WRKR4  WRKR5  WRKR12  WRKR13  WRKR14  Total
1      rcl0     4:   6080     0      0      0      0      0      0       0       0      64
   6144
1      rcl0     8:   6080     0      0      0      0      0      0       0       0      64
   6144
2       ipc     1:      0     0      0      0      0      0      0       0       0       0
      0
3 vxe_punti     1:    480     0      0      0      0      0      0       0       0      32
    512
4      vpg0     1:   1952     0      0      0      0      0      0       0       0      96
   2048
5      vpg1     1:   1952     0      0      0      0      0      0       0       0      96
   2048
6     vpg10     1:   1952     0      0      0      0      0      0       0       0      96
   2048
7      fpe0    LO:   1024     -      -      -      -      -      -       -       -       -
   1024
7      fpe0    HI:   1024     -      -      -      -      -      -       -       -       -
   1024
8      fpe1    LO:   1024     -      -      -      -      -      -       -       -       -
   1024
8      fpe1    HI:   1024     -      -      -      -      -      -       -       -       -
   1024
9      fpe2    LO:   1024     -      -      -      -      -      -       -       -       -
   1024
9      fpe2    HI:   1024     -      -      -      -      -      -       -       -       -
   1024
10      fpe3    LO:   1024     -      -      -      -      -      -       -       -
```

```
-   1024
10      fpe3    HI:   1024     -      -      -      -      -      -       -       -
-   1024
11      fpe4    LO:   1024     -      -      -      -      -      -       -       -
-   1024
11      fpe4    HI:   1024     -      -      -      -      -      -       -       -
-   1024
12      fpe5    LO:   1024     -      -      -      -      -      -       -       -
-   1024
12      fpe5    HI:   1024     -      -      -      -      -      -       -       -
-   1024
13       bp0    LO:   1024     -      -      -      -      -      -       -       -
-   1024
13       bp0    HI:   1024     -      -      -      -      -      -       -       -
-   1024
13       bp0    HI:   1024     -      -      -      -      -      -       -       -
-   1024
14     bp0_2    LO:   1024     -      -      -      -      -      -       -       -
-   1024
15     bp0_3    LO:   1024     -      -      -      -      -      -       -       -
-   1024
16    memif0   100:   5856     0      0      0      0      0      0       0       0    288
   6144
Core Utilization over preceding 372325.1424 seconds
 ---------------------------------------------------
ID:       0       1       2       3       4       5      12      13      14
% PP:    0.47    0.14    0.14    0.16    0.16    0.15    0.00    0.00    0.00
% RX:    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.74
% TM:    0.00    0.00    0.00    0.00    0.00    0.00    0.90    0.89    0.00
% IDLE:   99.53   99.86   99.86   99.84   99.84   99.85   99.10   99.11   99.26
```

Enabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is enabled by default on the router.

For more information on using CDP, see Cisco Discovery Protocol Configuration Guide.

Configuring command-line access

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

Procedure

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 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.

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

These configurations show 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 device. 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.

Procedure

Step 1 (Option 1) **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}

Example:

```
Router(config)# ip route 192.0.2.8 255.255.0.0 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:DB8:3000:1
```

Specifies a static route for the IP packets.

Step 3 **end**

Example:

```
Router(config)# end
```

Exits global configuration mode and enters privileged EXEC mode.

Verifying Configuration

In this configuration example, the static route sends out all IP packets with a destination IP address of 192.0.2.8 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 interface.

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 192.0.2.8 255.255.255.0 10.10.10.2
```

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 this example:

```
Router# show ip route
Codes: L - local, 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 10.0.10.1 to network 192.0.2.6

S*    192.0.2.6/0 [254/0] via 10.0.10.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0/0
L        10.0.10.13/32 is directly connected, GigabitEthernet0/0/0
C        10.108.1.0/24 is directly connected, Loopback0
L        10.108.1.1/32 is directly connected, Loopback0
```

When you use an IPv6 address, you should see verification output similar to this example:

```
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 devices in the network.

A device 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, on page 17
- Configuring Enhanced Interior Gateway Routing Protocol, on page 21

Configuring Routing Information Protocol

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

Procedure

Step 1 **router rip**

Example:

```
Router(config)# router rip
```

Enters router configuration mode, and enables RIP on the router.

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 192.0.2.8
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.

Example

Verifying Configuration

To see this configuration, use the **show running-config** command from privileged EXEC mode.

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

Current configuration : 6504 bytes
!
! Last configuration change at 05:04:58 UTC Mon Jul 6 2020
!
version 17.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform hardware throughput crypto 1G
!
hostname Router
!
boot-start-marker
boot system bootflash:c8000be-universalk9.17.03.01prd8.SPA.bin
boot-end-marker
!
!
!
no aaa new-model
!
login on-success log

!
subscriber templating
!
!
multilink bundle-name authenticated
no device-tracking logging theft
```

```
!
crypto pki trustpoint TP-self-signed-2347094934
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2347094934
 revocation-check none
 rsakeypair TP-self-signed-2347094934
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
!

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

!
!
license feature hseck9
license udi pid C8300-1N1S-6T sn FDO2320A0CF

diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
redundancy
 mode none

!
interface GigabitEthernet0/0/0
 ip dhcp client client-id ascii FDO2320A0CF
 ip address dhcp
 negotiation auto
!
interface GigabitEthernet0/0/1
```

```
 no ip address
 negotiation auto
!
!
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/0
ip forward-protocol nd

!
!
!
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

!
!
dspfarm profile 7 conference security
 shutdown

!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
 transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http

!
!
end
```

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 this 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    192.0.2.3/8 [120/1] via 192.0.2.2, 00:00:02, Ethernet0/0/0
```

Configuring Enhanced Interior Gateway Routing Protocol

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

Procedure

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 192.0.2.8
Router(config)# network 10.10.12.15
```

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.

Verifying the Configuration

The following configuration example shows the EIGRP routing protocol enabled in IP networks 192.0.2.8 and 10.10.12.15. 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 192.0.2.8
```

```
  network 10.10.12.15
!
.
.
.
```

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 this 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
D     192.0.2.3/8 [90/409600] via 192.0.2.2, 00:00:02, Ethernet0/0
```

CHAPTER 3

Using Cisco IOS XE Software

This chapter describes the basics of using the Cisco IOS XE software in autonomous mode and includes the following section:

Cisco IOS XE software

Before you begin

Use the console (CON) port to access the command-line interface (CLI) directly or when using Telnet.

This sections describes the main methods of accessing the device:

Procedure

Step 1 Access the CLI using a directly-connected console, on page 23

Step 2 Use SSH to access console, on page 24

Step 3 Access the CLI from a remote console using Telnet, on page 25

Step 4 Access the CLI from a USB serial console port, on page 27

Access 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.

These 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).

Using 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 Cisco 8300 Series Secure Routers.

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

```
Router# quit
```

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.
```

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

Step 2 Configure the DNS domain of the device:

```
Router(config)# ip domain name cisco.com
```

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

```
Router(config)#  crypto key generate rsa
The name for the keys will be: Router.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)
Router(config)#
```

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

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

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

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

Step 6 Verify remote connection to the device using SSH.

Access the CLI from a remote console using Telnet

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

- Prepare to connect to the device console using Telnet, on page 25
- Telnet to access a console interface, on page 26

Prepare to connect to the device console using Telnet

To access the device remotely using Telnet from a TCP/IP network, configure the device 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 add a line password to the vty, 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 device, you must have a valid hostname for the device or have an IP address configured on the device. For more information about the requirements for connecting to the device using Telnet, information about customizing your Telnet services, and using Telnet key sequences, see the Cisco IOS Configuration Fundamentals Configuration Guide.

Telnet to access a console interface

Procedure

Step 1 From your terminal or PC, enter one of these commands:

- **connect host** [*port*] [*keyword*]
- **telnet host** [*port*] [*keyword*]

Here, *host* is the device hostname or IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information about these commands, see the Cisco IOS Terminal Services Command Reference document.

Note
If you are using an access server, specify a valid port number, such as **telnet 198.51.100.2 2004**, in addition to the hostname or IP address.

This example shows how to use the **telnet** command to connect to a device named **router**:

```
unix_host% telnet router
Trying 198.51.100.2...
Connected to 198.51.100.2.
Escape character is '^]'.
unix_host% connect
```

Step 2 Enter your login password:

```
User Access Verification
Password: mypassword
```

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

Step 3 From user EXEC mode, enter the **enable** command:

```
Router> enable
```

Step 4 At the password prompt, enter your system password:

```
Password: enablepass
```

Step 5 When the **enable** password is accepted, the privileged EXEC mode prompt is displayed:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the Telnet session, use the **exit** or **logout** command.

```
Router# logout
```

Access the CLI from a USB serial console port

The router provides an additional mechanism for configuring the system: a type B miniport USB serial console that supports remote administration of the router using a type B USB-compliant cable. See the “Connecting to a Console Terminal or Modem” section in the Hardware Installation Guide for Cisco 8300 Series Secure Routers.

Use keyboard shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

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

Table 2: 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.
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 table lists the history substitution commands.

Table 3: 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.

Understand command modes

The command modes available in Cisco IOS XE are the same as those available in traditional Cisco IOS. This is supported only on the autonomous mode. Use the CLI to access Cisco IOS XE software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS XE software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

The table 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 4: 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.

Command Mode	Access Method	Prompt	Exit Method
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.
Diagnostic	The device 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 device 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 device 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 device rebooted to get out of diagnostic mode. If the device is in diagnostic mode because of a transport-map configuration, access the device 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.

Understand diagnostic mode

The device boots up or accesses diagnostic mode in these 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 device, and the device 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 device, 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 device, a module, or possibly other hardware components.
- Transfer files into or off of the device using remote access methods such as FTP, TFTP, and SCP.

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous devices, 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 device when the device 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 these 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.

Command	Purpose
`?`	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: example

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 table shows examples of using the question mark (**?**) to assist you in entering commands.

Table 5: 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)#`

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

```
Router(config)# interface GigabitEthernet ?
  <0-1>  GigabitEthernet interface number

Router(config)# interface GigabitEthernet 0/?
  <0-5>  Port Adapter number

Router (config)# interface GigabitEthernet 0/0/?

  <0-63>  GigabitEthernet interface number

Router (config)# interface GigabitEthernet0/0/1?
.  <0-5>
Router(config-if)#
```

</td><td>

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)#`

</td></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
  logging    Configure logging for interface
  mls        mls router sub/interface commands
  mpoa       MPOA interface configuration
commands
  mtu        Set the interface MTU
  no         Negate a command or set its
defaults
  ntp        Configure NTP
  .
  .
  .
Router(config-if)#
```

</td><td>

Enter **?** 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>
<tr><td>

```
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
  cgmp           Enable/disable CGMP
  dvmrp          DVMRP interface commands
  hello-interval Configures IP-EIGRP hello
interval
  hold-time      Configures IP-EIGRP hold time
  .
  .
  .
Router(config-if)# ip
```

</td><td>

Enter the command that you want to configure for the interface. This example uses the **ip** command.

Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

</td></tr>
</table>

Command	Comment

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

`Router(config-if)# ip address 198.51.100.5 ?`
`  A.B.C.D            IP subnet mask`
`Router(config-if)#` **`ip address 198.51.100.5`**
	Enter the keyword or argument that you want to use. This example uses the 198.51.100.5 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.

`Router(config-if)#` **`ip address 198.51.100.5 255.255.255.0 ?`**
`  secondary          Make this IP address a secondary address`
`  <cr>`
`Router(config-if)#` **`ip address 198.51.100.5 255.255.255.0`**
	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 198.51.100.5 255.255.255.0`**
`Router(config-if)#`
	Press **Enter** to complete the command.

How to 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.

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:

Example output for C8375-E-G2:

```
Router# show interface | include protocol
TwoGigabitEthernet0/0/0 is down, line protocol is down
0 unknown protocol drops
TwoGigabitEthernet0/0/1 is up, line protocol is up
0 unknown protocol drops
```

```
TwoGigabitEthernet0/0/2 is down, line protocol is down
0 unknown protocol drops
TwoGigabitEthernet0/0/3 is up, line protocol is up
0 unknown protocol drops
TenGigabitEthernet0/0/4 is up, line protocol is up
0 unknown protocol drops
TenGigabitEthernet0/0/5 is up, line protocol is up
 0 unknown protocol drops
TwoGigabitEthernet0/1/0 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
TwoGigabitEthernet0/1/1 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/2 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/3 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/4 is down, line protocol is down (notconnect)
0 unknown protocol drops
TwoGigabitEthernet0/1/5 is down, line protocol is down (notconnect)
 0 unknown protocol drops
TwoGigabitEthernet0/1/6 is up, line protocol is up
0 unknown protocol drops
TwoGigabitEthernet0/1/7 is up, line protocol is up
0 unknown protocol drops
TwoGigabitEthernet0/1/7.10 is up, line protocol is up
GigabitEthernet0 is up, line protocol is up
0 unknown protocol drops
Tunnel0 is up, line protocol is up
Tunnel protocol/transport multi-GRE/IP
0 unknown protocol drops
VirtualPortGroup0 is up, line protocol is up
0 unknown protocol drops
VirtualPortGroup1 is up, line protocol is up
0 unknown protocol drops
VirtualPortGroup10 is up, line protocol is up
0 unknown protocol drops
Vlan1 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
```

Power off a device

The device can be safely turned off at any time by moving the device'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 device. The copy running-config startup-config command saves the configuration in NVRAM and after the device is powered up, the device initializes with the saved configuration.

Find support information for platforms and Cisco software images

The Cisco IOS XE software is packaged in feature sets consisting of software images that support specific platforms. The group of feature sets that are available for a specific platform depends on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or see the Release Notes for Cisco 8300 Series Secure Routers.

Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator is a tool that enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To use the navigator tool, an account on Cisco.com is not required.

Software Advisor

Cisco maintains the Software Advisor tool to see if a feature is supported in a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your device. You must be a registered user on Cisco.com to access this tool.

Software Release Notes

See the Release Notes document for Cisco 8300 Series Secure Routers for information about:

- Memory recommendations
- Open and resolved severity 1 and 2 caveats

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. For cumulative feature information, refer to the Cisco Feature Navigator at: https://cfnng.cisco.com/.

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.

- Change the CLI session timeout, on page 36
- Lock a CLI session, on page 37

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
```

CHAPTER 4

Managing the device Using Web User Interface

The Web User Interface (Web UI) is an embedded GUI-based device-management tool that provides the ability to provision the device, to simplify device deployment and manageability, and to enhance the user experience. It comes with the default image, so there is no need to enable anything or install any license on the device. You can use WebUI to build configurations, and to monitor and troubleshoot the device without having CLI expertise. This chapter includes the these sections:

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 Web UI, you need to have the basic configuration on the device.

Procedure

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

Step 2 After the device initial configuration wizard appears, enter **No** to get into the device prompt when the following system message appears on the router.

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

Step 3 From the configuration mode, enter the following configuration parameters.

```
!
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 4 Connect the PC to the router using an Ethernet cable to the gig 0/0/1 interface.

Step 5 Set up your PC as a DHCP client to obtain the IP address of the router automatically.

Step 6 Launch the browser and enter the device IP address in your browser's address line. For a secure connection, type https://192.168.1.1/#/dayZeroRouting. For a less secure connection, enter http://192.168.1.1/#/dayZeroRouting.

Step 7 Enter the default username (admin) and the password as default.

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.

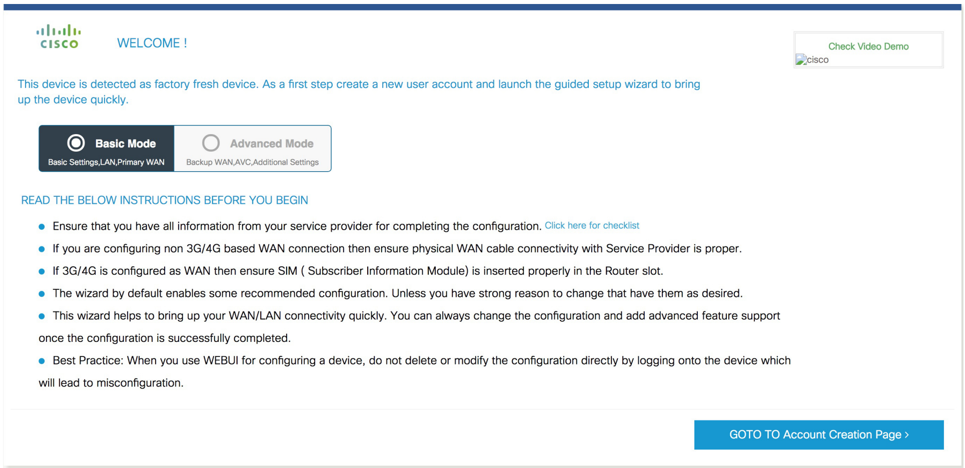
Step 3 Click **Create and Launch Wizard**.

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**.



WELCOME !

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.

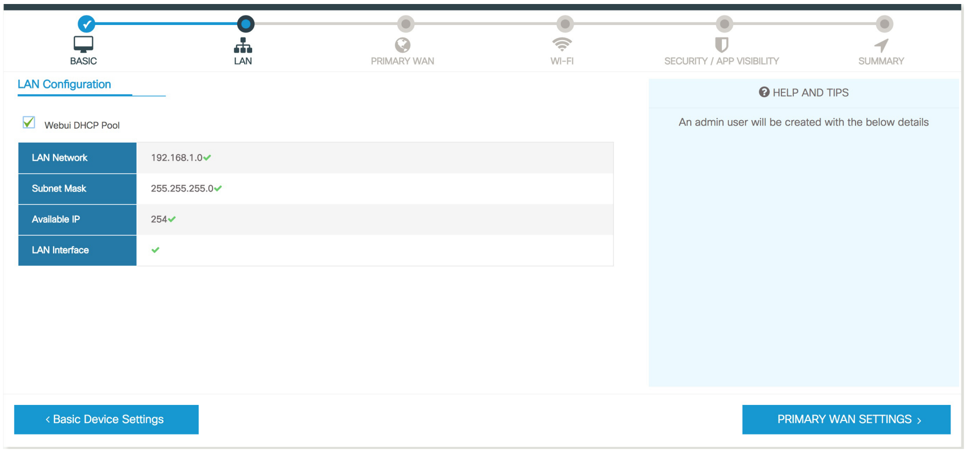
b) If you choose the Create and Associate Access VLAN option, specify the following:

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**.



LAN Configuration

☑ Webui DHCP Pool

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

HELP AND TIPS

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.

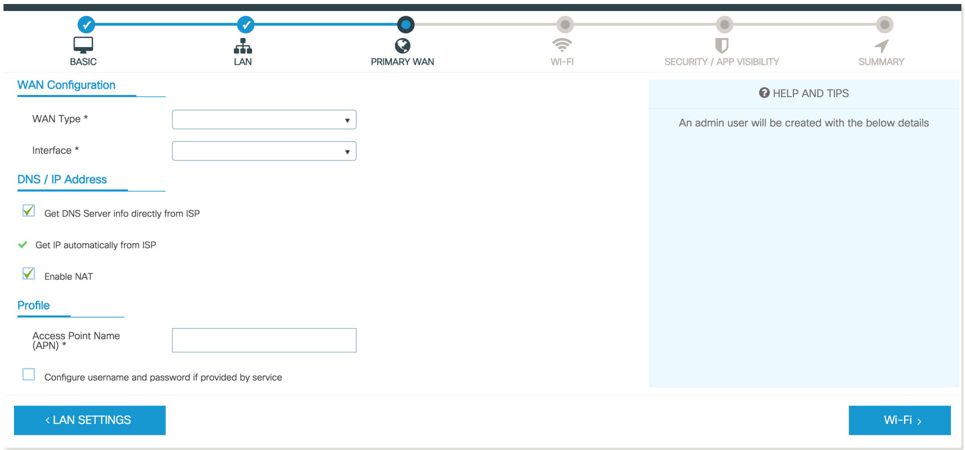
Step 4 Check the **Get IP automatically from ISP** check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.

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

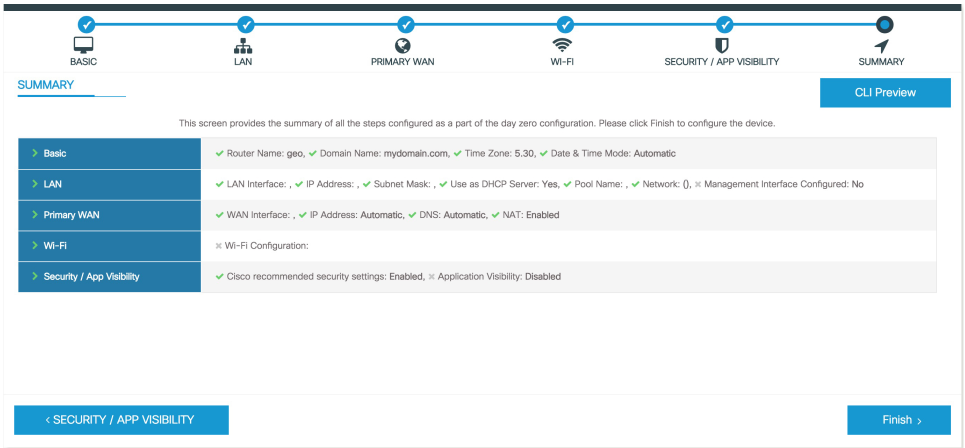
Procedure

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

Table 6: Feature History

Feature Name	Release Information	Description
Monitor and Troubleshoot Device PnP Onboarding using WebUI	Cisco IOS XE 17.15.3	You can now monitor and troubleshoot your Day-0 device onboarding using WebUI through PnP onboarding. If the automated PnP onboarding fails, you can manually onboard your device.

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 5

Console port, Telnet, and SSH handling

This chapter includes these sections:

Notes and restrictions for console port, Telnet, and SSH

- Telnet and Secure Shell (SSH) settings configured in the transport map override any other Telnet or SSH settings when the transport map is applied to the Ethernet management interface.
- Only local usernames and passwords can be used to authenticate users entering a Ethernet management interface. AAA authentication is not available for users accessing the device through a Ethernet management interface using persistent Telnet or persistent SSH.
- Applying a transport map to a Ethernet management interface with active Telnet or SSH sessions can disconnect the active sessions. Removing a transport map from an interface, however, does not disconnect any active Telnet or SSH session.
- 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

The console port on the device 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 device and is located on the front panel of the Route Processor.

For information on accessing the device using the console port, see Using Cisco IOS XE Software, on page 23.

Console port handling

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.

Configuring a console port transport map

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

Procedure

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.

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
```

View console port and SSH handling Configurations

Use these 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** [**ssh**]]

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

Example

The example shows transport maps that are configured on the device: a console port (`consolehandler`), persistent SSH (`sshhandler`), and persistent Telnet transport (`telnethandler`):

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

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0/0/0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt
```

```
Bshell banner:
Welcome to Diagnostic Mode




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

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode


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

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode


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



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

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode
```

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

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

Method : telnet
Rule : wait
Shell banner:
Wait banner :

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

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

Example

The example shows the **show platform software configuration access policy** command being issued both before and after a new transport map for SSH are configured. During the configuration, the connection policy and banners are set for a persistent SSH transport map, and the transport map for SSH is enabled.

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

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

Wait banner :
Waiting for IOS Process


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

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

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 1
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
Router(config)# exit

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

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

Wait banner :
Waiting for IOS process


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

Wait banner :
Waiting for IOS


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

CHAPTER 6

Install the software

This chapter includes these 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.

These are the two main methods to install the software:

- Manage and Configure a device to run using a consolidated package, on page 59—This method allows for individual upgrade of subpackages and generally has reduced boot times compared to the method below. Use this method if you want to individually upgrade a module's software.
- Manage and Configure a device to run using individual packages, on page 93—This a simple method that is similar to a typical Cisco router image installation and management that is supported across Cisco routers.

It is better to upgrade software in a planned period of maintenance when an interruption in service is acceptable. The router needs to be rebooted for a software upgrade to take effect.

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 Hardware Installation Guide for the Cisco 8300 Series Secure Routers.

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.

Provisioning files

This section provides background information about the files and processes used in Manage and Configure a device to run using individual packages, on page 93.

The consolidated package on a device 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 device 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 table provides a list of file systems that can be seen on the Cisco 8300 Series Secure Routers.

Table 7: Device file systems

File System	Description
bootflash:	Boot flash memory file system.
flash:	Alias to the boot flash memory file system above.

File System	Description
harddisk:	Hard disk file system (NVME-M2-600G or USB-M2-16G or USB-M2-32G with the CLI command harddisk).
cns:	Cisco Networking Services file directory.
nvram:	Device 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.
USB Type C	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: or usb1: ports.

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 8: 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 device operations, and can be erased without impacting the functioning of the device.
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 device 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 device.

File or Directory	Description
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 device operations, and can be erased without impacting the device'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. For flash storage, use the **dir bootflash:** command to list the file names.

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

Configure the configuration register for autoboot

The configuration register can be used to change behavior. This includes controlling how the device 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 Use of the Configuration Register on All Cisco Routers.

Note Setting the configuration register to 0x2102 will set the device 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.

How to install and upgrade the software

To install or upgrade the software, use one of thse methods to use the software from a consolidated package or an individual package. Also see the Install a software section.

- Manage and Configure a device to run using a consolidated package, on page 59
- Manage and Configure a device to run using individual packages, on page 93

Manage and Configure a device to run using a consolidated package

Note Do not use these procedures if you also need to install any optional subpackages or plan to upgrade individual subpackages. See Manage and Configure a device to run using individual packages, on page 93.

- Manage and configure a consolidated package using copy and boot Commands, on page 59
- Configure a device to boot the consolidated package via TFTP using the boot command: Example, on page 65

Manage and configure 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 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:/
23      -rw-                0   Jun 5 2025 09:50:37 +00:00  iox_alt_hdd.dsk

784897  drwx          3358720   Jun 5 2025 09:23:28 +00:00  tracelogs

392449  drwx             4096  May 21 2025 09:22:30 +00:00  .rollback_timer

11      -rw-              422  May 21 2025 09:12:33 +00:00  .iox_dir_list

915713  drwx             4096  May 21 2025 09:12:13 +00:00  SHARED-IOX

21      -rw-               30  May 21 2025 09:12:12 +00:00  throughput_monitor_params
```

```
15      -rw-           143041  May 21 2025 09:12:04 +00:00  memleak.tcl

1046531  drwx           73728  May 21 2025 09:12:00 +00:00  license_evlog

1046529  drwx            4096  May 21 2025 09:11:53 +00:00  .prst_sync

12      -rwx           261921  May 21 2025 09:11:47 +00:00  mode_event_log

59      -rw-             7762  May 21 2025 09:09:09 +00:00  packages.conf

48      -rw-             7762  May 21 2025 09:04:42 +00:00
c8kg2be-universalk9.17.15.03a.SPA.conf
1047801  -rw-       59995452  May 21 2025 09:04:39 +00:00  c8kg2be-rpboot.17.15.03a.SPA.pkg

1046537  drwx            4096  May 21 2025 09:04:38 +00:00  .images

130817  drwx             4096  May 21 2025 09:01:56 +00:00  sysboot

47      -rw-             9391  May 21 2025 08:59:39 +00:00
c8kg2be-universalk9.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.conf
1047773  -rw-        59995512  May 21 2025 08:59:38 +00:00
c8kg2be-rpboot.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg
785553  drwx             4096  May 21 2025 06:27:34 +00:00  memaudit_log
13      drwx             4096  May 19 2025 03:58:14 +00:00  core
46      -rw-       1003589796  May 14 2025 11:21:03 +00:00
c8kg2be-universalk9.BLD_V1718_THROTTLE_LATEST_20250423_010128.SSA.bin
45      -rw-              396  May 14 2025 05:39:34 +00:00  ct_persistent.txt
44      -rw-             7711   May 6 2025 08:36:06 +00:00
c8kg2be-universalk9.17.15.03.SPA.conf
1047740  -rw-        59987868   May 6 2025 08:36:03 +00:00  c8kg2be-rpboot.17.15.03.SPA.pkg

24      -rw-        953199576   May 6 2025 07:02:50 +00:00
c8kg2be-universalk9.17.15.03.SPA.bin
43      -rw-            16464   May 6 2025 05:38:49 +00:00  dizeng-crestone-confg

39      -rw-        957518956   May 5 2025 12:04:02 +00:00
c8kg2be-universalk9_npe.17.15.03a.SPA.bin
38      -rw-        953231736   May 4 2025 08:39:53 +00:00
c8kg2be-universalk9.17.15.03a.SPA.bin
1047812  -rw-       891244544   May 2 2025 19:08:25 +00:00
c8kg2be-mono-universalk9.17.15.03a.SPA.pkg
1047807  -rw-         5677056   May 2 2025 19:07:15 +00:00
c8kg2be-firmware_nim_xdsl.17.15.03a.SPA.pkg
1047809  -rw-        13889536   May 2 2025 19:07:15 +00:00
c8kg2be-firmware_sm_1t3e3.17.15.03a.SPA.pkg
1047808  -rw-        10444800   May 2 2025 19:07:15 +00:00
c8kg2be-firmware_prince.17.15.03a.SPA.pkg
1047810  -rw-        14671872   May 2 2025 19:07:15 +00:00
c8kg2be-firmware_sm_async.17.15.03a.SPA.pkg
1047804  -rw-        11956224   May 2 2025 19:07:14 +00:00
c8kg2be-firmware_ngwic_t1e1.17.15.03a.SPA.pkg
1047806  -rw-        11804672   May 2 2025 19:07:14 +00:00
c8kg2be-firmware_nim_shdsl.17.15.03a.SPA.pkg
1047805  -rw-        13254656   May 2 2025 19:07:14 +00:00
c8kg2be-firmware_nim_async.17.15.03a.SPA.pkg
1047811  -rw-          204800   May 2 2025 19:07:14 +00:00
c8kg2be-firmware_sm_nim_adpt.17.15.03a.SPA.pkg
29      -rw-        953227220  Apr 22 2025 12:40:25 +00:00
c8kg2be-universalk9.BLD_V1715_3_THROTTLE_LATEST_20250421_200058.SSA.bin
28      -rw-          5813308  Apr 22 2025 12:03:54 +00:00
SDK112312-Prod-SoC2-v17.15.3_1r-cp.pkg
26      -rw-           763701  Apr 17 2025 08:58:31 +00:00  wilson-running-cfg.txt
```

```
25      -rw-          8630272  Apr 11 2025 11:28:20 +00:00
c8kg2be-hw-programmables.C0x25033132_W0x25033132.pkg
14      -rw-         56012800   Apr 3 2025 08:56:15 +00:00
secapp-utd.17.15.03.1.0.8_SV3.1.81.0_XE17.15.aarch64.tar
75      -rw-       1002810808   Apr 1 2025 07:21:54 +00:00
c8kg2be-universalk9.BLD_POLARIS_DEV_LATEST_20250325_181737.SSA.bin
1047751  -rw-        891219968  Mar 26 2025 06:51:11 +00:00
c8kg2be-mono-universalk9.17.15.03.SPA.pkg
1047747  -rw-         10444800  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_prince.17.15.03.SPA.pkg
1047745  -rw-         11804672  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg
1047750  -rw-           204800  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg
1047744  -rw-         13254656  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_nim_async.17.15.03.SPA.pkg
1047743  -rw-         11956224  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg
1047748  -rw-         13889536  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg
1047746  -rw-          5677056  Mar 26 2025 06:50:09 +00:00
c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg
1047749  -rw-         14671872  Mar 26 2025 06:50:08 +00:00
c8kg2be-firmware_sm_async.17.15.03.SPA.pkg
74      -rw-          2510307  Mar 19 2025 07:08:14 +00:00  redirect.out

72      -rw-        953199060  Mar 12 2025 07:00:51 +00:00
c8kg2be-universalk9.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.bin

1047784  -rw-        891203584  Mar 10 2025 20:59:47 +00:00
c8kg2be-mono-universalk9.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

1047781  -rw-         13889536  Mar 10 2025 20:58:37 +00:00
c8kg2be-firmware_sm_1t3e3.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

1047779  -rw-          5677056  Mar 10 2025 20:58:37 +00:00
c8kg2be-firmware_nim_xdsl.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

1047780  -rw-         10444800  Mar 10 2025 20:58:37 +00:00
c8kg2be-firmware_prince.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

1047782  -rw-         14671872  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_sm_async.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

1047778  -rw-         11804672  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_nim_shdsl.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

1047776  -rw-         11956224  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_ngwic_t1e1.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

1047783  -rw-           204800  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_sm_nim_adpt.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg
1047777  -rw-         13254656  Mar 10 2025 20:58:36 +00:00
c8kg2be-firmware_nim_async.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

62      -rw-          5823548  Feb 25 2025 12:53:04 +00:00  C8000-NG-S2-17-15-1_17r.pkg

1046534  drwx             4096   Feb 3 2025 10:28:42 +00:00  pnp-tech

392450  drwx             4096  Jan 28 2025 07:20:24 +00:00  .dbpersist

71      -rw-           261214  Jan 28 2025 07:16:04 +00:00  ajay_backup.cfg

70      -rw-          5821500  Jan 24 2025 02:54:43 +00:00
```

```
SDK112312-Prod-SoC2-v17.15.1_14r-cp.pkg
68      -rw-          9754990  Jan 20 2025 05:17:19 +00:00  show-tech1717

69      -rw-           846347  Jan 20 2025 05:16:14 +00:00
CRFT_Admintech_C8375EG2_2025-01-20_05-16-14.tar.gz
66      -rw-             6928  Jan 13 2025 07:39:59 +00:00  ciscortr.cfg

65      -rw-             6928  Jan 13 2025 07:39:04 +00:00  C8375-E-G2.cfg

64      -rw-           301992   Jan 9 2025 09:08:37 +00:00  dual-public-ip.cfg

63      -rw-       1015740420   Jan 8 2025 07:33:57 +00:00
c8kg2be-universalk9.BLD_POLARIS_DEV_LATEST_20250106_030447.SSA.bin

60      -rw-          4653056  Dec 25 2024 03:50:16 +00:00
c8k30be-hw-programmables.C0x2408272B.pkg
37      -rw-        969660392  Dec 11 2024 05:40:52 +00:00
c8k30be-universalk9.BLD_POLARIS_DEV_LATEST_20241209_180254_V17_17_0_27.SSA.bin

32      -rw-        958470964   Dec 5 2024 05:25:07 +00:00
mira_rom_17.15_1.8r.s2.RelDebug.bin
50      -rw-           301239  Nov 22 2024 11:01:52 +00:00  rc_22_11_24

49      -rw-        952760408  Nov 21 2024 03:53:44 +00:00
c8k30be-universalk9.17.15.02.SPA.bin
42      -rw-          5733436   Nov 6 2024 06:19:35 +00:00
SDK112312-Prod-SoC2-v17.15.1_7d_RSA4K.pkg
41      -rw-             9044  Oct 30 2024 09:26:50 +00:00  cessna-snake.cfg

34      -rwx         39490752  Oct 23 2024 20:15:10 +00:00  mirabile_diag.14er.v0.1.6.0826

33      -rw-         14934016  Oct 23 2024 14:42:04 +00:00  mirabile_diag.zb.v1.0.0_qr3

36      drwx             4096  Oct 19 2024 11:42:32 +00:00  .geo

35      -rw-         56002560  Oct 10 2024 06:32:32 +00:00
secapp-utd.BLD_POLARIS_DEV_LATEST_20241007_181057.1.15.2_SV3.1.81.0_XEmain.aarch64.tar

1046539  -rw-         56309176  Aug 13 2024 09:04:49 +00:00
c8k30be-rpboot.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

20      drwx             4096  Aug 13 2024 09:01:06 +00:00  guest-share

785011  drwx             4096  Aug 13 2024 09:01:04 +00:00  pnp-info

915715  drwx             4096  Aug 13 2024 09:01:04 +00:00  onep

915714  drwx             4096  Aug 13 2024 09:00:58 +00:00  virtual-instance

19      -rw-             1939  Aug 13 2024 09:00:57 +00:00  trustidrootx3_ca_062035.ca

18      -rw-             1826  Aug 13 2024 09:00:57 +00:00  trustidrootx3_ca_092025.ca

1046550  -rw-        885977088  Jul 13 2024 06:13:59 +00:00
c8k30be-mono-universalk9.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

1046548  -rw-         14675968  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_sm_async.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

1046544  -rw-         11804672  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_nim_shdsl.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

1046547  -rw-         13889536  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_sm_1t3e3.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg
```

```
1046549  -rw-           204800  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_sm_nim_adpt.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

1046545  -rw-          5677056  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_nim_xdsl.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

1046543  -rw-         13258752  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_nim_async.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

1046542  -rw-         11956224  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_ngwic_t1e1.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

1046546  -rw-         10444800  Jul 13 2024 06:12:52 +00:00
c8k30be-firmware_prince.BLD_POLARIS_DEV_LATEST_20240713_033504_V17_16_0_22.SSA.pkg

27      -rw-          5788732  Feb 29 2024 18:42:07 +00:00
SDK112312-Prod-SoC2-v17.15.1_13d-cp.pkg
786101  -rw-         67728148  Feb 27 2024 17:30:28 +00:00
c8kg2be-rpboot.2024-12-12_16.42_sukhoo.SSA.pkg
31      -rw-          5784636  Feb 27 2024 17:30:19 +00:00
SDK112312-Prod-SoC2-v17.15.1_13r-cp.pkg
786100  -rw-        899686400  Feb 27 2024 17:28:58 +00:00
c8kg2be-mono-universalk9.2024-12-12_16.42_sukhoo.SSA.pkg
786095  -rw-         10444800  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_prince.2024-12-12_16.42_sukhoo.SSA.pkg
786096  -rw-            53248  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_pse_si3470a.2024-12-12_16.42_sukhoo.SSA.pkg
786097  -rw-         13889536  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_sm_1t3e3.2024-12-12_16.42_sukhoo.SSA.pkg
786099  -rw-           204800  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_sm_nim_adpt.2024-12-12_16.42_sukhoo.SSA.pkg
786098  -rw-         14675968  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_sm_async.2024-12-12_16.42_sukhoo.SSA.pkg
786091  -rw-         11956224  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_ngwic_t1e1.2024-12-12_16.42_sukhoo.SSA.pkg
786093  -rw-         11804672  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_nim_shdsl.2024-12-12_16.42_sukhoo.SSA.pkg
786094  -rw-          5677056  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_nim_xdsl.2024-12-12_16.42_sukhoo.SSA.pkg
786092  -rw-         13258752  Feb 27 2024 17:28:57 +00:00
c8kg2be-firmware_nim_async.2024-12-12_16.42_sukhoo.SSA.pkg
57      -rw-             9840  Feb 27 2024 17:28:56 +00:00  prev_packages.conf

40      -rw-           301569  Feb 27 2024 17:28:49 +00:00  original-xe-config

53      -rw-           301569  Feb 27 2024 17:28:31 +00:00  241213.cfg

523273  drwx             4096  Feb 27 2024 17:28:03 +00:00  dbgd

58      -rw-              107  Feb 27 2024 17:27:55 +00:00  pki_certificates

56      -rw-              147  Feb 27 2024 17:27:20 +00:00  utm_pf_filtered_luids.json

523266  drwx             4096  Feb 27 2024 17:26:56 +00:00  vmanage-admin

523265  drwx             4096  Feb 27 2024 17:26:55 +00:00  admin_tech

130830  drwx             4096  Feb 27 2024 17:26:55 +00:00  .sdwaninternal

130831  drwx             4096  Feb 27 2024 17:26:48 +00:00  sdwan

30      drwx             4096  Feb 27 2024 17:26:04 +00:00  lost+found
```

```
                                                            20237881344 bytes total
(1147678720 bytes free)

Router# copy tftp: bootflash:Address or name of remote host []? 203.0.113.2
Source filename []? /auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin
Destination filename [c8kg2be-universalk9.17.15.03prd1.SPA.bin]?
Accessing tftp://203.0.113.2//auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin...
%Error opening
tftp://203.0.113.2//auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin (Timed
out)
C8300-Router#
C8300-Router#copy tftp bootflash
Address or name of remote host [203.0.113.2]? 203.0.113.2
Source filename [/auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin]?
Destination filename [c8kg2be-universalk9.17.15.03prd1.SPA.bin]?
Accessing tftp://203.0.113.2//auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin...
Loading /auto/tftp-ngio/test/c8kg2be-universalk9.17.15.03prd1.SPA.bin from 203.0.113.2 (via
 GigabitEthernet0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
[OK - 696368193 bytes]

696368193 bytes copied in 478.600 secs (1455011 bytes/sec)

Router# dir bootflash:
Directory of bootflash:/

106497  drwx             4096   Jul 8 2020 11:38:27 -07:00  tracelogs
11      -rw-        696368193   Jul 8 2020 11:34:28 -07:00
c8kg2be-universalk9.17.15.03prd1.SPA.bin
458753  drwx             4096  Jun 24 2020 17:25:47 -07:00  sysboot

7693897728 bytes total (5950341120 bytes free)
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash bootflash:c8kg2be-universalk9.17.15.03prd1.SPA.bin
Router(config)# config-reg 0x2102
Router(config)# exit
Router# show run | include boot
boot-start-marker
boot system flash bootflash:c8kg2be-universalk9.17.15.03prd1.SPA.bin
boot-end-marker
diagnostic bootup level minimal
Router# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
```

Configure a device to boot the consolidated package via TFTP using the boot command: Example

```
Router#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#boot system tftp://10.124.19.169/c8kg2be-universalk9.17.15.03a.SPA.bin
Router(config)#end
Router#wr
Building configuration...
[OK]
Router#show bootvar
BOOT variable = tftp://10.124.19.169/c8kg2be-universalk9.17.15.03a.SPA.bin,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102

Standby not ready to show bootvar

Router#reload
Proceed with reload? [confirm]

System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory

........

h/w (environment):
 interface : eth0
 mac       : 48:74:10:4A:EF:1F
n/w (environment):
 ip        : 192.168.22.10
 mask      : 255.255.255.0
 gateway   : 192.168.22.1

h/w:
 interface : eth0 (Ethernet)
 status    : connected
 mac       : 48:74:10:4A:EF:1F
n/w (ip v4):
 ip        : 192.168.22.10
 mask      : 255.255.255.0
 route(s)  : 0.0.0.0 -> 192.168.22.0/255.255.255.0
           : 192.168.22.1 -> 0.0.0.0/0.0.0.0

tftp v4:
 server    : 10.124.19.169
 file      : c8kg2be-universalk9.17.15.03a.SPA.bin
 blocksize : 1460
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Performing Signature Verification of OS image...
Image validated

Jun  6 06:52:50.787: %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.
Jun  6 06:53:13.468: %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], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.15.3a, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 02-May-25 11:27 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.


Jun  6 06:53:16.982: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota exceeded
 [free space is 166800 kB] - [recommended free space is 5929066 kB] - Please clean up files
 on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906881K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.
No processes could be found for the command

 WARNING: Command has been added to the configuration using a type 0 password. However,
recommended to migrate to strong type-6 encryption

 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!
```

Install the software using install commands

From Cisco IOS XE 17.15.3a, Cisco 8300 Series Secure Routers are shipped in install mode by default. Users can boot the platform, and upgrade to Cisco IOS XE software versions using a set of **install** commands.

Restrictions

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

Information about installing the software using install commands

From Cisco IOS XE 17.15.3a release, for routers shipped in install mode, a set of **install** commands can be used for starting, upgrading and downgrading of platforms in install mode. This update is applicable to the Cisco 8300 Series Secure Routers.

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

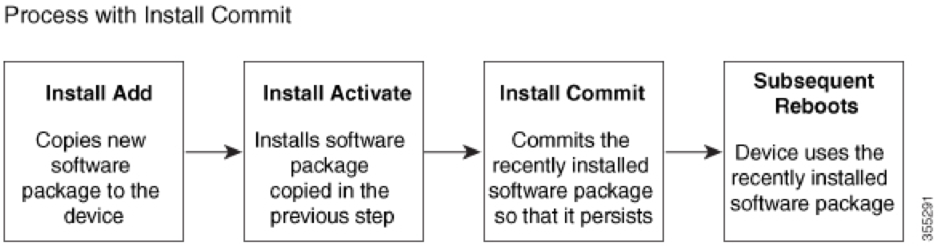
Table 9: Bundle mode vs Install mode

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 TFTP Boot 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 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.

A list install commands available:

Table 10: 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.

Command	Syntax	Purpose
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.
(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.

Command	Syntax	Purpose
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.
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.

Command	Syntax	Purpose
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.
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 11: 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.

Command	Syntax	Purpose
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.
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.

Command	Syntax	Purpose
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.

Procedure

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:c8kg2be-universalk9.17.15.03prd1.SPA.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.

Procedure

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:c8kg2be-universalk9.17.15.03prd1.SPA.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.

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 install mode

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

Downgrade in 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

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

```
Router# install add file bootflash:c8kg2be-universalk9.17.15.03.SPA.bin activate commit

May  6 08:35:19.308: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
add_activate_commit bootflash:c8kg2be-universalk9.17.15.03.SPA.bininstall_add_activate_commit:
 START Tue May 06 08:35:19 UTC 2025
install_add: START Tue May 06 08:35:19 UTC 2025
install_add: Adding IMG
--- Starting initial file syncing ---
Copying bootflash:c8kg2be-universalk9.17.15.03.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: 17.15.03.0.5635

Finished Add

install_activate: START Tue May 06 08:36:08 UTC 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c8kg2be-rpboot.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg
/bootflash/c8kg2be-mono-universalk9.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_sm_async.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_nim_async.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg
/bootflash/c8kg2be-firmware_prince.17.15.03.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]
May  6 08:36:08.538: %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

May  6 08:37:37.284: %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 Tue May 06 08:37:59 UTC 2025

Router#
May  6 08:37:59.818: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
 add_activate_commitMay  6 0


System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory

........
boot: reading file c8kg2be-universalk9.17.15.03.SPA.bin
##########################################################################################


Performing Signature Verification of OS image...
Image validated
May  6 08:40:59.347: %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.
May  6 08:41:21.936: %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], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 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.


May  6 08:41:25.397: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota exceeded
 [free space is 3172248 kB] - [recommended free space is 5929066 kB] - Please clean up files
 on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906887K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.

WARNING: Command has been added to the configuration using a type 0 password. However,
recommended to migrate to strong type-6 encryption

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!


*May  6 08:41:23.620: %CRYPTO-5-SELF_TEST_START: Crypto algorithms release (Rel5a), Entropy
 release (3.4.1)
       begin Crypto Module self-tests
*May  6 08:41:23.620: %CRYPTO-5-SELF_TEST_START: Crypto algorithms release (Rel5a), Entropy
 release (3.4.1)
       begin Crypto Module Integrity Test
*May  6 08:41:23.625: %CRYPTO-5-SELF_TEST_END: Crypto Integrity self-test completed
successfully
       All tests passed.
*May  6 08:41:23.808: %CRYPTO-5-SELF_TEST_END: Crypto Algorithm self-test completed
successfully
       All tests passed.
*May  6 08:41:24.426: %ISR_THROUGHPUT-6-LEVEL: Throughput level has been set to 3000000
kbps
*May  6 08:41:24.691: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled
```

```
ESG-PM-ACL:[subsys-init] Init ESG-ACL subsystem starting

*May  6 08:41:27.684: ESG-PM-ACL:[subsys-init] Init ESG-ACL platform API reg

*May  6 08:41:27.684: ESG-PM-ACL:[subsys-init] Init ESG-ACL subsystem ended

*May  6 08:41:27.684: NGIOLite module C-NIM-8M success read extended attr from conf file

*May  6 08:41:29.186: %TLSCLIENT-5-TLSCLIENT_IOS: TLS Client is IOS based
*May  6 08:41:29.203: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*May  6 08:41:29.252: %CRYPTO_ENGINE-5-CSDL_COMPLIANCE_ENFORCED: Cisco PSB security compliance
 is being enforced
*May  6 08:41:29.267: %CUBE-3-LICENSING:  SIP trunking (CUBE) licensing is now based on
dynamic sessions counting, static license capacity configuration through 'mode border-element
 license capacity' would be ignored.
*May  6 08:41:29.268: %SIP-5-LICENSING: CUBE license reporting period has been set to the
minimum value of 8 hours.
*May  6 08:41:29.286: %VOICE_HA-7-STATUS: CUBE HA-supported platform detected.
*May  6 08:41:30.029: %CRYPTO_SL_TP_LEVELS-6-PLATFORM_BASED_LIC: Platform Based License
Support, throughput is un-throttled
*May  6 08:41:30.061: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*May  6 08:41:30.069: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*May  6 08:41:30.069: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to up
*May  6 08:41:30.069: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, changed
state to up
*May  6 08:41:30.069: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*May  6 08:41:30.070: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*May  6 08:41:30.071: %IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL GigabitEthernet0 Physical
Port Link Down
*May  6 08:41:30.243: %PNP-6-PNP_DISCOVERY_STARTED: PnP Discovery started
*May  6 08:40:41.171: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: MPCCE: Failed to read
 idprom cookie; error code: 100
*May  6 08:40:41.184: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: Error logging in to
tam device, rc=0x64-TAM_LIB_ERR_MANDATORY_BUS_ENCRYPT_ENABLED
*May  6 08:40:41.184: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: Error initializing
tam device. PCR8 will not be extended.
*May  6 08:40:46.480: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: MPCCE: Failed to read
 idprom cookie; error code: 100
*May  6 08:40:46.493: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: Error logging in to
tam device, rc=0x64-TAM_LIB_ERR_MANDATORY_BUS_ENCRYPT_ENABLED
*May  6 08:40:46.493: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/updatepcr8d: Error initializing
tam device. PCR8 will not be extended.
*May  6 08:40:59.263: %SERVICES-2-NORESOLVE_ACTIVE: C0/0: cmcc: Error resolving active FRU:
 BINOS_FRU_RP
*May  6 08:40:59.346: %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.
*May  6 08:41:21.935: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode
*May  6 08:41:25.396: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota exceeded
 [free space is 3172248 kB] - [recommended free space is 5929066 kB] - Please clean up files
 on bootflash.
*May  6 08:41:25.952: %CMRP_PFU-6-PEM_INSERTED: R0/0: cmand: Power Supply in slot 0 not
operational.
*May  6 08:41:26.077: %CMRP_PFU-6-FANASSY_INSERTED: R0/0: cmand: Fan Assembly is inserted.
*May  6 08:41:30.313: %SYS-5-CONFIG_P: Configured programmatically by process MGMT VRF
Process from console as vty0
*May  6 08:41:30.519: %IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO: Management vrf Mgmt-intf created
 with ID 1, ipv4 table-id 0x1, ipv6 table-id 0x1E000001
*May  6 08:41:30.519: %SYS-5-CONFIG_P: Configured programmatically by process MGMT VRF
Process from console as vty0
*May  6 08:41:30.688: %IOSXE_RP_ALARM-2-PEM: ASSERT CRITICAL Power Supply Module 0 Power
Supply Failure
*May  6 08:41:30.688: %IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL POE Module 0 Power Supply
Failure
```

```
*May  6 08:41:30.714: %ONEP_BASE-6-SS_ENABLED: ONEP: Service set Base was enabled by Default
*May  6 08:41:31.046: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
 to down
*May  6 08:41:31.058: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state
 to up
*May  6 08:41:31.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state
 to up
*May  6 08:41:31.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state
 to up
*May  6 08:41:31.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to down
*May  6 08:41:31.262: %SMART_LIC-6-USAGE_NO_ACK: A Usage report acknowledgement has not
been received in the last 0 days.
*May  6 08:41:31.263: %SIP-5-LICENSING: smart license report is not acknowledged.
*May  6 08:41:31.773: %SYS-7-NVRAM_INIT_WAIT_TIME: Waited 0 seconds for NVRAM to be available
*May  6 08:41:31.944: %SYS-6-PRIVCFG_DECRYPT_SUCCESS: Successfully apply the private config
 file
*May  6 08:41:32.030: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: TP-self-signed-2220840378 created
 succesfully
*May  6 08:41:32.031: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: SLA-TrustPoint created succesfully
*May  6 08:41:32.034: %PKI-3-KEY_CMP_MISMATCH: Key in the certificate and stored key does
not match for Trustpoint-TP-self-signed-2220840378.
*May  6 08:41:32.041: %AAA-6-USERNAME_CONFIGURATION: user with username: admin configured
*May  6 08:41:32.041: %AAAA-4-CLI_DEPRECATED: WARNING: Command has been added to the
configuration using a type 0 password. However, recommended to migrate to strong type-6
encryption
*May  6 08:41:32.041: %AAA-6-USER_PRIVILEGE_UPDATE: username: admin privilege updated with
 priv-15
*May  6 08:41:32.259: %SYS-5-CONFIG_I: Configured from memory by console
*May  6 08:41:32.268: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled
*May  6 08:41:32.268: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*May  6 08:41:32.275: %SPA_OIR-6-OFFLINECARD: SPA (4M-2xSFP+) offline in subslot 0/0
*May  6 08:41:32.278: %SPA_OIR-6-OFFLINECARD: SPA (C-NIM-8M) offline in subslot 0/1
*May  6 08:41:32.306: %IOSXE_RP_ALARM-2-ESP: ASSERT CRITICAL module R0 No Working ESP
*May  6 08:41:32.309: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F0
*May  6 08:41:32.309: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 0
*May  6 08:41:32.309: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 1
*May  6 08:41:32.325: %CRYPTO-5-SELF_TEST_START: Crypto algorithms release (Rel5a), Entropy
 release (3.4.1)
       begin Crypto Module self-tests
*May  6 08:41:32.329: %CRYPTO-5-SELF_TEST_END: Crypto Algorithm self-test completed
successfully
       All tests passed.
*May  6 08:41:32.712: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server iox has been
notified to start
*May  6 08:41:33.077: %SYS-5-RESTART: System restarted --
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 by mcpre
*May  6 08:41:33.084: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing a cold
start
*May  6 08:41:33.084: %SYS-5-CONFIG_I: Configured from console by console
*May  6 08:41:33.759: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0
*May  6 08:41:34.091: %SYS-6-BOOTTIME: Time taken to reboot after reload =  215 seconds
*May  6 08:41:35.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup0,
changed state to up
*May  6 08:41:35.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup1,
changed state to up
*May  6 08:41:35.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup10,
changed state to up
*May  6 08:41:38.437: %PNP-6-PNP_BEST_UDI_UPDATE: Best UDI
[PID:C8375-E-G2,VID:V01,SN:FDO2833M01A] identified via (entity-mibs)
```

```
*May  6 08:41:38.437: %PNP-6-PNP_CDP_UPDATE: Device UDI
[PID:C8375-E-G2,VID:V01,SN:FDO2833M01A] identified for CDP
*May  6 08:41:38.437: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Startup Config
Present)
*May  6 08:41:39.699: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to up
*May  6 08:41:40.707: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to up
*May  6 08:41:42.333: %SYS-5-CONFIG_P: Configured programmatically by process EPM CREATE
DEFAULT CWA URL ACL from console as console
*May  6 08:41:46.197: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in slot 0
*May  6 08:41:46.230: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0
*May  6 08:41:46.587: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in slot 1
*May  6 08:41:47.126: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*May  6 08:41:47.126: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*May  6 08:41:48.779: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/1
*May  6 08:41:49.452: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*May  6 08:41:49.452: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*May  6 08:41:49.571: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: CISCO_IDEVID_SUDI created
succesfully
*May  6 08:41:49.573: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named CISCO_IDEVID_SUDI has been
 generated or imported by pki-sudi
*May  6 08:41:49.609: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: CISCO_IDEVID_SUDI0 created
succesfully
*May  6 08:41:49.610: %PKI-2-NON_AUTHORITATIVE_CLOCK: PKI functions can not be initialized
 until an authoritative time source, like NTP, can be obtained.
*May  6 08:41:53.146: %IOX-3-PD_PARTITION_CREATE: R0/0: run_ioxn_caf: IOX may take upto 3
mins to be ready. Wait for iox to be ready before installing the apps
*May  6 08:41:53.429: %IOX-3-PD_PARTITION_CREATE: R0/0: run_ioxn_caf: Successfully allocated
 4.0G in flash for hosting ApplicationsNGIOLite module C-NIM-8M success read extended attr
 from conf file

*May  6 08:42:15.679: %SPA_OIR-6-ONLINECARD: SPA (C-NIM-8M) online in subslot 0/1
*May  6 08:42:16.292: %ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P0, State: Minor_Low,
 Reading: 0 mV
*May  6 08:42:20.701: %ONEP_BASE-3-AUTHEN_ERR: [Element]: Authentication/authorization
failed. Application (utd_snort-utd): Username (*INVALID*)
*May  6 08:42:22.179: %TRANSCEIVER-6-INSERTED: C0/0: iomd: transceiver module inserted in
Te0/0/4
*May  6 08:42:22.255: %TRANSCEIVER-6-INSERTED: C0/0: iomd: transceiver module inserted in
Te0/0/5
*May  6 08:42:22.643: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/1/6, changed state to
up
*May  6 08:42:23.345: %SPA_OIR-6-ONLINECARD: SPA (4M-2xSFP+) online in subslot 0/0
*May  6 08:42:23.644: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwoGigabitEthernet0/1/6,
 changed state to up
*May  6 08:42:28.999: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/4, changed state to
up
*May  6 08:42:29.011: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/0/5, changed state to
up
*May  6 08:42:29.975: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/0/0, changed state to
up
*May  6 08:42:30.004: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/0/4,
 changed state to up
*May  6 08:42:30.010: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/0/5,
 changed state to up
*May  6 08:42:29.901: %IM-6-IOX_INST_INFO: R0/0: ioxman: IOX SERVICE guestshell LOG:
Guestshell is up at 04/06/2025 08:42:29
*May  6 08:42:30.974: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/0/1, changed state to
up
*May  6 08:42:30.976: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwoGigabitEthernet0/0/0,
 changed state to up
*May  6 08:42:31.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwoGigabitEthernet0/0/1,
 changed state to up
*May  6 08:42:31.983: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/0/3, changed state to
```

```
up
*May  6 08:42:32.644: %LINK-3-UPDOWN: Interface TwoGigabitEthernet0/1/7, changed state to
up
*May  6 08:42:32.366: %CMRP-5-CHASSIS_MONITOR_BOOT_TIME_PRINT: R0/0: cmand: Card F0 took
59 secs to boot
*May  6 08:42:32.367: %CMRP-5-CHASSIS_MONITOR_BOOT_TIME_PRINT: R0/0: cmand: Card 0 took 54
 secs to boot
*May  6 08:42:32.367: %CMRP-5-CHASSIS_MONITOR_BOOT_TIME_PRINT: R0/0: cmand: Card 1 took 54
 secs to boot
*May  6 08:42:32.984: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwoGigabitEthernet0/0/3,
 changed state to up
*May  6 08:42:33.642: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwoGigabitEthernet0/1/7,
 changed state to up
*May  6 08:42:34.003: ALL modules are online!
*May  6 08:42:34.765: %IM-6-IOX_ENABLEMENT: R0/0: ioxman: IOX is ready.
*May  6 08:42:34.766: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succeeded: utd is
started Current is in RUNNING
May  6 08:42:36.712: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
May  6 08:42:38.080: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will
be required in 0 days.
May  6 08:42:38.081: ALL modules are online!
May  6 08:42:41.695: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will
be required in 0 days.
Router>
May  6 08:42:51.407: %ONEP_BASE-6-CONNECT: [Element]: ONEP session Application:utd_snort
Host:utd ID:3545 User: has connected.
```

This is an example of the three-step installation:

```
Router#install add file bootflash:c8kg2be-universalk9.17.15.03a.SPA.bin
install_add: START Wed May 21 09:03:39 UTC 2025
install_add: Adding IMG
% UTD: Received appnav notification from LXC for   (src 192.0.2.5, dst 192.0.2.6)
% UTD successfully registered with Appnav (src 192.0.2.5, dst 192.0.2.6)
% UTD redirect interface set to VirtualPortGroup1 internally
--- Starting initial file syncing ---
Copying bootflash:c8kg2be-universalk9.17.15.03a.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: 17.15.03a.0.176

Finished Add

SUCCESS: install_add /bootflash/c8kg2be-universalk9.17.15.03a.SPA.bin Wed May 21 09:04:43
UTC 2025

Router#show install log
[0|install_op_boot]: START Wed May 21 09:02:03 Universal 2025
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS  Wed May 21 09:02:03 Universal 2025
[0|install_op_boot(INFO, )]: cleanup_trap  remote_invocation 0 operation install_op_boot
.. 0 .. 0
[remote|COMP_CHECK]: START Wed May 21 09:04:42 UTC 2025
[remote|COMP_CHECK]: END FAILED exit(1)  Wed May 21 09:04:43 UTC 2025

Router#
Router#install activate
```

```
install_activate: START Wed May 21 09:07:21 UTC 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c8kg2be-rpboot.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_sm_nim_adpt.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_nim_async.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_sm_async.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_prince.17.15.03a.SPA.pkg
/bootflash/c8kg2be-mono-universalk9.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_nim_shdsl.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_ngwic_t1e1.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_sm_1t3e3.17.15.03a.SPA.pkg
/bootflash/c8kg2be-firmware_nim_xdsl.17.15.03a.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

 [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

SUCCESS: install_activate Wed May 21 09:09:31 UTC 2025
Router#May 21 09:

System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory


........

boot: reading file packages.conf
#

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

Performing Signature Verification of OS image...
Image validated

May 21 09:11:47.581: %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], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.15.3a, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Fri 02-May-25 11:27 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.


May 21 09:11:51.161: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota exceeded
 [free space is 1111072 kB] - [recommended free space is 5929066 kB] - Please clean up files
 on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906881K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.
The process for the command is not responding or is otherwise unavailable

 WARNING: Command has been added to the configuration using a type 0 password. However,
recommended to migrate to strong type-6 encryption

 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!

% UTD: Received appnav notification from LXC for   (src 192.0.2.5, dst 192.0.2.6)
% UTD successfully registered with Appnav (src 192.0.2.5, dst 192.0.2.6)
% UTD redirect interface set to VirtualPortGroup1 internally

Router>
Router>en
Router#
Router#install commit
install_commit: START Wed May 21 09:22:28 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 Wed May 21 09:22:31 UTC 2025
```

These are sample outputs for show commands:

show install log

```
Device# show install log
[0|install_op_boot]: START Thu Oct 28 22:09:29 Universal 2021
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS  Thu Oct 28 22:09:30 Universal 2021
```

show install summary

```
Device# 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    17.15.03a.0.176


--------------------------------------------------------------------------------

Auto abort timer: inactive

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

show install package *filesystem: filename*

```
Device# show install package bootflash:c8kg2be-universalk9.17.15.03a.SPA.bin
  Package: c8kg2be-universalk9.17.15.03a.SPA.bin
  Size: 953231736
  Timestamp:
Canonical path: /bootflash/c8kg2be-universalk9.17.15.03a.SPA.bin

  Raw disk-file SHA1sum:
    d358592ccd2dd626889ef091401d06fae5458ff1
Header size:     1084 bytes
Package type:    30000
Package flags:   0
Header version:  3

Internal package information:
  Name: rp_super
  BuildTime: 2025-05-02_11.57
  ReleaseDate: 2025-05-02_16.50
  BootArchitecture: arm64
  RouteProcessor: mirabile
  Platform: C8KG2BE
  User: mcpre
  PackageName: universalk9
  Build: 17.15.03a
  CardTypes:

Package is bootable from media and tftp.
Package contents:

Package: c8kg2be-firmware_prince.17.15.03a.SPA.pkg
  Size: 10444800
  Timestamp:

  Raw disk-file SHA1sum:
    fa82bed30d349686d1d9700892076a3d66375698
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_prince
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_prince
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-mono-universalk9.17.15.03a.SPA.pkg
  Size: 891244544
  Timestamp:

  Raw disk-file SHA1sum:
    af7ba58491731d788d9f4528d74b5bfef9dfc7f2
  Header size:     4096 bytes
  Package type:    30000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: mono
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: arm64
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: mono-universalk9
    Build: 17.15.03a
    CardTypes:

  Package is bootable from media and tftp.
  Package contents:

Package: c8kg2be-firmware_nim_xdsl.17.15.03a.SPA.pkg
  Size: 5677056
  Timestamp:

  Raw disk-file SHA1sum:
    4af7a8764651253c73c7fadebeba6f3a8f0a133d
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_nim_xdsl
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_nim_xdsl
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_sm_1t3e3.17.15.03a.SPA.pkg
  Size: 13889536
  Timestamp:

  Raw disk-file SHA1sum:
    526aa41ccd8398e7691d316ca24289801e0417a8
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_sm_1t3e3
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_sm_1t3e3
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_sm_async.17.15.03a.SPA.pkg
  Size: 14671872
  Timestamp:
  Raw disk-file SHA1sum:
    7c7f4c06da5b3b0e1db879e074998130db22298f
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_sm_async
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_sm_async
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_nim_async.17.15.03a.SPA.pkg
  Size: 13254656
  Timestamp:

  Raw disk-file SHA1sum:
    27132c3a41c79991d1f71488ad325ad05cc7b0bb
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_nim_async
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_nim_async
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_nim_shdsl.17.15.03a.SPA.pkg
  Size: 11804672
  Timestamp:

  Raw disk-file SHA1sum:
    51da21dffb39d2ef6b266b7ffab083b3fb339651
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_nim_shdsl
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_nim_shdsl
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_ngwic_t1e1.17.15.03a.SPA.pkg
  Size: 11956224
  Timestamp:

  Raw disk-file SHA1sum:
    19376efa2ed616672c0d488b628a768e262bd8e6
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_ngwic_t1e1
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_ngwic_t1e1
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
Package: c8kg2be-firmware_sm_nim_adpt.17.15.03a.SPA.pkg
  Size: 204800
  Timestamp:

  Raw disk-file SHA1sum:
    b3a7ddd80df900d6217bb8db36ff8bdbc6241fa3
  Header size:     4096 bytes
  Package type:    40000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: firmware_sm_nim_adpt
    BuildTime: 2025-05-02_11.57
    ReleaseDate: 2025-05-02_16.50
    BootArchitecture: none
    RouteProcessor: mirabile
    Platform: C8KG2BE
    User: mcpre
    PackageName: firmware_sm_nim_adpt
    Build: 17.15.03a
    CardTypes:

  Package is not bootable.
```

show install active

```
Device# 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  17.15.03a.0.158
--------------------------------------------------------------------------------
```

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

show install inactive

```
Device# 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

```
Device# 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   17.15.03a.0.158
--------------------------------------------------------------------------------



--------------------------------------------------------------------------------

Auto abort timer: inactive

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

show install uncommitted

```
Device# 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
```

Troubleshoot software installation using install commands

Problem Troubleshooting the software installation

Solution Use these 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 these 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.

Manage and Configure a device to run using individual packages

To choose between running individual packages or a consolidated package, see Overview section.

These topics are included in this section:

- Installing subpackages from a consolidated package, on page 93
- Installing a firmware subpackage, on page 104
- Installing subpackages from a consolidated package on a flash drive, on page 103

Installing subpackages from a consolidated package

Perform this procedure to obtain the consolidated package from a TFTP server.

Another variation of this procedure obtains the consolidated package from a USB flash drive. This is described in Installing Subpackages from a Consolidated Package on a Flash Drive.

Before you begin

Copy the consolidated package to the TFTP server.

Procedure

Step 1 **show version**

Example:

```
Router# show version
```

Shows the version of software running on the router. This can later be compared with the version of software to be installed.

Step 2 **dir bootflash:**

Example:

```
Router# dir bootflash:
```

Displays the previous version of software and that a package is present.

Step 3 **show platform**

Example:

```
Router# show platform
Chassis type:: C8375-E-G2
```

Displays the inventory.

Step 4 **mkdir bootflash:** *URL-to-directory-name*

Example:

```
Router# mkdir bootflash:mydir
```

Creates a directory to save the expanded software image.

You can use the same name as the image to name the directory.

Step 5 **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*

Example:

```
Router#  request platform software package expand file
c8kg2be-universalk9.17.15.03prd1.SPA.bin to bootflash:mydir
```

Expands the software image from the TFTP server (*URL-to-consolidated-package*) into the directory used to save the image (*URL-to-directory-name*), which was created in Step 4.

Step 6 **reload**

Example:

```
Router# reload
rommon >
```

Enables ROMMON mode, which allows the software in the consolidated file to be activated.

Step 7 **boot** *URL-to-directory-name*/**packages.conf**

Example:

```
rommon 1 > boot bootflash:mydir/packages.conf
```

Boots the consolidated package, by specifying the path and name of the provisioning file: packages.conf.

Step 8 **show version installed**

Example:

```
Router# show version installed
Package: Provisioning File, version: n/a, status: active
```

Displays the version of the newly installed software.

Examples

The initial part of the example shows the consolidated package, c8kg2be-universalk9.17.15.03.SPA.bin , being copied to the TFTP server. This is a prerequisite step. The remaining part of the example shows the consolidated file, packages.conf, being booted.

```
Router# copy tftp:c8kg2be-universalk9.17.15.03.SPA.bin bootflash:
address or name of remote host []? 203.0.113.6
```

```
Destination filename [c8kg2be-universalk9.17.15.03.SPA.bin]
Accessing tftp://10.124.19.169/c8kg2be-universalk9.17.15.03a.SPA.bin...
Loading
Router# show version
Cisco IOS XE Software, Version BLD_V1718_THROTTLE_LATEST_20250513_033132_V17_18_0_38
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Experimental
 Version 17.18.20250513:042531
[BLD_V1718_THROTTLE_LATEST_20250513_033132:/nobackup/mcpre/s2c-build-ws 101]
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Mon 12-May-25 21:26 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: v17.15(1.19d).s2.cp.RSA2K
Crestone-1 uptime is 4 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "bootflash:c8kg2be-universalk9.17.18.01.0.700_V17_18_0_38.SSA.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  Subscription advantage          advantage

The current crypto throughput level is 10000 kbps (Aggregate)


Smart Licensing Status: Smart Licensing Using Policy

cisco C8375-E-G2 (1RU) processor with 3703488K/6147K bytes of memory.
Processor board ID FDO2721M02R
Router operating mode: Autonomous
```

```
1 Virtual Ethernet interface
4 Gigabit Ethernet interfaces
4 2.5 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Configuration register is 0x3922


Router# dir bootflash:
Directory of bootflash:/
23       -rw-                0  May 25 2025 18:20:03 +00:00  iox_alt_hdd.dsk

784897  drwx          3358720  May 25 2025 18:10:38 +00:00  tracelogs

392449  drwx             4096  May 21 2025 09:22:30 +00:00  .rollback_timer

11       -rw-              422  May 21 2025 09:12:33 +00:00  .iox_dir_list

915713  drwx             4096  May 21 2025 09:12:13 +00:00  SHARED-IOX

21       -rw-               30  May 21 2025 09:12:12 +00:00  throughput_monitor_params

15       -rw-           143041  May 21 2025 09:12:04 +00:00  memleak.tcl

1046531  drwx            73728  May 21 2025 09:12:00 +00:00  license_evlog

1046529  drwx             4096  May 21 2025 09:11:53 +00:00  .prst_sync

12       -rwx           261921  May 21 2025 09:11:47 +00:00  mode_event_log

59       -rw-             7762  May 21 2025 09:09:09 +00:00  packages.conf

48       -rw-             7762  May 21 2025 09:04:42 +00:00
c8kg2be-universalk9.17.15.03a.SPA.conf
1047801  -rw-       59995452  May 21 2025 09:04:39 +00:00  c8kg2be-rpboot.17.15.03a.SPA.pkg

1046537  drwx             4096  May 21 2025 09:04:38 +00:00  .images

130817  drwx             4096  May 21 2025 09:01:56 +00:00  sysboot

47       -rw-             9391  May 21 2025 08:59:39 +00:00
c8kg2be-universalk9.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.conf

1047773  -rw-         59995512  May 21 2025 08:59:38 +00:00
c8kg2be-rpboot.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg

785553  drwx             4096  May 21 2025 06:27:34 +00:00  memaudit_log

13       drwx             4096  May 19 2025 03:58:14 +00:00  core

46       -rw-       1003589796  May 14 2025 11:21:03 +00:00
c8kg2be-universalk9.BLD_V1718_THROTTLE_LATEST_20250423_010128.SSA.bin

45       -rw-              396  May 14 2025 05:39:34 +00:00  ct_persistent.txt

44       -rw-             7711   May 6 2025 08:36:06 +00:00
c8kg2be-universalk9.17.15.03.SPA.conf
1047740  -rw-        59987868   May 6 2025 08:36:03 +00:00  c8kg2be-rpboot.17.15.03.SPA.pkg

24       -rw-        953199576   May 6 2025 07:02:50 +00:00
c8kg2be-universalk9.17.15.03.SPA.bin
```

```
Router# show platformChassis type: C8375-E-G2

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C8375-E-G2          ok                    00:05:25
 0/0      4M-2xSFP+           ok                    00:04:20
 0/1      C-NIM-4X            ok                    00:04:20
1         C-SM-NIM-ADPT       ok                    00:04:24
 1/0      C-NIM-WAN-2X        ok                    00:04:10
 1/1      C-NIM-WAN-4S        ok                    00:04:09
R0        C8375-E-G2          ok, active            00:05:25
F0        C8375-E-G2          ok, active            00:05:25
P0        PWR-CC1-400WAC      ok                    00:04:42
P1        Unknown             empty                 never
P2        C8300-FAN-1R        ok                    00:04:41

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         2408272B            v17.15(1.19d).s2.cp.RSA2K
1         2408272B            v17.15(1.19d).s2.cp.RSA2K
R0        2408272B            v17.15(1.19d).s2.cp.RSA2K
F0        2408272B            v17.15(1.19d).s2.cp.RSA2K
```

```
Router# mkdir bootflash:c8kg2be-universalk9.17.15.03.dir1
Create directory filename [c8kg2be-universalk9.17.15.03.dir1]?
Created dir bootflash:/c8kg2be-universalk9.17.15.03.dir1
Router# request platform software package expand file
bootflash:c8kg2be-universalk9.17.15.03.SPA.bin
to c8kg2be-universalk9.17.15.03.dir1
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# reload
Proceed with reload? [confirm]

*Jul 13 19:39:06.354: %SYS-5-RELOAD: Reload requested by console.Reload Reason: Reload
Command.

rommon 1 > boot bootflash:c8kg2be-universalk9.17.15.03.dir1/packages.conf

File size is 0x00002836
Located c8kg2be-universalk9.17.15.03.dir1/packages.conf
Image size 10294 inode num 324484, bks cnt 3 blk size 8*512
#
File is comprised of 1 fragments (33%)

is_valid_sha1hash: SHA-1 hash:
calculated 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
expected 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
File size is 0x04b3dc00
Located
c8kg2be-universalk9.17.15.03.dir1/c8kg2be-rpboot.BLD_V1715_THROTTLE_LATEST_20250310_183113.SSA.pkg
Image size 78896128 inode num 324491, bks cnt 19262 blk size 8*512
##########################################################################################
File is comprised of 21 fragments (0%)
.....
```

```
Router# show version installedPackage: Provisioning File, version: n/a, status: active
```

```
  Role: provisioning file
  File: bootflash:sysboot/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 13ee655632f92cd539d7df87a3e2a0a063262948

Package: mono-universalk9, version: 17.15.03, status: active
  Role: rp_base
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: rpboot, version: 17.15.03, status: active
  Role: rp_boot
  File: bootflash:sysboot/c8kg2be-rpboot.17.15.03.SPA.pkg, on: RP0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: n/a

Package: firmware_ngwic_t1e1, version: 17.15.03, status: active
  Role: firmware_ngwic_t1e1
  File: bootflash:sysboot/c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 5d6f62fee606718d1d0fd21ae58172ebe612862c

Package: firmware_nim_async, version: 17.15.03, status: active
  Role: firmware_nim_async
  File: bootflash:sysboot/c8kg2be-firmware_nim_async.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 2e4fdb72b80e6b6899c6b7d534b1fd5694935810

Package: firmware_nim_shdsl, version: 17.15.03, status: active
  Role: firmware_nim_shdsl
  File: bootflash:sysboot/c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: f828bfa1261d76d3f21ff7d111fe26a3eb945433

Package: firmware_nim_xdsl, version: 17.15.03, status: active
  Role: firmware_nim_xdsl
  File: bootflash:sysboot/c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 41feadbead77fa101ca313348c71e594b54ff1a8

Package: firmware_prince, version: 17.15.03, status: active
  Role: firmware_prince
  File: bootflash:sysboot/c8kg2be-firmware_prince.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 9a95bbd18f7a9034050cae14106cac63e2ec4fc6

Package: firmware_sm_1t3e3, version: 17.15.03, status: active
  Role: firmware_sm_1t3e3
  File: bootflash:sysboot/c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: cb2d7a6f125023324f62c4ea65927305c0598332

Package: firmware_sm_async, version: 17.15.03, status: active
  Role: firmware_sm_async
  File: bootflash:sysboot/c8kg2be-firmware_sm_async.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 26f7a208998aaf2fdfd505e4c507be9a724560bb

Package: firmware_sm_nim_adpt, version: 17.15.03, status: active
  Role: firmware_sm_nim_adpt
  File: bootflash:sysboot/c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 3027103a036655ea42ae1428e6b854069483d692
```

```
Package: mono-universalk9, version: 17.15.03, status: active
  Role: rp_daemons
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: active
  Role: rp_iosd
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: active
  Role: rp_security
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: active
  Role: rp_webui
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: firmware_ngwic_t1e1, version: 17.15.03, status: n/a
  Role: firmware_ngwic_t1e1
  File: bootflash:sysboot/c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg, on: RP0/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 5d6f62fee606718d1d0fd21ae58172ebe612862c

Package: firmware_nim_async, version: 17.15.03, status: n/a
  Role: firmware_nim_async
  File: bootflash:sysboot/c8kg2be-firmware_nim_async.17.15.03.SPA.pkg, on: RP0/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 2e4fdb72b80e6b6899c6b7d534b1fd5694935810

Package: firmware_nim_shdsl, version: 17.15.03, status: n/a
  Role: firmware_nim_shdsl
  File: bootflash:sysboot/c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg, on: RP0/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: f828bfa1261d76d3f21ff7d111fe26a3eb945433

Package: firmware_nim_xdsl, version: 17.15.03, status: n/a
  Role: firmware_nim_xdsl
  File: bootflash:sysboot/c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg, on: RP0/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 41feadbead77fa101ca313348c71e594b54ff1a8

Package: firmware_prince, version: 17.15.03, status: n/a
  Role: firmware_prince
  File: bootflash:sysboot/c8kg2be-firmware_prince.17.15.03.SPA.pkg, on: RP0/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 9a95bbd18f7a9034050cae14106cac63e2ec4fc6

Package: firmware_sm_1t3e3, version: 17.15.03, status: n/a
  Role: firmware_sm_1t3e3
  File: bootflash:sysboot/c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg, on: RP0/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: cb2d7a6f125023324f62c4ea65927305c0598332

Package: firmware_sm_async, version: 17.15.03, status: n/a
  Role: firmware_sm_async
  File: bootflash:sysboot/c8kg2be-firmware_sm_async.17.15.03.SPA.pkg, on: RP0/1
```

```
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 26f7a208998aaf2fdfd505e4c507be9a724560bb

  Package: firmware_sm_nim_adpt, version: 17.15.03, status: n/a
    Role: firmware_sm_nim_adpt
    File: bootflash:sysboot/c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg, on: RP0/1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 3027103a036655ea42ae1428e6b854069483d692

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_daemons
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0/1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_iosd
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0/1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_security
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0/1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_webui
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP0/1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_base
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: rpboot, version: 17.15.03, status: n/a
    Role: rp_boot
    File: bootflash:sysboot/c8kg2be-rpboot.17.15.03.SPA.pkg, on: RP1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: n/a

  Package: firmware_ngwic_t1e1, version: 17.15.03, status: n/a
    Role: firmware_ngwic_t1e1
    File: bootflash:sysboot/c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 5d6f62fee606718d1d0fd21ae58172ebe612862c

  Package: firmware_nim_async, version: 17.15.03, status: n/a
    Role: firmware_nim_async
    File: bootflash:sysboot/c8kg2be-firmware_nim_async.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 2e4fdb72b80e6b6899c6b7d534b1fd5694935810

  Package: firmware_nim_shdsl, version: 17.15.03, status: n/a
    Role: firmware_nim_shdsl
    File: bootflash:sysboot/c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: f828bfa1261d76d3f21ff7d111fe26a3eb945433

  Package: firmware_nim_xdsl, version: 17.15.03, status: n/a
    Role: firmware_nim_xdsl
    File: bootflash:sysboot/c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 41feadbead77fa101ca313348c71e594b54ff1a8

  Package: firmware_prince, version: 17.15.03, status: n/a
    Role: firmware_prince
    File: bootflash:sysboot/c8kg2be-firmware_prince.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 9a95bbd18f7a9034050cae14106cac63e2ec4fc6

  Package: firmware_sm_1t3e3, version: 17.15.03, status: n/a
    Role: firmware_sm_1t3e3
    File: bootflash:sysboot/c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: cb2d7a6f125023324f62c4ea65927305c0598332

  Package: firmware_sm_async, version: 17.15.03, status: n/a
    Role: firmware_sm_async
    File: bootflash:sysboot/c8kg2be-firmware_sm_async.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 26f7a208998aaf2fdfd505e4c507be9a724560bb

  Package: firmware_sm_nim_adpt, version: 17.15.03, status: n/a
    Role: firmware_sm_nim_adpt
    File: bootflash:sysboot/c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 3027103a036655ea42ae1428e6b854069483d692

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_daemons
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_iosd
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_security
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: mono-universalk9, version: 17.15.03, status: n/a
    Role: rp_webui
    File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1/0
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

  Package: firmware_ngwic_t1e1, version: 17.15.03, status: n/a
    Role: firmware_ngwic_t1e1
    File: bootflash:sysboot/c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg, on: RP1/1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 5d6f62fee606718d1d0fd21ae58172ebe612862c

  Package: firmware_nim_async, version: 17.15.03, status: n/a
    Role: firmware_nim_async
    File: bootflash:sysboot/c8kg2be-firmware_nim_async.17.15.03.SPA.pkg, on: RP1/1
    Built: 2025-03-25_23.43, by: mcpre
    File SHA1 checksum: 2e4fdb72b80e6b6899c6b7d534b1fd5694935810
```

```
Package: firmware_nim_shdsl, version: 17.15.03, status: n/a
  Role: firmware_nim_shdsl
  File: bootflash:sysboot/c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: f828bfa1261d76d3f21ff7d111fe26a3eb945433

Package: firmware_nim_xdsl, version: 17.15.03, status: n/a
  Role: firmware_nim_xdsl
  File: bootflash:sysboot/c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 41feadbead77fa101ca313348c71e594b54ff1a8

Package: firmware_prince, version: 17.15.03, status: n/a
  Role: firmware_prince
  File: bootflash:sysboot/c8kg2be-firmware_prince.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 9a95bbd18f7a9034050cae14106cac63e2ec4fc6

Package: firmware_sm_1t3e3, version: 17.15.03, status: n/a
  Role: firmware_sm_1t3e3
  File: bootflash:sysboot/c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: cb2d7a6f125023324f62c4ea65927305c0598332

Package: firmware_sm_async, version: 17.15.03, status: n/a
  Role: firmware_sm_async
  File: bootflash:sysboot/c8kg2be-firmware_sm_async.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 26f7a208998aaf2fdfd505e4c507be9a724560bb

Package: firmware_sm_nim_adpt, version: 17.15.03, status: n/a
  Role: firmware_sm_nim_adpt
  File: bootflash:sysboot/c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: 3027103a036655ea42ae1428e6b854069483d692

Package: mono-universalk9, version: 17.15.03, status: n/a
  Role: rp_daemons
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: n/a
  Role: rp_iosd
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: n/a
  Role: rp_security
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: n/a
  Role: rp_webui
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: RP1/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: active
  Role: fp
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: ESP0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: fp, version: unknown, status: n/a
  Role: fp
  File: unknown, on: ESP1
  Built: unknown, by: unknown
  File SHA1 checksum: unknown

Package: mono-universalk9, version: 17.15.03, status: active
  Role: cc_spa
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: SIP0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: active
  Role: cc
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: SIP0/0
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: mono-universalk9, version: 17.15.03, status: active
  Role: cc
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: SIP0/1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec

Package: cc, version: unknown, status: n/a
  Role: cc
  File: unknown, on: SIP0/2
  Built: unknown, by: unknown
  File SHA1 checksum: unknown

Package: cc, version: unknown, status: n/a
  Role: cc
  File: unknown, on: SIP0/3
  Built: unknown, by: unknown
  File SHA1 checksum: unknown

Package: cc, version: unknown, status: n/a
  Role: cc
  File: unknown, on: SIP0/4
  Built: unknown, by: unknown
  File SHA1 checksum: unknown

Package: cc, version: unknown, status: n/a
  Role: cc
  File: unknown, on: SIP0/5
  Built: unknown, by: unknown
  File SHA1 checksum: unknown

Package: mono-universalk9, version: 17.15.03, status: active
  Role: cc_spa
  File: bootflash:sysboot/c8kg2be-mono-universalk9.17.15.03.SPA.pkg, on: SIP1
  Built: 2025-03-25_23.43, by: mcpre
  File SHA1 checksum: d03cbeaae0843eeb59138276c67627521e9ffaec
```

Installing subpackages from a consolidated package on a flash drive

The steps for installing subpackages from a consolidated package on a USB flash drive are similar to those described in Installing Subpackages from a Consolidated Pacakage section .

Procedure

Step 1 **show version**

Step 2 **dir usb***n***:**

Step 3 **show platform**

Step 4 **mkdir bootflash:***URL-to-directory-name*

Step 5 **request platform software package expand fileusb***n***:** ***package-name to URL-to-directory-name***

Step 6 **reload**

Step 7 **boot** *URL-to-directory-name/***packages.conf**

Step 8 **show version installed**

Installing a firmware subpackage

Before you begin

Obtain a consolidated package that contains your required firmware package and expand the package. (See Manage and Configure a device to run using individual packages, on page 93.) Make a note of the location and name of the firmware package and use this information in the steps below for *URL-to-package-name*.

You can install a firmware subpackage if the device has been configured using, for example, Manage and Configure a device to run using individual packages, on page 93.

Firmware subpackages are not released individually. You can select a firmware package from within a consolidated package after expanding the consolidated package. The firmware package can then be installed as shown in the procedure below.

Note Read the Release Notes document pertaining to the consolidated package to verify that the firmware within the consolidated package is compatible with the version of Cisco IOS XE software that is currently installed on a device.

Procedure

Step 1 **show version**

Example:

```
Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
15.3(20120627:221639) [build_151722 111]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 28-Jun-12 15:17 by mcpre
.
```

```
.
.
```

Shows the version of software running on the device. This can later be compared with the version of software to be installed.

Step 2 **dir bootflash:**

Example:

```
Router# dir bootflash:
```

Displays the previous version of software and that a package is present.

Step 3 **show platform**

Example:

```
Router# show platform
Chassis type: C8375-E-G2
```

Checks the inventory.

Also see the example in Installing Subpackages from a Consolidated Package section.

Step 4 **mkdir bootflash:** *URL-to-directory-name*

Example:

```
Router# mkdir bootflash:mydir
```

Creates a directory to save the expanded software image.

You can use the same name as the image to name the directory.

Step 5 **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*

Example:

```
Router#   request platform software package expand file
bootflash:c8kg2be-universalk9.17.15.03.SPA.bin:mydir
```

Expands the software image from the TFTP server (*URL-to-consolidated-package*) into the directory used to save the image (*URL-to-directory-name*), which was created in the Step 4.

Step 6 **reload**

Example:

```
Router# reload
rommon >
```

Enables ROMMON mode, which allows the software in the consolidated file to be activated.

Step 7 **boot** *URL-to-directory-name* **/packages.conf**

Example:

```
rommon 1 > boot bootflash:mydir/packages.conf
```

Boots the consolidated package by specifying the path and name of the provisioning file: packages.conf.

Step 8 **show version installed**

Example:

```
Router# show version installed
Package: Provisioning File, version: n/a, status: active
```

Displays the version of the newly installed software.

Examples

The initial part of the following example shows the consolidated package, c8kg2be-universalk9.17.15.03.SPA.bin, being copied to the TFTP server. This is a prerequisite step. The remaining part of the example shows the consolidated file, packages.conf, being booted.

```
Router#request platform software package expand file
bootflash:c8kg2be-universalk9.17.15.03.SPA.bin to bootflash:c8kg2be
Verifying parameters
Expanding superpackage bootflash:c8kg2be-universalk9.17.15.03.SPA.bin
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#do dir bootflash:c8kg2be
Directory of bootflash:/c8kg2be/

52      -rw-             7711   Jun 6 2025 07:39:20 +00:00  packages.conf
82      -rw-         59987868   Jun 6 2025 07:39:20 +00:00  c8kg2be-rpboot.17.15.03.SPA.pkg
81      -rw-        891219968   Jun 6 2025 07:38:50 +00:00
c8kg2be-mono-universalk9.17.15.03.SPA.pkg
80      -rw-           204800   Jun 6 2025 07:38:33 +00:00
c8kg2be-firmware_sm_nim_adpt.17.15.03.SPA.pkg
79      -rw-         14671872   Jun 6 2025 07:38:33 +00:00
c8kg2be-firmware_sm_async.17.15.03.SPA.pkg
77      -rw-         10444800   Jun 6 2025 07:38:32 +00:00
c8kg2be-firmware_prince.17.15.03.SPA.pkg
73      -rw-         11804672   Jun 6 2025 07:38:32 +00:00
c8kg2be-firmware_nim_shdsl.17.15.03.SPA.pkg
67      -rw-         13254656   Jun 6 2025 07:38:32 +00:00
c8kg2be-firmware_nim_async.17.15.03.SPA.pkg
61      -rw-         11956224   Jun 6 2025 07:38:32 +00:00
c8kg2be-firmware_ngwic_t1e1.17.15.03.SPA.pkg
78      -rw-         13889536   Jun 6 2025 07:38:32 +00:00
c8kg2be-firmware_sm_1t3e3.17.15.03.SPA.pkg
76      -rw-          5677056   Jun 6 2025 07:38:32 +00:00
c8kg2be-firmware_nim_xdsl.17.15.03.SPA.pkg

20237881344 bytes total (0 bytes free)
Router(config)#boot system bootflash:c8kg2be/packages.conf
Router(config)#end
Router#wr
Building configuration...
[OK]
Router#reload
Proceed with reload? [confirm]
Jun  6 07:44:50.27

System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.


Current image running: Boot ROM0
```

```
Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory


........

boot: reading file packages.conf
#

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

Performing Signature Verification of OS image...
Image validated

Jun  6 07:46:41.428: %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], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 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.
```

```
Jun  6 07:46:45.004: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota exceeded
 [free space is 115824 kB] - [recommended free space is 5929066 kB] - Please clean up files
 on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906887K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.
No processes could be found for the command

 WARNING: Command has been added to the configuration using a type 0 password. However,
recommended to migrate to strong type-6 encryption

 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!
```

Configuring No Service Password-Recovery

The Cisco IOS password recovery procedure allows you to to gain access, using the console, to the ROMMON mode by using the Break key during system startup and reload. When the device software is loaded from ROMMON mode, the configuration is updated with the new password. The password recovery procedure makes anyone with console access have the ability to access the device and its network.

The No Service Password-Recovery feature is designed to prevent the service password-recovery procedure from being used to gain access to the device and network.

Configuration registers and system boot configuration

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the device boots manually from ROM or automatically from flash or the network. For example, when the configuration register boot field value is set to any value from 0x2 to 0xF, the device uses the register boot field value to form a default boot filename for autobooting from a network server.

Bit 8, when set to 1, ignores the startup configuration. Bit 6, when set to 1, enables break key detection. You must set the configuration register to autoboot to enable this feature. Any other configuration register setting will prevent the feature from being enabled.

Note By default, the no confirm prompt and messages are not displayed after reloads.

How to enable No Service Password-Recovery

You can enable the No Service Password-Recovery in the following two ways:

- Using the **no service password-recovery** command. This option allows password recovery once it is enabled.
- Using the **no service password-recovery strict** command. This option does not allow for device recovery once it is enabled.

Note As a precaution, a valid Cisco IOS image should reside in the bootflash: before this feature is enabled.

If you plan to enter the no service password-recovery command, Cisco recommends that you save a copy of the system configuration file in a location away from the device.

Befor you beging, ensure that this feature is disabled before making any change to the device regardless of the significance of the change—such as a configuration, module, software version, or ROMMON version change.

The configuration register boot bit must be enabled to load the startup configuration by setting bit-8 to 0, to ignore the break key in Cisco IOS XE by setting bit-6 to 0, and to auto boot a Cisco IOS XE image by setting the lowest four bits 3-0, to any value from 0x2 to 0xF. Changes to the configuration register are not saved after the No Service Password-Recovery feature is enabled.

Note If Bit-8 is set to 1, the startup configuration is ignored. If Bit-6 is set to 1, break key detection is enabled in Cisco IOS XE. If both Bit-6 and Bit-8 are set to 0, the No Service Password-Recovery feature is enabled.

This example shows how to enable the No Service Password-Recovery feature:

```
Router> enable
Router# show version
Router# configure terminal
Router(config)# config-register 0x2012
Router(config)# no service password-recovery
Router(config)# exit
```

Recovering a Device with the No Service Password-Recovery Feature Enabled

To recover a device after the no service password-recovery feature is enabled using the **no service password-recovery** command, look out for the following message that appears during the boot: “PASSWORD RECOVERY FUNCTIONALITY IS DISABLED.” As soon as “.. ” appears, press the Break key. You are then prompted to confirm the Break key action:

- If you confirm the action, the startup configuration is erased and the device boots with the factory default configuration with the No Service Password-Recovery enabled.

- If you do not confirm the Break key action, the device boots normally with the No Service Password-Recovery feature enabled.

Note You cannot recover a device if the No Service Password-Recovery feature was enabled using the **no service password-recovery strict** command.

This example shows a Break key action being entered during boot up, followed by confirmation of the break key action. The startup configuration is erased and the device then boots with the factory default configuration with the No Service Password-Recovery feature enabled.

```
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly


System Bootstrap, Version 17.3(1r), RELEASE SOFTWARE
Copyright (c) 1994-2020  by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory


PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

..

telnet> send brk

..

PASSWORD RECOVERY IS DISABLED.

Do you want to reset the router to the factory default
configuration and proceed [y/n] ? y

Router clearing configuration. Please wait for ROMMON prompt...

File size is 0x17938a80

Located c8kg2be-universalk9.BLD_V1718_THROTTLE_LATEST_20250423_010128.SSA.bin

...
```

This example shows a Break key action being entered during boot up, followed by the non-confirmation of the break key action. The device then boots normally with the No Service Password-Recovery feature enabled.

```
Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.

Current image running: Boot ROM0
```

```
Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

..

telnet> send brk

...

PASSWORD RECOVERY IS DISABLED.

Do you want to reset the router to the factory default
configuration and proceed [y/n] ? n

Router continuing with existing configuration...

File size is 0x17938a80

Located c8kg2be-universalk9.BLD_V1718_THROTTLE_LATEST_20250423_010128.SSA.bin


...

######################################################################## …
```

Configuration Examples for No Service Password-Recovery

The following example shows how to obtain the configuration register setting (which is set to autoboot), disable password recovery capability, and then verify that the configuration persists through a system reload:

```
Router>en
Router#show version
Cisco IOS XE Software, Version 17.15.03
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 by xxxx

Router(config)#no service password-recovery
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
Router(config)#end
Router#wr
Building configuration...
[OK]
Router#reload
Proceed with reload? [confirm]
Jun  9

System integrity status: 0x32042000
Rom image verified correctly

System Bootstrap, Version v17.15(3.1r).s2.cp, RELEASE SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.
```

```
Current image running: Boot ROM0

Last reset cause: LocalSoft
C8375-E-G2 platform with 33554432 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

.
telnet> send brk
.....


PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to the factory default
configuration and proceed  y/n [n]: n

Router continuing with existing configuration...

boot: reading file packages.conf
###########################################################

Performing Signature Verification of OS image...
Image validated

Jun  9 05:40:13.287: %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], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.15.3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Tue 25-Mar-25 23:37 by xxxx


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.


Jun  9 05:40:16.793: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: bootflash quota exceeded
 [free space is 115484 kB] - [recommended free space is 5929066 kB] - Please clean up files
 on bootflash.
cisco C8375-E-G2 (1RU) processor with 11906887K/6147K bytes of memory.
Processor board ID FDO2833M01A
Router operating mode: Autonomous
1 Virtual Ethernet interface
12 2.5 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
33554432K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Warning: When Cisco determines that a fault or defect can be traced to
the use of third-party transceivers installed by a customer or reseller,
then, at Cisco's discretion, Cisco may withhold support under warranty or
a Cisco support program. In the course of providing support for a Cisco
networking product Cisco may require that the end user install Cisco
transceivers if Cisco determines that removing third-party parts will
assist Cisco in diagnosing the cause of a support issue.
No processes could be found for the command

 WARNING: Command has been added to the configuration using a type 0 password. However,
recommended to migrate to strong type-6 encryption

 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!
```

The following example shows how to disable password recovery capability using the no service password-recovery strict command:

```
Router# configure terminal

Router(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
Router(config)#end
Router#wr
Building configuration...
[OK]
..
```

CHAPTER 7

Interface configuration

This chapter contains information on interface configuration. The slots specify the chassis slot number in your device and subslots specify the slot where the service modules are installed.

For further information on the slots and subslots, see the “About Slots and Interfaces” sections:

- Hardware Installation Guide for Cisco 8300 Series Secure Routers

These section is included in this chapter:

Configure the interfaces

These sections describe how to configure Gigabit interfaces and also provide examples of configuring the router interfaces:

Configure Gigabit Ethernet interfaces

Procedure

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 TwoGigabitEthernet** *slot/subslot/port*

Example:

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

Configures a GigabitEthernet interface.

- **TwoGigabitEthernet**—Type of interface.
- *slot*—Chassis slot number.
- */subslot*—Secondary slot number. The slash (/) is required.
- /port—Port or interface number. The slash (/) is required.

Step 4 **ip address** *ip-address mask* [**secondary**] **dhcp pool**

Example:

```
Router(config-if)# ip address 10.0.0.1 255.255.255.0 dhcp pool
```

Assigns an IP address to the GigabitEthernet

- **ip address** *ip-address*—IP address for the interface.
- *mask*—Mask for the associated IP subnet.
- **secondary** (optional)—Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
- **dhcp**—IP address negotiated via DHCP.
- **pool**—IP address autoconfigured from a local DHCP pool.

Step 5 **negotiation auto**

Example:

```
Router(config-if)# negotiation auto
```

Selects the negotiation mode.

- **auto**—Performs link autonegotiation.

Step 6 **end**

Example:

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

Ends the current configuration session and returns to privileged EXEC mode.

Configure the interfaces: Example

This example shows the **interface TwogigabitEthernet** command being used to add the interface and set the IP address. **0/0/1** is the slot/subslot/port. The ports are numbered 0 to 5.

```
Router# show running-config interface TwogigabitEthernet 0/0/1
Building configuration...
Current configuration : 108 bytes
!
interface TwoGigabitEthernet0/0/1
no ip address
shutdown
negotiation auto
mka policy priority100
end
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface TwogigabitEthernet 0/0/1
```

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.

View a list of all interfaces: Example

In this example, the **show interfaces summary**, and **show platform software status control-process brief** commands are used to display all the interfaces for C8375-E-G2:

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

 Tw0/0/0                       0         0         0         0         0         0
 0         0         0
 Tw0/0/1                       0         0         0         0         0         0
 0         0         0
 Tw0/0/2                       0         0         0         0         0         0
 0         0         0
*Tw0/0/3                       0         0         0         0         0         0
 0         0         0
```

```
*Tw0/0/3.10                   -         -         -         -         -         -
 -         -         -
*Te0/0/4                      0         0         0         0         0         0
 0         0         0
*Te0/0/4.10                   -         -         -         -         -         -
 -         -         -
*Te0/0/5                      0         0         0         0         0         0
 0         0         0
*Te0/0/5.10                   -         -         -         -         -         -
 -         -         -
 Tw0/1/0                      0         0         0         0         0         0
 0         0         0
 Tw0/1/1                      0         0         0         0         0         0
 0         0         0
 Tw0/1/2                      0         0         0         0         0         0
 0         0         0
 Tw0/1/3                      0         0         0         0         0         0
 0         0         0
 Tw0/1/4                      0         0         0         0         0         0
 0         0         0
 Tw0/1/5                      0         0         0         0         0         0
 0         0         0
*Tw0/1/6                      0         0         0         0         0         0
 0         0         0
*Tw0/1/7                      0         0         0         0         0         0
 0         0         0
*Tw0/1/7.10                   -         -         -         -         -         -
 -         -         -
*Service-Engine0/4/0          0         0         0         0         0         0
 0         0         0
*GigabitEthernet0             0         0         0         0      2000         3
 0         0         0
*Tunnel0                      0         0         0         3         0         0
 0         0         0
*VirtualPortGroup0            0         0         0         0         0         0
 0         0         0
*VirtualPortGroup1            0         0         0         0      4000         4
3000         4         0
*VirtualPortGroup10           0         0         0         0         0         0
 0         0         0
 Vlan1                        0         0         0         0         0         0
 0         0         0
NOTE:No separate counters are maintained for subinterfaces

Hence Details of subinterface are not shown


Router#show platform software status control-process brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.83   0.91   0.91

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  7768456  2654936 (34%)  5113520 (66%)   3115212 (40%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   2.70   1.70   0.00  95.59   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   2.40   1.40   0.00  96.19   0.00   0.00   0.00
         5   0.80   1.60   0.00  97.59   0.00   0.00   0.00
         6  12.40  12.30   0.00  75.30   0.00   0.00   0.00
         7  11.20  12.40   0.00  76.40   0.00   0.00   0.00
         8   2.80   1.80   0.00  95.40   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
```

View information about an interface: Example

This 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 for C8375-E-G2:

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

Tw0/0/0                192.168.10.1    YES NVRAM  down                  down

Tw0/0/1                unassigned      YES NVRAM  administratively down down

Tw0/0/2                192.168.11.1    YES NVRAM  down                  down

Tw0/0/3                unassigned      YES NVRAM  up                    up

Tw0/0/3.10             192.168.3.1     YES NVRAM  up                    up

Te0/0/4                unassigned      YES NVRAM  up                    up

Te0/0/4.10             192.168.4.1     YES NVRAM  up                    up

Te0/0/5                unassigned      YES NVRAM  up                    up

Te0/0/5.10             192.168.4.2     YES NVRAM  up                    up

Tw0/1/0                unassigned      YES unset  administratively down down

Tw0/1/1                unassigned      YES unset  down                  down

Tw0/1/2                unassigned      YES unset  down                  down

Tw0/1/3                unassigned      YES unset  down                  down

Tw0/1/4                unassigned      YES unset  down                  down

Tw0/1/5                unassigned      YES unset  down                  down

Tw0/1/6                192.168.22.200  YES NVRAM  up                    up

Tw0/1/7                unassigned      YES NVRAM  up                    up

Tw0/1/7.10             192.168.3.2     YES NVRAM  up                    up

Service-Engine0/4/0    unassigned      YES unset  up                    up

GigabitEthernet0       10.79.58.164    YES NVRAM  up                    up

Tunnel0                192.0.2.5       YES unset  up                    up

VirtualPortGroup0      192.0.2.1       YES NVRAM  up                    up

VirtualPortGroup1      192.0.2.5       YES NVRAM  up                    up

VirtualPortGroup10     10.88.88.1      YES NVRAM  up                    up
```

```
Vlan1                  unassigned      YES unset  up                    down
```

CHAPTER 8

Support for Security-Enhanced Linux

This chapter describes the SELinux feature, and includes the following sections:

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

Facility-Severity-Mnemonic	**%SELINUX-1-VIOLATION**
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 9

Process health monitoring

This chapter describes how to manage and monitor the health of various components of your device. It contains these sections:

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

Device 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.

Monitor bootFlash disk

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 example:

```
Aug 22 13:40:41.038 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 7084440 kB] - Please clean up files on bootflash.
```

The size of the bootflash disk must be at least of the same size as that of the physical memory installed on the device. If this condition is not met, a syslog alarm is generated as shown in the example:

```
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Flash capacity (8 GB) is insufficient for fault
analysis based on
installed memory of RP (16 GB)
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Please increase the size of installed flash to at
least 16 GB (same as
physical memory size)
```

Approaches for monitoring hardware alarms

- Onsite network administrator responds to audible or visual Alarms, on page 132
- View the console or syslog for alarm messages, on page 133
- Alarm reported through SNMP, on page 136

Onsite network administrator responds to audible or visual Alarms

- About audible and visual alarms, on page 132
- Clear an audible alarm, on page 132
- Clearing a visual alarm, on page 132

About audible and visual alarms

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

If an alarm illuminates the CRIT, MIN, or MAJ LED on the faceplate of the device, and a visual or audible alarm is wired, the alarm also activates an alarm relay in the power supply DB-25 connector, and either the bell rings or the light bulb flashes.

Clear an audible alarm

To clear an audible alarm, perform one of these tasks:

- Press the **Audible Cut Off** button on the faceplate.
- Enter the **clear facility-alarm** command.

Clearing a visual alarm

To clear a visual alarm, you must resolve the alarm condition. The **clear facility-alarm** command does not clear an alarm LED on the faceplate or turn off the DC light bulb. For example, if a critical alarm LED is illuminated because an active module was removed without a graceful deactivation, the only way to resolve that alarm is to replace the module.

View 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, on page 133
- Examples of alarm messages, on page 133
- Reviewing and Analyzing Alarm Messages, on page 136

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 when a module is removed before performing a graceful deactivation. The alarm is cleared when the module is reinserted.

Module removed

```
*Aug 22 13:27:33.774: %C-SM-X-16G4M2X: Module removed from subslot 1/1, interfaces disabled
*Aug 22 13:27:33.775: %SPA_OIR-6-OFFLINECARD: Module (SPA-4XT-SERIAL) offline in subslot
1/1
```

Module reinserted

```
*Aug 22 13:32:29.447: %CC-SM-X-16G4M2X: Module inserted in subslot 1/1
*Aug 22 13:32:34.916: %SPA_OIR-6-ONLINECARD: Module (SPA-4XT-SERIAL) online in subslot 1/1
*Aug 22 13:32:35.523: %LINK-3-UPDOWN: SIP1/1: Interface EOBC1/1, changed state to up
```

Alarms

To view alarms, use the **show facility-alarm status** command. This example shows a critical alarm for the power supply:

```
Router# show facility-alarm status
System Totals  Critical: 1  Major: 0  Minor: 0

Source                     Time                   Severity      Description [Index]
------                     ------                 --------      -------------------

Power Supply Bay 1         Jul 08 2020 11:51:34   CRITICAL      Power Supply/FAN Module
Missing [0]

POE Bay 0                  Jul 08 2020 11:51:34   INFO          Power Over Ethernet Module
```

```
 Missing [0]

POE Bay 1                  Jul 08 2020 11:51:34   INFO          Power Over Ethernet Module
 Missing [0]

xcvr container 0/0/4       Jul 08 2020 11:51:47   INFO          Transceiver Missing - Link
 Down [1]

TenGigabitEthernet0/1/0    Jul 08 2020 11:52:24   INFO         Physical Port Administrative
 State Down [2]

GigabitEthernet1/0/0      Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

GigabitEthernet1/0/1      Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

GigabitEthernet1/0/2      Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

GigabitEthernet1/0/3      Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

GigabitEthernet1/0/4      Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

GigabitEthernet1/0/5      Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

GigabitEthernet1/0/6      Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

GigabitEthernet1/0/7      Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

TwoGigabitEthernet1/0/17   Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

TwoGigabitEthernet1/0/18   Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]

TwoGigabitEthernet1/0/19   Jul 08 2020 11:56:35   INFO         Physical Port Administrative
 State Down [2]
```

To view critical alarms, use the **show facility-alarm status critical** command, as shown in this example:

```
Router# show facility-alarm status critical
System Totals  Critical: 1  Major: 0  Minor: 0

Source                     Time                   Severity      Description [Index]
------                     ------                 --------      -------------------

Power Supply Bay 1         Jul 08 2020 11:51:34   CRITICAL      Power Supply/FAN Module
Missing [0]
```

To view the operational state of the major hardware components on the device, use the **show platform diag** command.

```
Router# show platform diag
Slot: 0, C8375-E-G2
Running state               : ok
Internal state              : online
Internal operational state  : ok
Physical insert detect time : 00:00:23 (2d01h ago)
Software declared up time   : 00:01:07 (2d01h ago)
```

```
CPLD version                : 25033132
Firmware version            : v17.15(3.1r).s2.cp
Sub-slot: 0/0, 4M-2xSFP+
Operational status          : ok
Internal state              : inserted
Physical insert detect time : 00:01:17 (2d01h ago)
Logical insert detect time  : 00:01:17 (2d01h ago)
Sub-slot: 0/1, C-NIM-8M
Operational status          : ok
Internal state              : inserted
Physical insert detect time : 00:01:17 (2d01h ago)
Logical insert detect time  : 00:01:17 (2d01h ago)
Slot: 1, C8375-E-G2
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:23 (2d01h ago)
  Software declared up time   : 00:01:13 (2d01h ago)
  CPLD version                : 25033132

  Firmware version            : v17.15(3.1r).s2.cp

                                                            Slot: R0, C8375-E-G2


  Running state               : ok, active

  Internal state              : online

  Internal operational state  : ok

  Physical insert detect time : 00:00:23 (2d01h ago)

  Software declared up time   : 00:00:23 (2d01h ago)

  CPLD version                : 25033132

  Firmware version            : v17.15(3.1r).s2.cp

                                                            Slot: F0, C8375-E-G2
  Running state               : ok, active
  Internal state              : online

  Internal operational state  : ok
  Physical insert detect time : 00:00:23 (2d01h ago)
  Software declared up time   : 00:01:00 (2d01h ago)

  Hardware ready signal time  : 00:00:58 (2d01h ago)
  Packet ready signal time    : 00:01:13 (2d01h ago)

  CPLD version                : 25033132
  Firmware version            : v17.15(3.1r).s2.cp

Slot: P0, PWR-CC1-760WAC
  State                       : fail, badinput
  Physical insert detect time : 00:00:01 (2d01h ago)
Slot: P1, PWR-CC1-400WAC
  State                       : ok
  Physical insert detect time : 00:00:01 (2d01h ago)
  Slot: P2, C8300-FAN-1R
  State                       : ok
  Physical insert detect time : 00:00:02 (2d01h ago)
  Slot: POE0, PWR-CC1-760WAC
  State                       : fail, badinput
```

```
Physical insert detect time : 00:00:01 (2d01h ago)
Slot: POE1, Unknown
State                       : empty
Physical insert detect time : 00:00:00 (never ago)
```

Reviewing and Analyzing Alarm Messages

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

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

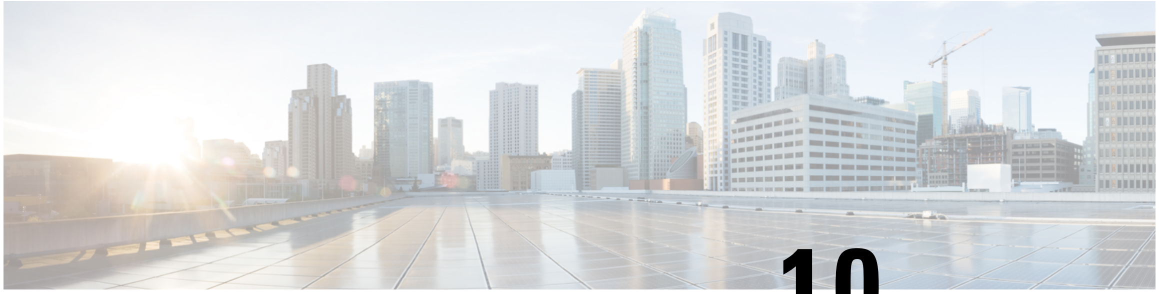
Alarm reported through SNMP

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. Of all the approaches to monitor alarms, SNMP is the best approach to monitor more than one device in an enterprise and service provider setup.

SNMP provides notification of faults, alarms, and conditions that might affect services. It allows a network administrator to access device 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, RFC 4133 (required for the CISCO-ENTITY-ALARM-MIB and CISCO-ENTITY-SENSOR-MIB to work)
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-SENSOR-MIB (for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)



CHAPTER 10

System Messages

System messages are saved in a log file or directed to other devices from the software running on a router. These messages are also known as syslog messages. System messages provide you with logging information for monitoring and troubleshooting purposes.

These sections are included in this chapter:

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 see further details about a process management or a syslog error message, see the System Error Messages Guide For Access and Edge Routers Guide.

These are examples of the description and the recommended action displayed by 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 11

Trace Management

These sections are included in this chapter:

Trace Management

Tracing is a function that logs internal events. Trace files containing trace messages are automatically created and saved to the tracelogs directory on the hard disk: file system on the router, which stores tracing files in bootflash.

The contents of trace files are useful for the following purposes:

- Troubleshooting—Helps to locate and solve an issue with a router. The trace files can be accessed in diagnostic mode even if other system issues are occurring simultaneously.
- Debugging—Helps to obtain a detailed view of system actions and operations.

How tracing works

Tracing logs the contents of internal events on a router. Trace files containing all the trace output pertaining to a module are periodically created and updated and stored in the tracelog directory. Trace files can be erased from this directory to recover space on the file system without impacting system performance. The files can be copied to other destinations using file transfer functions (such as FTP and TFTP) and opened using a plain text editor.

Note Tracing cannot be disabled on a router.

Use these commands to view trace information and set tracing levels:

- **show logging process module**—Shows the most recent trace information for a specific module. This command can be used in privileged EXEC and diagnostic modes. When used in diagnostic mode, this command can gather trace log information during a Cisco IOS XE failure.
- **set platform software trace**—Sets a tracing level that determines the types of messages that are stored in the output. For more information on tracing levels, see Tracing levels, on page 146.

Configure Packet Tracer with UDF offset

Perform these steps to configure the Packet-Trace UDF with offset:

Procedure

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 **udf** *udf name* **header** {**inner** | **outer**} {**13**|**14**} **offset** *offset-in-bytes* **length** *length-in-bytes*

Example:

```
Router(config)# udf TEST_UDF_NAME_1 header  inner l3 64 1


Router(config)# udf TEST_UDF_NAME_2 header  inner l4 77 2


Router(config)# udf TEST_UDF_NAME_3 header outer l3 65 1

Router(config)# udf TEST_UDF_NAME_4 header outer l4 67 1
```

Configures individual UDF definitions. You can specify the name of the UDF, the networking header from which offset, and the length of data to be extracted.

The **inner** or **outer** keywords indicate the start of the offset from the unencapsulated Layer 3 or Layer 4 headers, or if there is an encapsulated packet, they indicate the start of offset from the inner L3/L4.

The **length** keyword specifies, in bytes, the length from the offset. The range is from 1 to 2.

.

Step 4 **udf** *udf name* {**header** | **packet-start**} *offset-base offset length*

Example:

```
Router(config)# udf TEST_UDF_NAME_5 packet-start 120 1
```

- header—Specifies the offset base configuration.
- packet-start—Specifies the offset base from packet-start. packet-start" can vary depending on if packet-trace is for an inbound packet or outbound packet. If the packet-trace is for an inbound packet then the packet-start will be layer2. For outbound, he packet-start will be layer3.
- offset—Specifies the number of bytes offset from the offset base. To match the first byte from the offset base (Layer 3/Layer 4 header), configure the offset as 0.
- length—Specifies the number of bytes from the offset. Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs.

Step 5 **ip access-list extended** {*acl-name* |*acl-num*}

Example:

```
Router(config)# ip access-list extended acl2
```

Enables extended ACL configuration mode. The CLI enters the extended ACL configuration mode in which all subsequent commands apply to the current extended access list. Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL.

Step 6 **ip access-list extended { deny | permit } udf udf-name value mask**

Example:

```
Router(config-acl)# permit ip any any udf TEST_UDF_NAME_5 0xD3 0xFF
```

Configures the ACL to match on UDFs along with the current access control entries (ACEs) . The bytes defined in ACL is 0xD3. Masks are used with IP addresses in IP ACLs to specify what should be permitted and denied.

Step 7 **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 gi0/0/0 ipv4 access-list acl2 both
```

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 8 **debug platform condition start**

Example:

```
Router# debug platform condition start
```

Enables the specified matching criteria and starts packet tracing.

Step 9 **debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]**

Example:

```
Router# debug platform packet-trace packet 1024 fia-trace data-size 2048
```

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 10 **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 11 **debug platform condition stop**

Example:

```
Router# debug platform condition start
```

Deactivates the condition and stops packet tracing.

Step 12 **exit**

Example:

```
Router# exit
```

Exits the privileged EXEC mode.

Tracing levels

Tracing levels determine how much information should be stored about a module in the trace buffer or file.

The table shows all the tracing levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

Table 12: Tracing levels and descriptions

Tracing Level	Level Number	Description
Emergency	0	The message is regarding an issue that makes the system unusable.

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

If a tracing level is set, messages are collected from both lower tracing levels and from its own level.

For example, setting the tracing level to 3 (error) means that the trace file will contain output messages for levels: 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error).

If you set the trace level to 4 (warning), it results in output messages for levels: 0 (emergencies), 1 (alerts), 2 (critical), 3 (error), and 4 (warning).

The default tracing level for every module on the router is 5 (notice).

A tracing level is not set in a configuration mode, which results in tracing-level settings being returned to default values after the router reloads.

Caution Setting the tracing level of a module to debug level or higher can have a negative impact on the performance.

Caution Setting high tracing levels on a large number of modules can severely degrade performance. If a high tracing level is required in a specific context, it is almost always preferable to set the tracing level of a single module to a higher level rather than setting multiple modules to high levels.

View tracing level

By default, all the modules on a router are set to 5 (notice). This setting is maintained unless changed by a user.

To see the tracing level for a module on a router, enter the **show logging process** command in privileged EXEC mode or diagnostic mode.

This example shows how the **show logging process** command is used to view the tracing levels of the forwarding manager processes on an active RP:

```
Router# showlogging process forwarding-manager rp active
Module Name                     Trace Level
-----------------------------------------------
acl                             Notice
binos                           Notice
binos/brand                     Notice
bipc                            Notice
bsignal                         Notice
btrace                          Notice
cce                             Notice
cdllib                          Notice
cef                             Notice
chasfs                          Notice
chasutil                        Notice
erspan                          Notice
ess                             Notice
ether-channel                   Notice
evlib                           Notice
evutil                          Notice
file_alloc                      Notice
fman_rp                         Notice
fpm                             Notice
fw                              Notice
icmp                            Notice
interfaces                      Notice
iosd                            Notice
ipc                             Notice
ipclog                          Notice
iphc                            Notice
IPsec                           Notice
mgmte-acl                       Notice
mlp                             Notice
mqipc                           Notice
nat                             Notice
nbar                            Notice
netflow                         Notice
om                              Notice
```

```
peer                             Notice
qos                              Notice
route-map                        Notice
sbc                              Notice
services                         Notice
sw_wdog                          Notice
tdl_acl_config_type              Notice
tdl_acl_db_type                  Notice
tdl_cdlcore_message              Notice
tdl_cef_config_common_type       Notice
tdl_cef_config_type              Notice
tdl_dpidb_config_type            Notice
tdl_fman_rp_comm_type            Notice
tdl_fman_rp_message              Notice
tdl_fw_config_type               Notice
tdl_hapi_tdl_type                Notice
tdl_icmp_type                    Notice
tdl_ip_options_type              Notice
tdl_ipc_ack_type                 Notice
tdl_IPsec_db_type                Notice
tdl_mcp_comm_type                Notice
tdl_mlp_config_type              Notice
tdl_mlp_db_type                  Notice
tdl_om_type                      Notice
tdl_ui_message                   Notice
tdl_ui_type                      Notice
tdl_urpf_config_type             Notice
tdllib                           Notice
trans_avl                        Notice
uihandler                        Notice
uipeer                           Notice
uistatus                         Notice
urpf                             Notice
vista                            Notice
wccp                             Notice
```

Set a tracing level

To set a tracing level for a module on a router, or for all the modules within a process on a router, enter the **set platform software trace** command in the privileged EXEC mode or diagnostic mode.

This example shows the tracing level for the ACL module in the Forwarding Manager of the ESP processor in slot 0 set to `info`:

```
set platform software trace forwarding-manager F0 acl info
```

View the content of the trace buffer

To view the trace messages in the trace buffer or file, enter the **show logging process** command in privileged EXEC or diagnostic mode. In the example, the trace messages for the Host Manager process in Route Processor slot 0 are viewed using the **show logging process command**:

```
Router# show logging process host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
```

```
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
```

Example: Use packet trace

This example provides a scenario in which packet trace is used to troubleshoot packet drops for a NAT configuration on a Cisco ASR 1006 Router. 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 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 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 12

Environmental Monitoring and PoE Management

The Cisco 8300 Series Secure Routers have hardware and software features that periodically monitor the router's environment. This chapter provides information on the environmental monitoring features on your router that allow you to monitor critical events and generate statistical reports on the status of various router components. This chapter includes these sections:

- Environmental monitoring, on page 155
- Environmental monitor and report functions, on page 155
- Configure power supply mode, on page 172

Environmental monitoring

The router provides a robust environment-monitoring system with several sensors that monitor the system temperatures. Microprocessors generate interrupts to the HOST CPU for critical events and generate a periodic status and statistics report. Some of the key functions of the environmental monitoring system:

- Monitoring temperature of CPUs, motherboard, and midplane
- Monitoring fan speed
- Recording abnormal events and generating notifications
- Monitoring Simple Network Management Protocol (SNMP) traps
- Generating and collecting Onboard Failure Logging (OBFL) data
- Sending call home event notifications
- Logging system error messages
- Displaying present settings and status

Environmental monitor and report functions

Monitoring and reporting functions allow you to maintain normal system operation by identifying and resolving adverse conditions prior to loss of operation.

- Environmental monitoring functions, on page 156
- Environmental reporting functions, on page 158

Environmental monitoring functions

Environmental monitoring functions use sensors to monitor the temperature of the cooling air as it moves through the chassis.

The local power supplies provide the ability to monitor:

- Input and output current
- Output voltage
- Input and output power
- Temperature
- Fan speed

The device is expected to meet the following environmental operating conditions:

- Operating Temperature Nominal—32°F to 104°F (0°C to 40°C)
- Operating Humidity Nominal—10% to 85% RH noncondensing
- Operating Humidity Short Term—10% to 85% RH noncondensing
- Operating Altitude—Sea level 0 ft to 10,000 ft (0 to 3000 m)
- AC Input Range—85 to 264 VAC

In addition, each power supply monitors its internal temperature and voltage. A power supply is either within tolerance (normal) or out of tolerance (critical). If an internal power supply's temperature or voltage reaches a critical level, the power supply shuts down without any interaction with the system processor.

The following table displays the levels of status conditions used by the environmental monitoring system.

Table 13: Levels of Status Conditions Used by the Environmental Monitoring System

Status Level	Description
Normal	All monitored parameters are within normal tolerance.
Warning	The system has exceeded a specified threshold. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
Critical	An out-of-tolerance temperature or voltage condition exists. Although the system continues to operate, it is approaching shutdown. Immediate operator action is required.

The environmental monitoring system sends system messages to the console, for example, when the conditions described here are met:

Fan Failure

When the system power is on, all the fans should be operational. Although the system continues to operate if a fan fails, the system displays this message:

```
%IOSXE_PEM-3-FANFAIL: The fan in slot 2/0 is encountering a failure condition
```

Sensors Out of Range

When sensors are out of range, the system displays this message:

```
%ENVIRONMENTAL-1-ALERT: V: 1.0v PCH, Location: R0, State: Warning, Reading: 1102 mV
```

```
%ENVIRONMENTAL-1-ALERT: V: PEM Out, Location: P1, State: Warning, Reading: 0 mV
```

```
%ENVIRONMENTAL-1-ALERT: Temp: Temp 3, Location R0, State : Warning, Reading : 90C
```

Fan Tray (Slot P2) Removed

When the fan tray for slot P2 is removed, the system displays this message:

```
%IOSXE_PEM-6-REMPEM_FM: PEM/FM slot P2 removed
```

Fan Tray (Slot P2) Reinserted

When the fan tray for slot P2 is reinserted, the system displays this message:

```
%IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P2 inserted
```

Fan Tray (Slot 2) is Working Properly

When the fan tray for slot 2 is functioning properly, the system displays this message:

```
%IOSXE_PEM-6-PEMOK: The PEM in slot P2 is functioning properly
```

Fan 0 in Slot 2 (Fan Tray) is Not Working

When Fan 0 in the fan tray of slot 2 is not functioning properly, the system displays this message:

```
%IOSXE_PEM-3-FANFAIL: The fan in slot 2/0 is encountering a failure condition
```

Fan 0 in Slot 2 (Fan Tray) is Working Properly

When Fan 0 in the fan tray of slot 2 is functioning properly, the system displays this message:

```
%IOSXE_PEM-6-FANOK: The fan in slot 2/0 is functioning properly
```

Main Power Supply in Slot 1 is Powered Off

When the main power supply in slot 1 is powered off, the system displays this message:

```
%IOSXE_PEM-3-PEMFAIL: The PEM in slot 1 is switched off or encountering a
failure condition.
```

Main Power Supply is Inserted in Slot 1

When the main power supply is inserted in slot 1, the system displays these messages:

```
%IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P1 inserted
%IOSXE_PEM-6-PEMOK: The PEM in slot 1 is functioning properly
```

Temperature and Voltage Exceed Max/Min Thresholds

The example shows the warning messages indicating the maximum and minimum thresholds of the temperature or voltage:

```
Warnings :
--------
For all the temperature sensors (name starting with “Temp:”) above,
the critical warning threshold is 100C (100C and higher)
the warning threshold is 80C (range from 80C to 99C)
the low warning threshold is 1C (range from -inf to 1C).

For all voltage sensors (names starting with "V:"),
the high warning threshold starts at that voltage +10%. (voltage + 10% is warning)
the low warning threshold starts at the voltage -10%. (voltage - 10% is warning)
```

Environmental reporting functions

You can retrieve and display environmental status reports using these commands:

- **debug environment**
- **debug platform software cman env monitor polling**
- **debug ilpower**
- **debug power** [**inline** | **main**]
- **show diag all eeprom**
- **show diag slot R0 eeprom detail**
- **show environment**
- **show environment all**
- **show inventory**
- **show platform all**
- **show platform diag**
- **show platform software status control-processor**
- **show version**
- **show power**
- **show power inline**

These commands show the current values of parameters such as temperature and voltage.

The environmental monitoring system updates the values of these parameters every 60 seconds. Brief examples of these commands are:

debug environment: Example

```
Router# debug environment location P0
Environmental sensor Temp: Temp 1 P0 debugging is on
Environmental sensor Temp: Temp 2 P0 debugging is on
Environmental sensor Temp: Temp 3 P0 debugging is on
Environmental sensor V: PEM Out P0 debugging is on
Environmental sensor I: PEM In P0 debugging is on
Environmental sensor I: PEM Out P0 debugging is on
Environmental sensor W: In pwr P0 debugging is on
Environmental sensor W: Out pwr P0 debugging is on
Environmental sensor RPM: fan0 P0 debugging is on
```

```
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 1 P0, In queue 1
*Jul  8 21:49:23.292 PDT:     State=Normal  Reading=35
*Jul  8 21:49:23.292 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 1 P0  State=Normal Reading=35
*Jul  8 21:49:23.292 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.292 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 2 P0, In queue 1
*Jul  8 21:49:23.292 PDT:     State=Normal  Reading=40
*Jul  8 21:49:23.292 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 2 P0  State=Normal Reading=40
*Jul  8 21:49:23.292 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.292 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 3 P0, In queue 1
*Jul  8 21:49:23.292 PDT:     State=Normal  Reading=44
*Jul  8 21:49:23.292 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.292 PDT:     Sensor: Temp: Temp 3 P0  State=Normal Reading=44
*Jul  8 21:49:23.292 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.292 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.292 PDT:     Sensor: V: PEM In P0, In queue 1
*Jul  8 21:49:23.292 PDT:     State=Normal  Reading=118501
*Jul  8 21:49:23.292 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: V: PEM In P0  State=Normal Reading=118501
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: V: PEM Out P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=12000
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: V: PEM Out P0  State=Normal Reading=12000
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: I: PEM In P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=820
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: I: PEM In P0  State=Normal Reading=828
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: I: PEM Out P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=7200
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: I: PEM Out P0  State=Normal Reading=7100
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: P: In pwr P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=97
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: P: In pwr P0  State=Normal Reading=98
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: P: Out pwr P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=87
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: P: Out pwr P0  State=Normal Reading=89
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:23.293 PDT:     Sensor: RPM: fan0 P0, In queue 1
*Jul  8 21:49:23.293 PDT:     State=Normal  Reading=5824
*Jul  8 21:49:23.293 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:23.293 PDT:     Sensor: RPM: fan0 P0  State=Normal Reading=5824
*Jul  8 21:49:23.293 PDT:     Inserting into queue 1 on spoke 189.
*Jul  8 21:49:23.293 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 1 P0, In queue 1
*Jul  8 21:49:43.296 PDT:     State=Normal  Reading=35
*Jul  8 21:49:43.296 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 1 P0  State=Normal Reading=35
```

```
*Jul  8 21:49:43.296 PDT:     Inserting into queue 1 on spoke 209.
*Jul  8 21:49:43.296 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 2 P0, In queue 1
*Jul  8 21:49:43.296 PDT:     State=Normal  Reading=40
*Jul  8 21:49:43.296 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 2 P0  State=Normal Reading=40
*Jul  8 21:49:43.296 PDT:     Inserting into queue 1 on spoke 209.
*Jul  8 21:49:43.296 PDT:     Rotation count=20 Displacement=0
*Jul  8 21:49:43.296 PDT:     Sensor: Temp: Temp 3 P0, In queue 1
*Jul  8 21:49:43.296 PDT:     State=Normal  Reading=44
*Jul  8 21:49:43.296 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:53:43.329 PDT:     State=Normal  Reading=5824
*Jul  8 21:53:43.329 PDT:     Rotation count=0  Poll period=20000
*Jul  8 21:53:43.329 PDT:     Sensor: RPM: fan0 P0  State=Normal Reading=5824
*Jul  8 21:53:43.329 PDT:     Inserting into queue 1 on spoke 149.
*Jul  8 21:53:43.329 PDT:     Rotation count=20 Displacement=0
```

debug platform software cman env monitor polling: Example

```
Router# debug platform software cman env monitor polling
platform software cman env monitor polling debugging is on
Router#
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 1 P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=35
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Temp 1, P0, 35
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 1 P0  State=Normal Reading=35
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 2 P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=40
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Temp 2, P0, 40
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 2 P0  State=Normal Reading=40
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 3 P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=44
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Temp 3, P0, 44
*Jul  8 21:56:23.351 PDT: Sensor: Temp: Temp 3 P0  State=Normal Reading=44
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: V: PEM In P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=118501
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback V: PEM In, P0, 118501
*Jul  8 21:56:23.351 PDT: Sensor: V: PEM In P0  State=Normal Reading=118501
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: V: PEM Out P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=12100
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback V: PEM Out, P0, 12000
*Jul  8 21:56:23.351 PDT: Sensor: V: PEM Out P0  State=Normal Reading=12000
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: I: PEM In P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=820
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback I: PEM In, P0, 828
*Jul  8 21:56:23.351 PDT: Sensor: I: PEM In P0  State=Normal Reading=828
```

```
*Jul  8 21:56:23.351 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.351 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.351 PDT: Sensor: I: PEM Out P0, In queue 1
*Jul  8 21:56:23.351 PDT: State=Normal  Reading=7200
*Jul  8 21:56:23.351 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.351 PDT: IOS-RP-ENVMON: sensor READ callback I: PEM Out, P0, 7100
*Jul  8 21:56:23.352 PDT: Sensor: I: PEM Out P0  State=Normal Reading=7100
*Jul  8 21:56:23.352 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.352 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.352 PDT: Sensor: P: In pwr P0, In queue 1
*Jul  8 21:56:23.352 PDT: State=Normal  Reading=97
*Jul  8 21:56:23.352 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback P: In pwr, P0, 98
*Jul  8 21:56:23.352 PDT: Sensor: P: In pwr P0  State=Normal Reading=98
*Jul  8 21:56:23.352 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.352 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.352 PDT: Sensor: P: Out pwr P0, In queue 1
*Jul  8 21:56:23.352 PDT: State=Normal  Reading=88
*Jul  8 21:56:23.352 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback P: Out pwr, P0, 88
*Jul  8 21:56:23.352 PDT: Sensor: P: Out pwr P0  State=Normal Reading=88
*Jul  8 21:56:23.352 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.352 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.352 PDT: Sensor: RPM: fan0 P0, In queue 1
*Jul  8 21:56:23.352 PDT: State=Normal  Reading=5888
*Jul  8 21:56:23.352 PDT: Rotation count=0  Poll period=20000
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P0, 5888
*Jul  8 21:56:23.352 PDT: Sensor: RPM: fan0 P0  State=Normal Reading=5888
*Jul  8 21:56:23.352 PDT: Inserting into queue 1 on spoke 9.
*Jul  8 21:56:23.352 PDT: Rotation count=20 Displacement=0
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P2, 12600
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback RPM: fan1, P2, 12840
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback RPM: fan2, P2, 12900
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback P: pwr, P2, 8
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Inlet 1, R0, 29
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Inlet 2, R0, 30
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Outlet 1, R0, 35
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: Outlet 2, R0, 36
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback Temp: CP-CPU, R0, 42
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 12v, R0, 12127
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 5v, R0, 5022
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 3.3v, R0, 3308
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 3.0v, R0, 3023
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 2.5v, R0, 2490
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.8v, R0, 1798
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.2v, R0, 1203
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.2v_CPU, R0, 1201
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.05v_CPU, R0, 1052
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.05v, R0, 1062
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 1.0v, R0, 1002
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback V: 0.6v, R0, 593
*Jul  8 21:56:23.352 PDT: IOS-RP-ENVMON: sensor READ callback P: pwr, R0, 86
*Jul  8 21:56:25.352 PDT: IOS-RP-ENVMON: sensor READ callback P: pwr: Pwr, 0/1, 5
*Jul  8 21:56:32.354 PDT: IOS-RP-ENVMON: sensor READ callback P: pwr: Pwr, 1/0, 27
```

debug ilpower: Example

```
Router# debug ilpower ?
  cdp         ILPOWER CDP messages
  controller  ILPOWER controller
  event       ILPOWER event
  ha          ILPOWER High-Availability
  port        ILPOWER port management
  powerman    ILPOWER powerman
  registries  ILPOWER registries
  scp         ILPOWER SCP messages
  upoe        ILPOWER upoe
```

debug power [inline|main]: Example

In this example, there is one 1000W power supply and one 450W power supply. Inline and main power output is shown.

```
Router# debug power ?
  inline  ILPM inline power related
  main    Main power related
  <cr>    <cr>
Router# debug power
POWER all debug debugging is on

Router# show debugging | include POWER
POWER:
POWER main debugging is on
POWER inline debugging is on
Router#
..

*Jul  8 21:56:23.351: %ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P1, State: Warning,
Reading: 0 mV
*Jul  8 21:56:23.351: %IOSXE_PEM-6-PEMOK: The PEM in slot P1 is functioning properly
*Jul  8 21:56:23.351: %PLATFORM_POWER-6-MODEMATCH: Main power is in Boost mode
*Jul  8 21:56:23.351: Power M: Received Msg for 12V/Main, total power 1450, Run same as cfg
 Yes
*Jul  8 21:56:23.351: Power M: Received Msg for POE/ILPM, total power 500, Run same as cfg
 No
*Jul  8 21:56:23.351: Power I: Updating pool power is 500 watts
*Jul  8 21:56:23.351: Power I: Intimating modules of total power 500 watts
*Jul  8 21:56:23.351: Power M: Received Msg for 12V/Main, total power 1450, Run same as cfg
 Yes
*Jul  8 21:56:23.351: Power M: Received Msg for POE/ILPM, total power 500, Run same as cfg
 No
*Jul  8 21:56:23.351: Power I: Updating pool power is 500 watts
*Jul  8 21:56:23.351: Power I: Intimating modules of total power 500 watts
Router#
```

show diag all eeprom: Example for C8375-E-G2

```
Router# show diag all eeprom
MIDPLANE EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
        Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
Power/Fan Module P0 EEPROM data:

        Product Identifier (PID) : PWR-CC1-760WAC
        Version Identifier (VID) : V01
        PCB Serial Number        : LIT2748A9MU
        CLEI Code                : CMUPAKBCAA
```

```
Power/Fan Module P1 EEPROM data:

        Product Identifier (PID) : PWR-CC1-400WAC
        Version Identifier (VID) : V01
        PCB Serial Number        : LIT2650C53E
        CLEI Code                : CMUPAG4CAA
External PoE Module POE0 EEPROM data:

        Product Identifier (PID) : PWR-CC1-760WAC
        Version Identifier (VID) : V01
        PCB Serial Number        : LIT2748A9MU
        CLEI Code                : CMUPAKBCAA
External PoE Module POE1 EEPROM data is not initialized

Slot R0 EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
        Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
Slot F0 EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
Slot 0 EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
        Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
Slot 1 EEPROM data:

        Product Identifier (PID) : C8375-E-G2
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO28310870
        Top Assy. Part Number    : 68-7625-01
        Hardware Revision        : 1.0
        CLEI Code                : CMM8K00ARA
SPA EEPROM data for subslot 0/0:

        Product Identifier (PID) : 4M-2xSFP+
        Version Identifier (VID) : V01
        PCB Serial Number        :
        Top Assy. Part Number    : 68-2236-01
        Top Assy. Revision       : A0
        Hardware Revision        : 2.2
        CLEI Code                : CNUIAHSAAA
SPA EEPROM data for subslot 0/1:

        Product Identifier (PID) : C-NIM-8M
        Version Identifier (VID) : V01
        PCB Serial Number        : FDO26500YDL
        Hardware Revision        : 1.0
        CLEI Code                : CMUIAYSCAA
SPA EEPROM data for subslot 0/2 is not available
SPA EEPROM data for subslot 0/3 is not available

SPA EEPROM data for subslot 0/4 is not available

SPA EEPROM data for subslot 0/5 is not available

SPA EEPROM data for subslot 0/6 is not available

SPA EEPROM data for subslot 1/0 is not available

SPA EEPROM data for subslot 1/1 is not available

SPA EEPROM data for subslot 1/2 is not available

SPA EEPROM data for subslot 1/3 is not available

SPA EEPROM data for subslot 1/4 is not available

SPA EEPROM data for subslot 1/5 is not available

SPA EEPROM data for subslot 1/6 is not available
```

show environment: Example for C8375-E-G2

In this example, note the output for the slots POE0 and POE1.

```
Router# show environment
 Number of Critical alarms:  0
Number of Major alarms:     0
Number of Minor alarms:     2

 Slot        Sensor          Current State   Reading
Threshold(Minor,Major,Critical,Shutdown)
 ----------  --------------  --------------- ------------
---------------------------------------
 R0          Temp: Inlet 1   Normal          23    Celsius      (40 ,na ,42 ,na )(Celsius)
 R0          Temp: Inlet 2   Normal          26    Celsius      (90 ,na ,100,na )(Celsius)
 R0          Temp: Outlet 1  Normal          24    Celsius      (70 ,na ,75 ,na )(Celsius)
 R0          Temp: Outlet 2  Normal          26    Celsius      (70 ,na ,75 ,na )(Celsius)
 R0          Temp: CPU       Normal          34    Celsius      (na ,na ,na ,na )(Celsius)
 R0          Temp: Working   Normal          23    Celsius      (na ,na ,na ,na )(Celsius)
 R0          V: 12V          Normal          12044 mV           na
 R0          V: 5V           Normal          5010  mV           na
 R0          V: 3.3V_STBY    Normal          3314  mV           na
 R0          V: 3.3V         Normal          3315  mV           na
 R0          V: 3.3V_USB     Normal          3315  mV           na
 R0          V: 2.5V         Normal          2502  mV           na
 R0          V: 1.8V         Normal          1799  mV           na
 R0          V: 1.2V_CPU     Normal          1197  mV           na
 R0          V: 1.2V         Normal          1208  mV           na
 R0          V: 1.1V         Normal          1100  mV           na
 R0          V: 1.0V         Normal          1001  mV           na
 R0          V: 0.8V_SW      Normal          790   mV           na
 R0          V: 0.85V_DDR    Normal          850   mV           na
 R0          V: 0.8V_SYS     Normal          848   mV           na
 R0          V: 0.8V_CORE    Normal          800   mV           na
 R0          V: 0.75V        Normal          750   mV           na
 R0          P: Power        Normal          41    Watts        na
 P0          Temp: Temp 1    Normal          0     Celsius      (na ,na ,na ,na )(Celsius)
 P0          Temp: Temp 2    Normal          0     Celsius      (na ,na ,na ,na )(Celsius)
 P0          Temp: Temp 3    Normal          0     Celsius      (na ,na ,na ,na )(Celsius)
 P0          V: PEM In       Normal          0     mV           na
 P0          V: PEM Out      Minor_Low       0     mV           na
 P0          I: PEM In       Normal          0     mA           na
 P0          I: PEM Out      Normal          0     mA           na
 P0          P: In power     Normal          0     Watts        na
 P0          P: Out power    Normal          0     Watts        na
 P0          RPM: fan0       Minor_Low       0     RPM          na
 P1          Temp: Temp 1    Normal          28    Celsius      (na ,na ,na ,na )(Celsius)
 P1          Temp: Temp 2    Normal          31    Celsius      (na ,na ,na ,na )(Celsius)
P1          Temp: Temp 3    Normal          30    Celsius      (na ,na ,na ,na )(Celsius)
 P1          V: PEM In       Normal          226503mV           na
 P1          V: PEM Out      Normal          12000 mV           na
 P1          I: PEM In       Normal          265   mA           na
 P1          I: PEM Out      Normal          3600  mA           na
 P1          P: In power     Normal          54    Watts        na
 P1          P: Out power    Normal          42    Watts        na
 P1          RPM: fan0       Normal          6080  RPM          na
 P2          P: Power        Normal          3     Watts        na
 P2          RPM: fan0       Normal          9480  RPM          na
 P2          RPM: fan1       Normal          9540  RPM          na
 P2          RPM: fan2       Normal          9360  RPM          na
 0/1         P: pwr: Pwr     Normal          11    Watts        na
```

show environment all: Example for C8375-E-G2

```
Router# show environment all
Sensor List:  Environmental Monitoring
 Sensor           Location          State             Reading
 Temp: Temp 1     P0                Normal            36 Celsius
 Temp: Temp 2     P0                Normal            38 Celsius
 Temp: Temp 3     P0                Normal            38 Celsius
 V: PEM In        P0                Normal            206502 mV
 V: PEM Out       P0                Normal            12000 mV
 I: PEM In        P0                Normal            281 mA
 I: PEM Out       P0                Normal            3500 mA
 P: In pwr        P0                Normal            53 Watts
 P: Out pwr       P0                Normal            43 Watts
 RPM: fan0        P0                Normal            3712 RPM
 RPM: fan0        P2                Normal            7260 RPM
 RPM: fan1        P2                Normal            7260 RPM
 RPM: fan2        P2                Normal            7200 RPM
 P: pwr           P2                Normal            3 Watts
 Temp: Inlet 1    R0                Normal            19 Celsius
 Temp: Inlet 2    R0                Normal            21 Celsius
 Temp: Outlet 1   R0                Normal            25 Celsius
 Temp: Outlet 2   R0                Normal            23 Celsius
 Temp: CP-CPU     R0                Normal            29 Celsius
 V: 12v           R0                Normal            11984 mV
 V: 5v            R0                Normal            5018 mV
 V: 3.3v          R0                Normal            3311 mV
 V: 3.0v          R0                Normal            2992 mV
 V: 2.5v          R0                Normal            2488 mV
 V: 1.8v          R0                Normal            1785 mV
 V: 1.2v          R0                Normal            1201 mV
 V: 1.2v_CPU      R0                Normal            1200 mV
 V: 1.05v_CPU     R0                Normal            1051 mV
 V: 1.05v         R0                Normal            1058 mV
 V: 1.0v          R0                Normal            1001 mV
 V: 0.6v          R0                Normal            595 mV
 P: pwr           R0                Normal            45 Watts
```

show inventory: Example for C8375-E-G2

```
Router# show inventory

+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

INFO: Please use "show license UDI" to get serial number for licensing.

+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++


NAME: "Chassis", DESCR: "Cisco C8375-E-G2 Chassis"

PID: C8375-E-G2        , VID: V01  , SN: FDO2833M01A


NAME: "Power Supply Module 0", DESCR: "760W AC Power Supply for Cisco C8375"

PID: PWR-CC1-760WAC    , VID: V01  , SN: LIT2748A9MU


NAME: "Power Supply Module 1", DESCR: "400W AC power supply for Cisco C8300 1RU"

PID: PWR-CC1-400WAC    , VID: V01  , SN: LIT2650C53E


NAME: "Fan Tray", DESCR: "Cisco C8300 1RU Fan Assembly"

PID: C8300-FAN-1R      , VID: V02  , SN: LIT2214364L


NAME: "POE Module 0", DESCR: "760W AC Power Supply for Cisco C8375"

PID: PWR-CC1-760WAC    , VID: V01  , SN: LIT2748A9MU


NAME: "module 0", DESCR: "Cisco C8375-E-G2 Built-In NIM controller"

PID: C8375-E-G2        , VID:      , SN:


NAME: "NIM subslot 0/1", DESCR: "C-NIM-8M"

PID: C-NIM-8M          , VID: V01  , SN: FDO26500YDL


NAME: "NIM subslot 0/0", DESCR: "4M-2xSFP+"

PID: 4M-2xSFP+         , VID: V01  , SN:
NAME: "subslot 0/0 transceiver 4", DESCR: "10G AOC5M"

PID: SFP-10G-AOC5M       , VID: V01  , SN: DPZ2618A261-B


NAME: "subslot 0/0 transceiver 5", DESCR: "10G AOC5M"

PID: SFP-10G-AOC5M       , VID: V01  , SN: DPZ2618A261-A


NAME: "module 1", DESCR: "Cisco C8375-E-G2 Built-In SM controller"

PID: C8375-E-G2        , VID:      , SN:
```

```
NAME: "module R0", DESCR: "Cisco C8375-E-G2 Route Processor"

PID: C8375-E-G2        , VID: V01  , SN: FDO28310870


NAME: "module F0", DESCR: "Cisco C8375-E-G2 Forwarding Processor"

PID: C8375-E-G2        , VID:      , SN:
```

show platform: Example for C8375-E-G2

```
Router# show platform
 Chassis type: C8375-E-G2

Slot      Type                State                 Insert time (ago)

--------- ------------------- --------------------- -----------------

0         C8375-E-G2          ok                    3d17h

0/0       4M-2xSFP+           ok                    3d17h

0/1       C-NIM-8M            ok                    3d17h

1         C8375-E-G2          ok                    3d17h

R0        C8375-E-G2          ok, active            3d17h

F0        C8375-E-G2          ok, active            3d17h

P0        PWR-CC1-760WAC      fail, badinput        3d17h

P1        PWR-CC1-400WAC      ok                    3d17h

P2        C8300-FAN-1R        ok                    3d17h

POE0      PWR-CC1-760WAC      fail, badinput        3d17h


Slot      CPLD Version        Firmware Version

--------- ------------------- ---------------------------------------

0         25033132            v17.15(1.17r).s2.cp

1         25033132            v17.15(1.17r).s2.cp

R0        25033132            v17.15(1.17r).s2.cp

F0        25033132            v17.15(1.17r).s2.cp
```

show platform diag: Example for C8375-E-G2

```
Router# show platform diag
Chassis type: C8375-E-G2
```

```
Slot: 0, C8375-E-G2

Running state               : ok

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:24 (3d17h ago)

Software declared up time   : 00:01:16 (3d17h ago)

CPLD version                : 25033132

Firmware version            : v17.15(1.17r).s2.cp


Sub-slot: 0/0, 4M-2xSFP+

Operational status          : ok

Internal state              : inserted

Physical insert detect time : 00:01:24 (3d17h ago)

Logical insert detect time  : 00:01:24 (3d17h ago)


Sub-slot: 0/1, C-NIM-8M

Operational status          : ok

Internal state              : inserted

Physical insert detect time : 00:01:26 (3d17h ago)

Logical insert detect time  : 00:01:26 (3d17h ago)


Sub-slot: 0/4, VDSP-CC

Operational status          : ok

Internal state              : inserted

Physical insert detect time : 00:01:27 (3d17h ago)

Logical insert detect time  : 00:01:27 (3d17h ago)
Slot: 1, C8375-E-G2

Running state               : ok

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:24 (3d17h ago)

Software declared up time   : 00:01:17 (3d17h ago)

CPLD version                : 25033132

Firmware version            : v17.15(1.17r).s2.cp
```

```
Slot: R0, C8375-E-G2

Running state               : ok, active

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:24 (3d17h ago)

Software declared up time   : 00:00:24 (3d17h ago)

CPLD version                : 25033132

Firmware version            : v17.15(1.17r).s2.cp


Slot: F0, C8375-E-G2

Running state               : ok, active

Internal state              : online

Internal operational state  : ok

Physical insert detect time : 00:00:24 (3d17h ago)

Software declared up time   : 00:01:04 (3d17h ago)

Hardware ready signal time  : 00:01:02 (3d17h ago)

Packet ready signal time    : 00:01:17 (3d17h ago)

CPLD version                : 25033132

Firmware version            : v17.15(1.17r).s2.cp
Slot: P0, PWR-CC1-760WAC

State                       : fail, badinput

Physical insert detect time : 00:00:02 (3d17h ago)


Slot: P1, PWR-CC1-400WAC

State                       : ok

Physical insert detect time : 00:00:02 (3d17h ago)


Slot: P2, C8300-FAN-1R

State                       : ok

Physical insert detect time : 00:00:02 (3d17h ago)


Slot: POE0, PWR-CC1-760WAC

State                       : fail, badinput

Physical insert detect time : 00:00:02 (3d17h ago)
```

```
Slot: POE1, Unknown

State                       : empty

Physical insert detect time : 00:00:00 (never ago)
```

show platform software status control-processor: Example for C8375-E-G2

```
Router# show platform software status control-processor
RP0: online, statistics updated 10 seconds ago
Load Average: healthy
  1-Min: 0.53, status: healthy, under 5.00
  5-Min: 0.90, status: healthy, under 5.00
  15-Min: 0.87, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3884836
  Used: 1976928 (51%), status: healthy
  Free: 1907908 (49%)
  Committed: 3165956 (81%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  2.10, System:  2.20, Nice:  0.00, Idle: 95.69
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  2.80, System:  2.60, Nice:  0.00, Idle: 94.50
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  1.90, System:  2.10, Nice:  0.00, Idle: 96.00
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 10.12, System:  0.60, Nice:  0.00, Idle: 89.27
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
```

show diag slot RO eeprom detail: Example for C8375-E-G2

```
Router# show diag slot R0 eeprom detail

       Slot R0 EEPROM data:

                                                                           EEPROM version
          : 4

Compatible Type          : 0xFF

FRU Specific Info        : 0100

PCB Serial Number        : FDO28310870

Controller Type          : 4487

Hardware Revision        : 1.0

PCB Part Number          : 73-20702-08

Board Revision           : 03

Top Assy. Part Number    : 68-7625-01

Deviation Number         : 0
```

```
Fab Version             : 08

Product Identifier (PID) : C8375-E-G2

Version Identifier (VID) : V01

CLEI Code               : CMM8K00ARA

Chassis Serial Number    : FDO2833M01A

Chassis MAC Address      : 481b.a465.9470

MAC Address block size   : 144

Manufacturing Test Data  : 00 00 00 00 00 00 00 00

Asset ID                :
```

show version: Example for C8375-E-G2

```
Router# show version
Cisco IOS XE Software, Version BLD_V1718_THROTTLE_LATEST_20250513_033132_V17_18_0_38
Cisco IOS Software [IOSXE], c8kg2be Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Experimental
 Version 17.18.20250513:042531
[BLD_V1718_THROTTLE_LATEST_20250513_033132:/nobackup/mcpre/s2c-build-ws 101]
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Mon 12-May-25 21:26 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: v17.15(1.19d).s2.cp.RSA2K
Crestone-1 uptime is 4 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "bootflash:c8kg2be-universalk9.17.18.01.0.700_V17_18_0_38.SSA.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  Subscription advantage          advantage

The current crypto throughput level is 10000 kbps (Aggregate)


Smart Licensing Status: Smart Licensing Using Policy

cisco C8375-E-G2 (1RU) processor with 3703488K/6147K bytes of memory.
Processor board ID FDO2721M02R
Router operating mode: Autonomous
1 Virtual Ethernet interface
4 Gigabit Ethernet interfaces
4 2.5 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
20257791K bytes of flash memory at bootflash:.

Configuration register is 0x3922
```

Configure power supply mode

You can configure the power supplies of both the device and a connected Power over Ethernet (PoE) module.

- Configure the external PoE Service Module power supply mode, on page 172
- Examples to configure power supply mode, on page 173
- Available PoE power, on page 174

For more information on the Power Supply Mode, See the Overview of the Power Options section.

- Hardware Installation Guide for Cisco 8300 Series Secure Routers

Configure the external PoE Service Module power supply mode

Configure the power supply of an external PoE service module using the **power inline redundant** command:

- **power inline redundant**—Sets the external PoE service module power supply in redundant mode.
- **no power inline redundant**—Sets the external PoE service module power supply in boost mode.

Note The default mode for the external PoE service module power supply is redundant mode.

The **show power** command shows whether boost or redundant mode is configured and whether this mode is currently running on the system.

Examples to configure power supply mode

Example—Configured Mode of Redundant for Main PSU and PoE Module

In this example, the **show power** command shows the configured mode is `Redundant` for both the main and inline power. The system has one 400 W and one 360 W power supply.

```
Router# show powerMain PSU :
    Router#show power
Main PSU :
    Power Operating Mode : Normal
    Configured Mode : Redundant
    Current runtime state same : Yes
    Total power available : 400 Watts
POE Module :
    Configured Mode : Redundant
    Current runtime state same : Yes
    Total power available : 360 Watts

Router#
```

Example—Configured Mode of Boost for PoE Power

In this example, an attempt is made to configure the inline power in boost mode by using the **no** form of the **power inline redundant** command. The inline power mode is **not** changed to boost mode because that would require a total power available in redundant mode of 1000 W. The inline power mode is redundant and is shown by the following values for the PoE Module:

- `Configured Mode : Boost`
- `Current runtime state same : No`

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power inline redundant
Router(config)#
*Jan 31 03:42:40.947: %PLATFORM_POWER-6-MODEMISMATCH: Inline power not in Boost mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
    Main PSU :
    Power Operating Mode : Normal
    Configured Mode : Redundant
    Current runtime state same : Yes
    Total power available : 400 Watts
POE Module :
    Configured Mode : Boost
    Current runtime state same : Yes
    Total power available : 720 Watts
Router#
```

Available PoE power

For the PoE feature to be available on the external PoE module, the total power from the power supplies must be 760 W or higher.

Note To ensure the PoE feature is functional on the external PoE module, verify the availability of PoE power on your router using the **show platform** and **show power** commands.

To determine there is enough PoE power for use by an external PoE service module, use the **show platform** and **show power** commands to calculate the available PoE power based on the wattage values of the main power supplies and PoE inverters.

Take the values of your main P0 and P1 power supplies to give the Total Power (for main power supplies.) Then take the values of your PoE1 and PoE2 power inverters to calculate the Total PoE Power.

The following table shows example modes of operation, which may be similar to your configuration.

The Total PoE Power value, in the final column of the table needs to be 760 W or higher for the PoE feature to be functional on a connected PoE service module.

Note Add power inverters to the router before inserting an external PoE module. Otherwise, even if the Total PoE Power is sufficient, the PoE power will not be used by the external PoE module and the module will need to be re-booted for the PoE feature to be functional.

Configuring a power mode of boost or redundant on the main power supplies, or PoE inverters, may affect the value for Total PoE Power.

The following table shows all power values in Watts. The wattage ratings of the main power supplies are shown in columns Main P0 and Main P1. The wattage ratings of the PoE inverters are shown in columns PoE0 and PoE1.

Table 14: Modes of operation for C8375-E-G2

Mode Example	Main P0	Main P1	Config Mode	Total Power (Main)	PoE0	PoE1	Config Mode	Total PoE Power
1	400	None	Redundant	400	None	None	Redundant or Boost	0 (None)
2	None	400	Redundant	400	None	None	Redundant or Boost	0 (None)
3	400	None	Redundant	400	360	None	Redundant or Boost	360

Mode Example	Main P0	Main P1	Config Mode	Total Power (Main)	PoE0	PoE1	Config Mode	Total PoE Power
4	None	400	Redundant	400	None	360	Redundant or Boost	360
5	400	400	Redundant	400	None	None	Redundant or Boost	0 (None)
6 **Note** When installed 760WAC in P0 only	400	None	Redundant	400	360	None	Redundant or Boost	360
7 **Note** When installed 760WAC in P1 only	None	400	Redundant	400	None	360	Redundant or Boost	360
8	400	400	Redundant	400	360	360	Redundant	360
9	400	400	Redundant	400	360	360	Boost	720
10	500	None	Redundant	500	None	None	Redundant or Boost	0 (None)
11	None	500	Redundant	500	None	None	Redundant or Boost	0 (None)
12	500	500	Redundant	500	None	None	Redundant or Boost	0 (None)

Note In the table above, for 360 W or higher Total PoE Power to be available, the "Total Power" (of the main power supplies) must be 760 W or higher.

For 720 W Total PoE Power (see Mode Example 6), there must be two 760 W main power supplies (in `Boost` mode) and two PoE inverters (also in `Boost` mode).

⚠

Caution Care should be taken while removing the power supplies and power inverters (especially in `Boost` mode of operation). If the total power consumption is higher than can be supported by one power supply alone and in this condition a power supply is removed, the hardware can be damaged. This may then result in the system being unstable or unusable.

Similarly, in the case where there is only one PoE inverter providing PoE power to a service module, and in this condition the PoE inverter is removed, the hardware may be damaged, and may result in the system being unstable or unusable.

CHAPTER 13

Configure High Availability

The Cisco High Availability (HA) technology enable network-wide protection by providing quick recovery from disruptions that may occur in any part of a network. A network's hardware and software work together with Cisco High Availability technology, which besides enabling quick recovery from disruptions, ensures fault transparency to users and network applications.

These sections describe how to configure Cisco High Availability features on your device:

Cisco High Availability

The unique hardware and software architecture of your router is designed to maximize router uptime during any network event, and thereby provide maximum uptime and resilience within any network scenario.

This section covers some aspects of Cisco High Availability that may be used on the Cisco 8300 Series Secure Routers:

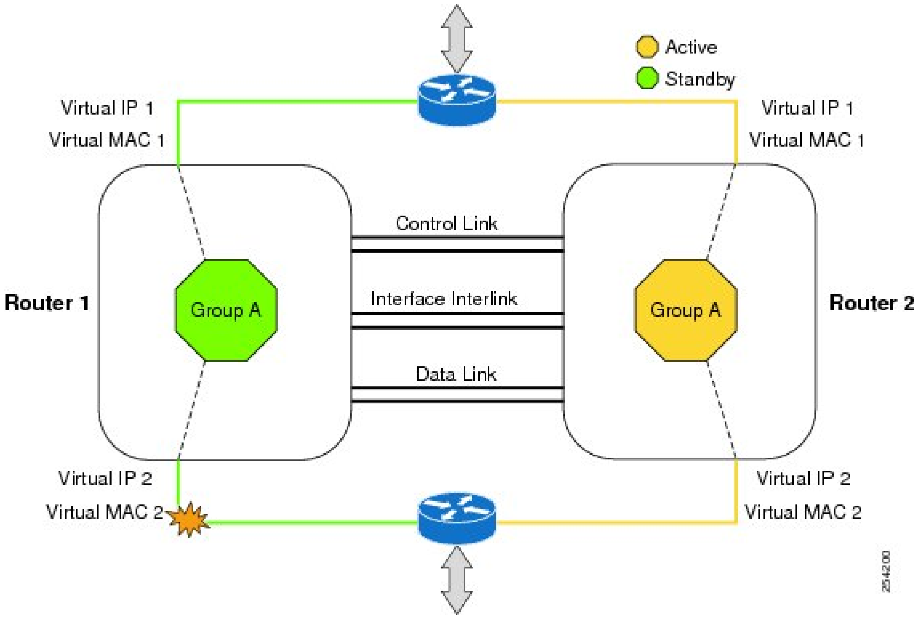
- Interchassis High Availability, on page 177
- Bidirectional Forwarding Detection, on page 178

Interchassis High Availability

The Interchassis High Availability feature is also known as the box-to-box redundancy feature. Interchassis High Availability enables the configuration of pairs of devices to act as backup for each other. This feature can be configured to determine the active device based on several failover conditions. When a failover occurs, the standby device seamlessly takes over and starts processing call signaling and performing media forwarding tasks.

Groups of redundant interfaces are known as redundancy groups. The following figure depicts the active-standby device scenario. It shows how the redundancy group is configured for a pair of devices that have a single outgoing interface.

Figure 1: Redundancy group configuration



The device are joined by a configurable control link and data synchronization link. The control link is used to communicate the status of the devices. The data synchronization link is used to transfer stateful information to synchronize the stateful database for the calls and media flows. Each pair of redundant interfaces are configured with the same unique ID number, also known as the RII. For information on configuring Interchassis HA on your device, see Configure Interchassis High Availability, on page 179.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast-forwarding path-failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast-forwarding path-failure detection, BFD provides a consistent failure detection method for network administrators. Because a network administrator can use BFD to detect forwarding path failures at a uniform rate rather than variable rates for different routing protocol hello mechanisms, network profiling and planning is easier, and reconvergence time is consistent and predictable.

For more information on BFD, see the “Bidirectional Forwarding Detection” section in the IP Routing: BFD Configuration Guide .

Bidirectional Forwarding Detection Offload

The Bidirectional Forwarding Detection Offload feature allows the offload of BFD session management to the forwarding engine for improved failure detection times. BFD offload reduces the overall network convergence time by sending rapid failure detection packets (messages) to the routing protocols for recalculating the routing table. See Configuring BFD Offload, on page 180.

Configure Cisco High Availability

Configure Interchassis High Availability

Prerequisites

- The active device and the standby device must run on the identical version of the Cisco IOS XE software.
- The active device and the standby device must be connected through an L2 connection for the control path.
- Either the Network Time Protocol (NTP) must be configured or the clock must be set identical on both devices to allow timestamps and call timers to match.
- Virtual Routing and Forwarding (VRF) must be defined in the same order on both active and standby devices for an accurate synchronization of data.
- The latency times must be minimal on all control and data links to prevent timeouts.
- Physically redundant links, such as Gigabit EtherChannel, must be used for the control and data paths.

Restrictions

- The failover time for a box-to-box application is higher for a non-box-to-box application.
- LAN and MESH scenarios are not supported.
- VRFs are not supported and cannot be configured under ZBFW High Availability data and control interfaces.
- The maximum number of virtual MACs supported by the Front Panel Gigabit Ethernet (FPGE) interfaces depends on the platform. For information about the FPGE interfaces, see the Hardware Installation Guide for Cisco 8300 Series Secure Router.
- When the configuration is replicated to the standby device, it is not committed to the startup configuration; it is in the running configuration. A user must run the **write memory** command to commit the changes that have been synchronized from the active device, on the standby device.

How to configure Interchassis High Availability

For more information on configuring Interchassis High Availability on the device, see the IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S.

Configure Bidirectional Forwarding

For information on configuring BFD on your device, see the IP Routing BFD Configuration Guide.

For BFD commands, see the Cisco IOS IP Routing: Protocol-Independent Command Reference document.

Configuring BFD Offload

Restrictions

- Only BFD version 1 is supported.
- When configured, only offloaded BFD sessions are supported;, BFD session on RP are not supported.
- Only Asynchronous mode or no echo mode of BFD is supported.
- 511 asynchronous BFD sessions are supported.
- BFD hardware offload is supported for IPv4 sessions with non-echo mode only.
- BFD offload is supported only on port-channel interfaces.
- BFD offload is supported only for the Ethernet interface.
- BFD offload is not supported for IPv6 BFD sessions.
- BFD offload is not supported for BFD with TE/FRR.

How to Configure BFD Offload

BFD offload functionality is enabled by default. You can configure BFD hardware offload on the route processor. For more information, see Configuring BFD and the IP Routing BFD Configuration Guide.

Verifying Interchassis High Availability

Use these **show** commands to verify the Interchassis High Availability.

Note Prerequisites and links to additional documentation configuring Interchassis High Availability are listed in Configure Interchassis High Availability, on page 179.

- **show redundancy application group [group-id | all]**
- **show redundancy application transport {client | group [group-id]}**
- **show redundancy application control-interface group [group-id]**
- **show redundancy application faults group [group-id]**
- **show redundancy application protocol {protocol-id | group [group-id]}**
- **show redundancy application if-mgr group [group-id]**
- **show redundancy application data-interface group [group-id]**

The example shows the redundancy application groups configured on the device:

```
Router# show redundancy application group
Group ID    Group Name                      State
--------    ----------                      -----
1           Generic-Redundancy-1            STANDBY
2           Generic-Redundancy2             ACTIVE
```

The example shows the details of redundancy application group 1:

```
Router# show redundancy application group 1
Group ID:1
Group Name:Generic-Redundancy-1

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE
```

The example shows the details of redundancy application group 2:

```
Router# show redundancy application group 2
Group ID:2
Group Name:Generic-Redundancy2

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

The example shows details of the redundancy application transport client:

```
Router# show redundancy application transport client
Client         Conn#  Priority   Interface   L3        L4
( 0)RF           0      1         CTRL       IPV4      SCTP

( 1)MCP_HA       1      1         DATA       IPV4      UDP_REL

( 4)AR           0      1         ASYM       IPV4      UDP

( 5)CF           0      1         DATA       IPV4      SCTP
```

The example shows configuration details for the redundancy application transport group:

```
Router# show redundancy application transport group
Transport Information for RG (1)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
0    0       192.0.2.8       59000    192.0.2.4       59000    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
1    1       10.10.2.10      53000    10.10.6.9       53000    DATA    IPV4    UDP_REL
```

```
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
2    0       192.0.2.3       0       192.0.2.3        0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
3    0       10.10.2.10      59001    10.10.6.9       59001    DATA    IPV4    SCTP
Transport Information for RG (2)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
8    0       192.0.2.8       59004    192.0.2.2       59004    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
9    1       10.10.2.10      53002    10.10.6.9       53002    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
10   0       192.0.2.3       0        192.0.2.3       0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
11   0       10.10.2.10      59005    10.10.6.9       59005    DATA    IPV4    SCTP
```

The example shows the configuration details of redundancy application transport group 1:

```
Router# show redundancy application transport group 1
Transport Information for RG (1)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
0    0       192.0.2.8       59000    192.0.2.4       59000    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
1    1       10.10.2.10      53000    10.10.2.10      53000    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
2    0       192.0.2.3       0        192.0.2.3       0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
3    0       10.10.2.10      59001    10.10.2.10      59001    DATA    IPV4    SCTP
```

The example shows configuration details of redundancy application transport group 2:

```
Router# show redundancy application transport group 2
Transport Information for RG (2)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
8    0       192.0.2.8       59004    192.0.2.4       59004    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
9    1       10.10.2.10      53002    10.10.2.10      53002    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
10   0       192.0.2.3       0        192.0.2.3       0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
11   0       10.10.2.10      59005    10.10.2.10      59005    DATA    IPV4    SCTP
```

The example shows configuration details of the redundancy application control-interface group:

```
Router# show redundancy application control-interface group
The control interface for rg[1] is TwoGigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 192.0.2.4 Active RGs: 1 Standby RGs: 2 BFD handle: 0

The control interface for rg[2] is TwoGigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
```

```
Interface Neighbors:
Peer: 192.0.2.4 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

The example shows configuration details of the redundancy application control-interface group 1:

```
Router# show redundancy application control-interface group 1
The control interface for rg[1] is TwoGigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 192.0.2.4 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

The example shows configuration details of the redundancy application control-interface group 2:

```
Router# show redundancy application control-interface group 2
The control interface for rg[2] is TwoGigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 192.0.2.4 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

The example shows configuration details of the redundancy application faults group:

```
Router# show redundancy application faults group
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

The example shows configuration details specific to redundancy application faults group 1:

```
Router# show redundancy application faults group 1
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

The example shows configuration details specific to redundancy application faults group 2:

```
Router# show redundancy application faults group 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

The example shows configuration details for the redundancy application protocol group:

```
Router# show redundancy application protocol group
RG Protocol RG 1
------------------
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 192.0.4.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
```

```
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: TwoGigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 117, Bytes 7254, HA Seq 0, Seq Number 117, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 115, Bytes 3910, HA Seq 0, Seq Number 1453975, Pkt Loss 0



RG Protocol RG 2
------------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 192.0.4.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: TwoGigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 118, Bytes 7316, HA Seq 0, Seq Number 118, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 102, Bytes 3468, HA Seq 0, Seq Number 1453977, Pkt Loss 0
```

The example shows configuration details for the redundancy application protocol group 1:

```
Router# show redundancy application protocol group 1
RG Protocol RG 1
------------------
```

```
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 192.0.4.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: TwoGigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 120, Bytes 7440, HA Seq 0, Seq Number 120, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 118, Bytes 4012, HA Seq 0, Seq Number 1453978, Pkt Loss 0
```

The example shows configuration details for the redundancy application protocol group 2:

```
Router# show redundancy application protocol group 2
RG Protocol RG 2
------------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 192.0.4.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: TwoGigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 123, Bytes 7626, HA Seq 0, Seq Number 123, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
```

```
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 107, Bytes 3638, HA Seq 0, Seq Number 1453982, Pkt Loss 0
```

The example shows configuration details for the redundancy application protocol 1:

```
Router# show redundancy application protocol 1
Protocol id: 1, name: rg-protocol-1
BFD: ENABLE
Hello timer in msecs: 3000
Hold timer in msecs: 10000
OVLD-1#show redundancy application protocol 2
Protocol id: 2, name: rg-protocol-2
BFD: ENABLE
Hello timer in msecs: 3000
Hold timer in msecs: 10000
```

The example shows configuration details for redundancy application interface manager group:

```
Router# show redundancy application if-mgr group
 RG ID: 1
 ==========

 interface      TwoGigabitEthernet0/0/3.152
 ---------------------------------------
 VMAC           0007.b421.4e21
 VIP            203.0.113.1
 Shut           shut
 Decrement      10

 interface      TwoGigabitEthernet0/0/2.152
 ---------------------------------------
 VMAC           0007.b421.5209
 VIP            203.0.113.4
 Shut           shut
 Decrement      10


 RG ID: 2
 ==========

 interface      TwoGigabitEthernet0/0/3.166
 ---------------------------------------
 VMAC           0007.b422.14d6
 VIP            203.0.113.6
 Shut           no shut
 Decrement      10

 interface      TwoGigabitEthernet0/0/2.166
 ---------------------------------------
 VMAC           0007.b422.0d06
 VIP            203.0.113.9
 Shut           no shut
 Decrement      10
```

The examples shows configuration details for redundancy application interface manager group 1 and group 2:

```
Router# show redundancy application if-mgr group 1

 RG ID: 1
 ==========

 interface      TwoGigabitEthernet0/0/3.152
 ---------------------------------------
 VMAC          0007.b421.4e21
 VIP           203.0.113.3
 Shut          shut
 Decrement     10

 interface     TwoGigabitEthernet0/0/2.152
 ---------------------------------------
 VMAC          0007.b421.5209
 VIP           203.0.113.2
 Shut          shut
 Decrement     10

Router# show redundancy application if-mgr group 2
 RG ID: 2
 ==========

 interface    TwoGigabitEthernet0/0/3.166
 ---------------------------------------
 VMAC          0007.b422.14d6
 VIP           203.0.113.5
 Shut          no shut
 Decrement     10

 interface     TwoGigabitEthernet0/0/2.166
 ---------------------------------------
 VMAC          0007.b422.0d06
 VIP           203.0.113.7
 Shut          no shut
 Decrement     10
```

The example shows configuration details for redundancy application data-interface group:

```
Router# show redundancy application data-interface group
The data interface for rg[1] is TwoGigabitEthernet0/0/1
The data interface for rg[2] is TwoGigabitEthernet0/0/1
```

The examples show configuration details specific to redundancy application data-interface group 1 and group 2:

```
Router# show redundancy application data-interface group 1
The data interface for rg[1] is TwoGigabitEthernet0/0/1

Router # show redundancy application data-interface group 2
The data interface for rg[2] is TwoGigabitEthernet0/0/1
```

Verify BFD Offload

Use these commands to verify and monitor BFD offload feature on your device.

Note Configuration of BFD Offload is described in Configure Bidirectional Forwarding, on page 180.

- **show bfd neighbors [details]**
- **debug bfd [packet | event]**
- **debug bfd event**

The **show bfd neighbors** command displays the BFD adjacency database:

```
Router# show bfd neighbor

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.1                            362/1277       Up        Up        Gi0/0/1.2
192.0.2.5                            445/1278       Up        Up        Gi0/0/1.3
192.0.2.3                           1093/961        Up        Up        Gi0/0/1.4
192.0.2.2                           1244/946        Up        Up        Gi0/0/1.5
192.0.2.6                           1094/937        Up        Up        Gi0/0/1.6
192.0.2.7                           1097/1260       Up        Up        Gi0/0/1.7
192.0.2.4                           1098/929        Up        Up        Gi0/0/1.8
192.0.2.9                           1111/928        Up        Up        Gi0/0/1.9
192.0.2.8                           1100/1254       Up        Up        Gi0/0/1.10
```

The **debug bfd neighbor detail** command displays the debugging information related to BFD packets:

```
Router# show bfd neighbor detail

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.1                            362/1277       Up        Up        Gi0/0/1.2
Session state is UP and not using echo function.
Session Host: Hardware
OurAddr: 192.0.2.2
Handle: 33
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 50(0)
Rx Count: 3465, Rx Interval (ms) min/max/avg: 42/51/46
Tx Count: 3466, Tx Interval (ms) min/max/avg: 39/52/46
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: CEF EIGRP
Uptime: 00:02:50
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 1
             Multiplier: 3               - Length: 24
             My Discr.: 1277             - Your Discr.: 362
             Min tx interval: 50000      - Min rx interval: 50000
             Min Echo interval: 0
```

The **show bfd summary** command displays the BFD summary:

```
Router# show bfd summary

                    Session          Up          Down

Total                   400         400             0
```

The **show bfd drops** command displays the number of packets dropped in BFD:

```
Router# show bfd drops
BFD Drop Statistics
                      IPV4     IPV6    IPV4-M    IPV6-M    MPLS_PW   MPLS_TP_LSP
Invalid TTL             0         0       0         0           0       0
BFD Not Configured      0         0       0         0           0       0
No BFD Adjacency        33        0       0         0           0       0
Invalid Header Bits     0         0       0         0           0       0
Invalid Discriminator   1         0       0         0           0       0
Session AdminDown       94        0       0         0           0       0
Authen invalid BFD ver  0         0       0         0           0       0
Authen invalid len      0         0       0         0           0       0
Authen invalid seq      0         0       0         0           0       0
Authen failed           0         0       0         0           0       0
```

The **debug bfd packet** command displays debugging information about BFD control packets.

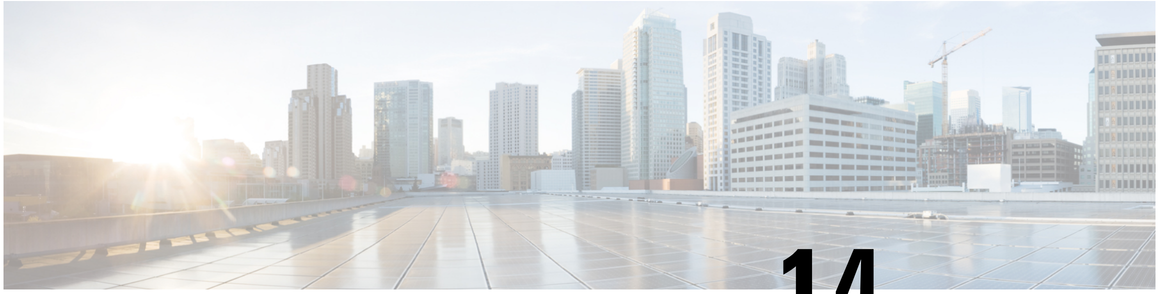
```
Router# debug bfd packet
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/0 diag:0(No Diagnostic)
 Down C cnt:4 ttl:254 (0)
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:983/1941 diag:3(Neighbor
Signaled Session Down) Init  C cnt:44 (0)
*Nov 12 23:08:28.007: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/983 diag:0(No Diagnostic)
 Up PC cnt:4 ttl:254 (0)
*Nov 12 23:08:28.007: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:983/1941 diag:0(No Diagnostic)
 Up F C cnt:0 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/983 diag:0(No Diagnostic)
 Up FC cnt:0 ttl:254 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:983/1941 diag:0(No Diagnostic)
 Up  C cnt:0 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/0 diag:0(No Diagnostic)
 Down C cnt:3 ttl:254 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Tx IP:192.0.2.3 ld/rd:993/1907 diag:3(Neighbor
Signaled Session Down) Init  C cnt:43 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/983 diag:0(No Diagnostic)
 Up C cnt:0 ttl:254 (0)
*Nov 12 23:08:28.626: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/993 diag:0(No Diagnostic)
 Up PC cnt:3 ttl:254 (0)
*Nov 12 23:08:28.626: BFD-DEBUG Packet: Tx IP:192.0.2.3 ld/rd:993/1907 diag:0(No Diagnostic)
 Up F C cnt:0 (0)
*Nov 12 23:08:28.645: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/993 diag:0(No Diagnostic)
 Up C cnt:0 ttl:254 (0)
*Nov 12 23:08:28.700: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/993 diag:0(No Diagnostic)
 Up FC cnt:0 ttl:254 (0)
*Nov 12 23:08:28.700: BFD-DEBUG Packet: Tx IP:192.0.2.3 ld/rd:993/1907 diag:0(No Diagnostic)
 Up  C cnt:0 (0)
*Nov 12 23:08:28.993: BFD-DEBUG Packet: Rx IP:192.0.2.3 ld/rd:1907/993 diag:0(No Diagnostic)
 Up C cnt:0 ttl:254 (0)
```

The **debug bfd event** displays debugging information about BFD state transitions:

```
Router# deb bfd event

*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.6, ld:1401, handle:77,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.6, ld:1401, handle:77,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.10, ld:1400, handle:39,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.10, ld:1400, handle:39,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.8, ld:1399, handle:25,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.8, ld:1399, handle:25,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.5, ld:1403, handle:173,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.6, ld:1403, handle:173,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.4, ld:1402, handle:95,
 event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.4, ld:1402, handle:95,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Timers: Tx timer 1000000 Detect timer 0
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Flags: Poll 0 Final 0
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Buffer: 0x23480318 0x0000057C 0x00000000
0x000F4240 0x000F4240 0x00000000 size 24
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Timers: Tx timer 1000000 Detect timer 0
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Flags: Poll 0 Final 0
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Buffer: 0x23480318 0x0000057D 0x00000000
```

```
0x000F4240 0x000F4240 0x00000000 size 24
*Nov 12 23:11:30.649: BFD-DEBUG Packet: Rx IP:192.0.2.6 ld/rd:1601/1404
diag:7(Administratively Down) AdminDown C cnt:0 ttl:254 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: V1 FSM ld:1404 handle:207 event:RX ADMINDOWN state:UP
 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: resetting timestamps ld:1404 handle:207 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.1, ld:1404, handle:207,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:1404/0 diag:3(Neighbor Signaled
 Session Down) Down C cnt:0 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1620/1405
diag:7(Administratively Down) AdminDown C cnt:0 ttl:254 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: V1 FSM ld:1405 handle:209 event:RX ADMINDOWN state:UP
 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: resetting timestamps ld:1405 handle:209 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.1, ld:1405, handle:209,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Tx IP:192.0.2.7 ld/rd:1405/0 diag:3(Neighbor Signaled
 Session Down) Down C cnt:0 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.7, ld:1404, handle:207,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.7, ld:1404, handle:207,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.7, ld:1405, handle:209,
 event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.7, ld:1405, handle:209,
 event:DOWN adminDown, (0)
*Nov 12 23:11:31.035: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 192.0.2.8
```



CHAPTER 14

Configure Secure Storage

Secure Storage feature allows you to secure critical configuration information by encrypting it. It encrypts VPN, IPSec, and other asymmetric key-pairs, pre-shared secrets, the type 6 password encryption key and certain credentials. An instance-unique encryption key is stored in the hardware trust anchor to prevent it from being compromised.

By default, this feature is enabled on platforms that come with a hardware trust anchor. This feature is not supported on platforms that do not have hardware trust anchor.

Enable Secure Storage

Before you begin

By default, this feature is enabled on a platform. Use this procedure on a platform where it is disabled.

Procedure

Step 1 Config terminal

Example:

```
router#config terminal
```

Enters the configuration mode.

Step 2 service private-config-encryption

Example:

```
router(config)# service private-config-encryption
```

Enables the Secure Storage feature on your platform.

Step 3 do write memory

Example:

```
router(config)# do write memory
```

Encrypts the private-config file and saves the file in an encrypted format.

Example

This example shows how to enable Secure Storage:

```
router#config terminal
router(config)# service private-config-encryption
router(config)# do write memory
```

Disable Secure Storage

Before you begin

To disable Secure Storage feature on a platform, perform this task:

Procedure

Step 1 Config terminal

Example:

```
router#config terminal
```

Enters the configuration mode.

Step 2 no service private-config-encryption

Example:

```
router(config)# no service private-config-encryption
```

Disables the Secure Storage feature on your platform.

Step 3 do write memory

Example:

```
router(config)# do write memory
```

Decrypts the private-config file and saves the file in plane format.

Example

This example shows how to disable Secure Storage:

```
router#config terminal
router(config)# no service private-config-encryption
router(config)# do write memory
```

Verify the status of encryption

Use the **show parser encrypt file status** command to verify the status of encryption. This command output indicates that the feature is available but the file is not encrypted. The file is in ‘plain text’ format.

```
router#show parser encrypt file status
Feature: Enabled
File Format: Plain Text
Encryption Version: Ver1
```

This command output indicates that the feature is enabled and the file is encrypted. The file is in ‘cipher text’ format.

```
router#show parser encrypt file status
Feature: Enabled
File Format: Cipher Text
Encryption Version: Ver1
```

Verify the platform identity

Use the **show platform sudi certificate** command to display the SUDI certificate in standard PEM format. The command output helps you verify the platform identity.

In the command output, the first certificate is the Cisco Root CA 2048 and the second is the Cisco subordinate CA (ACT2 SUDI CA). The third is the SUDI certificate.

```
router#show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
```

```
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 MIIDhzCCAm+gAwIBAgIEAJT3DDANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE1MTExNDA5MzMzN1oXDTI1
MTExNDA5MzMzN1owczEsMCoGA1UEBRMjUElEOldTLUMzNjUwLTEyWDQ4VVEgU046
RkRPMTk0NkJHMDUxDjAMBgNVBAoTBUNpc2NvMRgwFgYDVQQLEw9BQ1QtMiBMaXRl
IFNVREkxGTAXBgNVBAMTEFdTLUMzNjUwLTEyWDQ4VVEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC6SARWyImWrRV/x7XQogAE+02WmzKki+4arMVBvl9o
GgvJfkoJDdaHOROSUkEE3qXtd8N3lfKy3TZ+jtHD85m2aGz6+IRx/e/lLsQzi6dl
WIB+N94pgecFBONPR9wJriox1IGD3B43b0hMLkmro4R5Zrs8XFkDo9k1tBU7F2O7
GEzb/WkO5NLexznef2Niglx9fCDL0HC27BbsR5+03p8jhG0+mvrp8M9du1HKiGin
ZIV4XgTMp1/k/TVaIepEGZuWM3hxdUZjkNGG1c1m+oB8vLX3UlSL76sDBBoiaprD
rjXBgBIozyFW8tTjh50jMDG84hKD5s31ifOe4KpqEcnVAgMBAAGjbzBtMA4GA1Ud
DwEB/wQEAwIF4DAMBgNVHRMBAf8EAjAAME0GA1UdEQRGMESgQgYJKwYBBAEJFQID
oDUTM0NoaXBJRD1VWUpOTlZJMENBUkhVM1Z1SUVSbFl5QXlPQ0F4TXpvek5Ub3lN
U0EwS0NnPTANBgkqhkiG9w0BAQsFAAOCAQEADjtM8vdlf+p1WKSKX1C1qQ4aEnD5
p8T5e4iTer7Y1fbCrHIEEm3mnip+568j299z0H8V7PDp1ljuLHyMFTC+945F9RfA
eAuVWVb5A9dnGL8MssBJe2lVSnZwrWkT1EIdxLYrTiPAQHtll6CN77S4u/f71oYE
tzPE5AGfyGw7ro1MEPVGffaQmYUDAwKFNBH1uI7c2S1qlwk4WWZ6xxci+lhaQnIG
pWzapaiAYL1XrcBz4KwFc1ZZpQT6hHw24jzYaYimvCo+/kSKuA9xNdtSu18ycox0
zKnXQ17s6aChMMt7Y8Nh4iz9BDejoOF6/b3sM0wRi+2/4j+6/GhcMRs0Og==
-----END CERTIFICTAE
Signature version: 1
Signature:
405C70D802B73947EDBF8D0D2C8180F10D4B3EF9694514219C579D2ED52F7D583E0F40813FC4E9F549B2EB1C21725F7C
B1C79F98271E47E780E703E67472380FB52D4963E1D1FB9787B38E28B8E696570A180B7A2F131B1F174EA79F5DB4765DF67386126D8
9E07EDF6C26E0A81272EA1437D03F2692937082756AE1F1BFAFBFACD6BE9CF9C84C961FACE9FA0FE64D85AE4FA086969D0702C536ABD
B8FBFDC47C14C17D02FEBF4F7F5B24D2932FA876F56B4C07816270A0B4195C53D975C85AEAE3A74F2DBF293F52423ECB7B853967080A
9C57DA3E4B08B2B2CA623B2CBAF7080A0AEB09B2E5B756970A3A27E0F1D17C8A243
```

CHAPTER 15

Configure Call Home

The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, and use of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

This chapter includes these sections:

Find feature information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use the Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. A Cisco account is not required to access the Cisco Feature Navigator.

Prerequisites for Call Home

These are the prerequisites before you configure Call Home:

- Contact e-mail address (required for full registration with Smart Call Home, optional if Call Home is enabled in anonymous mode), phone number (optional), and street address information (optional) should be configured so that the receiver can determine the origin of messages received.

- At least one destination profile (predefined or user-defined) must be configured. The destination profile you use depends on whether the receiving entity is a pager, an e-mail address, or an automated service such as Cisco Smart Call Home.

  If the destination profile uses e-mail message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server.

- The router must have IP connectivity to an e-mail server or the destination HTTP server.
- If Cisco Smart Call Home is used, an active service contract covering the device is required to provide full Cisco Smart Call Home service.

Information about Call Home

The Call Home feature can deliver alert messages containing information on configuration, environmental conditions, inventory, syslog, snapshot, and crash events. It provides these alert messages as either e-mail-based or web-based messages. Multiple message formats are available, allowing for compatibility with pager services, standard e-mail, or XML-based automated parsing applications. This feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles, each with configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC (callhome@cisco.com). You can also define your own destination profiles.

Flexible message delivery and format options make it easy to integrate specific support requirements.

This section contains these subsections:

- Benefits of Using Call Home
- Obtaining Smart Call Home Services

Benefits of Call Home

The Call Home feature offers these benefits:

- Multiple message-format options, which include:

  Short Text—Suitable for pagers or printed reports.

  Plain Text—Full formatted message information suitable for human reading.

  XML—Machine-readable format using XML and Adaptive Markup Language (AML) document type definitions (DTDs). The XML format enables communication with the Cisco TAC.

- Multiple concurrent message destinations.
- Multiple message categories including configuration, environmental conditions, inventory, syslog, snapshot, and crash events.
- Filtering of messages by severity and pattern matching.
- Scheduling of periodic message sending.

Obtaining Smart Call Home services

If you have a service contract directly with Cisco, you can register for the Smart Call Home service. Smart Call Home analyzes Smart Call Home messages and provides background information and recommendations. For known issues, particularly online diagnostics failures, Automatic Service Requests are generated with the Cisco TAC.

Smart Call Home offers these features:

- Continuous device health monitoring and real-time diagnostic alerts.
- Analysis of Smart Call Home messages and, if needed, Automatic Service Request generation routed to the correct TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device or through an HTTP proxy server or a downloadable Transport Gateway (TG). You can use a TG aggregation point to support multiple devices or in cases where security dictates that your devices may not be connected directly to the Internet.
- Web-based access to Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices provides access to associated field notices, security advisories, and end-of-life information.

You need the following items to register for Smart Call Home:

- SMARTnet contract number for your router
- Your e-mail address
- Your Cisco.com username

For more information about Smart Call Home, see https://supportforums.cisco.com/community/4816/smart-call-home.

Anonymous Reporting

Smart Call Home is a service capability included with many Cisco service contracts and is designed to assist customers resolve problems more quickly. In addition, the information gained from crash messages helps Cisco understand equipment and issues occurring in the field. If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your customer identity will remain anonymous, and no identifying information will be sent.

Note When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to Cisco or to vendors operating on behalf of Cisco (including countries outside the United States). Cisco maintains the privacy of all customers. For information about how Cisco treats personal information, see the Cisco Privacy Statement at http://www.cisco.com/web/siteassets/legal/privacy.html.

When Call Home is configured in an anonymous way, only crash, inventory, and test messages are sent to Cisco. No customer identifying information is sent.

For more information about what is sent in these messages, see Alert Group trigger events and commands, on page 233.

How to configure Call Home

These sections show how to configure Call Home using a single command:

- Configure Smart Call Home (Single Command), on page 198
- Configure and Enable Smart Call Home, on page 199

These sections show detailed or optional configurations:

- Enable and Disable Call Home, on page 199
- Configure contact information, on page 200
- Configure destination profiles, on page 201
- Subscribe to alert groups, on page 205
- Configure general e-mail options, on page 210
- Specify rate limit for sending Call Home messages, on page 212
- Specify HTTP proxy server, on page 212
- Enable AAA authorization to run IOS commands for Call Home messages, on page 213
- Configure syslog throttling, on page 214
- Configure Call Home data privacy, on page 214
- Send Call Home communications manually, on page 215

Configure Smart Call Home (Single Command)

To enable all Call Home basic configurations using a single command, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*]

Example:

```
Router(config)# call-home reporting contact-email-addr email@company.com
```

Enables the basic configurations for Call Home using a single command.

- **anonymous**—Enables Call-Home TAC profile to send only crash, inventory, and test messages and send the messages anonymously.
- **contact-email-addr**—Enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process.
- **http-proxy** {*ipv4-address* | *ipv6-address* | *name*}—Configures an ipv4 or ipv6 address or server name. Maximum length is 64 characters.
- **port** *port-number*—Port number.

  Range is 1 to 65535.

Note

The HTTP proxy option allows you to make use of your own proxy server to buffer and secure Internet connections from your devices.

Note

After successfully enabling Call Home either in anonymous or full registration mode using the **call-home reporting** command, an inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out. For more information about what is sent in these messages, see Alert Group trigger events and commands, on page 233.

Configure and Enable Smart Call Home

For application and configuration information about the Cisco Smart Call Home service, see the "Getting Started" section of the Smart Call Home User Guide at https://supportforums.cisco.com/community/4816/smart-call-home. This document includes configuration examples for sending Smart Call Home messages directly from your device or through a transport gateway (TG) aggregation point.

Note For security reasons, we recommend that you use the HTTPS transport options, due to the additional payload encryption that HTTPS offers. The Transport Gateway software is downloadable from Cisco.com and is available if you require an aggregation point or a proxy for connection to the Internet.

Enable and Disable Call Home

To enable or disable the Call Home feature, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **service call-home**

Example:

```
Router(config)# service call-home
```

Enables the Call Home feature.

Step 3 **no service call-home**

Example:

```
Router(config)# no service call-home
```

Disables the Call Home feature.

Configure contact information

Each router must include a contact e-mail address (except if Call Home is enabled in anonymous mode). You can optionally include a phone number, street address, contract ID, customer ID, and site ID.

To assign the contact information, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters the Call Home configuration submode.

Step 3 **contact-email-addr** *email-address*

Example:

```
Router(cfg-call-home)# contact-email-addr username@example.com
```

Designates your e-mail address. Enter up to 200 characters in e-mail address format with no spaces.

Step 4 **phone-number** +*phone-number*

Example:

```
Router(cfg-call-home)# phone-number +1-800-555-4567
```

(Optional) Assigns your phone number.

Note

The number must begin with a plus (+) prefix and may contain only dashes (-) and numbers. Enter up to 17 characters. If you include spaces, you must enclose your entry in quotes (“”).

Step 5 **street-address** *street-address*

Example:

```
Router(cfg-call-home)# street-address "1234 Picaboo Street, Any city, Any state, 12345"
```

(Optional) Assigns your street address where RMA equipment can be shipped. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes (“”).

Step 6 **customer-id** *text*

Example:

```
Router(cfg-call-home)# customer-id Customer1234
```

(Optional) Identifies customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes (“”).

Step 7 **site-id** *text*

Example:

```
Router(cfg-call-home)# site-id Site1ManhattanNY
```

(Optional) Identifies customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes (“”).

Step 8 **contract-id** *text*

Example:

```
Router(cfg-call-home)# contract-id Company1234
```

(Optional) Identifies your contract ID for the router. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes (“”).

Example

This example shows how to configure contact information:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
Router(cfg-call-home)# phone-number +1-800-555-4567
Router(cfg-call-home)# street-address "1234 Picaboo Street, Any city, Any state, 12345"
Router(cfg-call-home)# customer-id Customer1234
Router(cfg-call-home)# site-id Site1ManhattanNY
Router(cfg-call-home)# contract-id Company1234
Router(cfg-call-home)# exit
```

Configure destination profiles

A destination profile contains the required delivery information for an alert notification. At least one destination profile is required. You can configure multiple destination profiles of one or more types.

You can create and define a new destination profile or copy and use the predefined destination profile. If you define a new destination profile, you must assign a profile name.

Note If you use the Cisco Smart Call Home service, the destination profile must use the XML message format.

You can configure the following attributes for a destination profile:

- Profile name—String that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case-sensitive.

Note You cannot use **all** as a profile name.

- Transport method—Transport mechanism, either e-mail or HTTP (including HTTPS), for delivery of alerts.
    - For user-defined destination profiles, e-mail is the default, and you can enable either or both transport mechanisms. If you disable both methods, e-mail is enabled.
    - For the predefined Cisco TAC profile, you can enable either transport mechanism, but not both.
- Destination address—The actual address related to the transport method to which the alert should be sent.
- Message formatting—The message format used for sending the alert. The format options for a user-defined destination profile are long-text, short-text, or XML. The default is XML. For the predefined Cisco TAC profile, only XML is allowed.
- Message size—The maximum destination message size. The valid range is 50 to 3,145,728 Bytes. The default is 3,145,728 Bytes.

  Anonymous reporting—You can choose for your customer identity to remain anonymous, and no identifying information is sent.
- Subscribing to interesting alert-groups—You can choose to subscribe to alert-groups highlighting your interests.

This section contains these subsections:

- Create a new destination profile, on page 202
- Copy a destination profile, on page 204
- Set profiles to anonymous mode, on page 204

Create a new destination profile

To create and configure a new destination profile, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters the Call Home configuration submode.

Step 3 **profile** *name*

Example:

```
Router(config-call-home)# profile profile1
```

Enters the Call Home destination profile configuration submode for the specified destination profile. If the specified destination profile does not exist, it is created.

Step 4 [**no**] **destination transport-method** {**email** | **http**}

Example:

```
Router(cfg-call-home-profile)# destination transport-method email
```

(Optional) Enables the message transport method. The **no** option disables the method.

Step 5 **destination address** {**email** *email-address* | **http** *url*}

Example:

```
Router(cfg-call-home-profile)# destination address email myaddress@example.com
```

Configures the destination e-mail address or URL to which Call Home messages are sent.

Note
When entering a destination URL, include either **http://** or **https://**, depending on whether the server is a secure server.

Step 6 **destination preferred-msg-format** {**long-text** | **short-text** | **xml**}

Example:

```
Router(cfg-call-home-profile)# destination preferred-msg-format xml
```

(Optional) Configures a preferred message format. The default is XML.

Step 7 **destination message-size-limit** *bytes*

Example:

```
Router(cfg-call-home-profile)# destination message-size-limit 3145728
```

(Optional) Configures a maximum destination message size for the destination profile.

Step 8 **active**

Example:

```
Router(cfg-call-home-profile)# active
```

Enables the destination profile. By default, the profile is enabled when it is created.

Step 9 **end**

Example:

```
Router(cfg-call-home-profile)# end
```

Returns to privileged EXEC mode.

Step 10 **show call-home profile** {*name* | **all**}

Example:

```
Router# show call-home profile profile1
```

Displays the destination profile configuration for the specified profile or all configured profiles.

Copy a destination profile

To create a new destination profile by copying an existing profile, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters the Call Home configuration submode.

Step 3 **copy profile** *source-profile target-profile*

Example:

```
Router(cfg-call-home)# copy profile profile1 profile2
```

Creates a new destination profile with the same configuration settings as the existing destination profile.

Set profiles to anonymous mode

To set an anonymous profile, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters the Call Home configuration submode.

Step 3 **profile** *name*

Example:

```
Router(cfg-call-home) profile Profile-1
```

Enables the profile configuration mode.

Step 4 **anonymous-reporting-only**

Example:

```
Router(cfg-call-home-profile)# anonymous-reporting-only
```

Sets the profile to anonymous mode.

Note
By default, Call Home sends a full report of all types of events subscribed in the profile. When **anonymous-reporting-only** is set, only crash, inventory, and test messages will be sent.

Subscribe to alert groups

An alert group is a predefined subset of Call Home alerts supported in all routers. Different types of Call Home alerts are grouped into different alert groups depending on their type. These alert groups are available:

- Crash
- Configuration
- Environment
- Inventory
- Snapshot
- Syslog

This section contains these subsections:

- Periodic notification, on page 208
- Message severity threshold, on page 208
- Configure a snapshot command list, on page 209

The triggering events for each alert group are listed in Alert Group trigger events and commands, on page 233, and the contents of the alert group messages are listed in Message Contents, on page 240.

You can select one or more alert groups to be received by a destination profile.

Note A Call Home alert is only sent to destination profiles that have subscribed to the alert group containing that Call Home alert. In addition, the alert group must be enabled.

To subscribe a destination profile to one or more alert groups, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog** | **crash** | **snapshot**}

Example:

```
Router(cfg-call-home)# alert-group all
```

Enables the specified alert group. Use the keyword **all** to enable all alert groups. By default, all alert groups are enabled.

Step 4 **profile** *name*

Example:

```
Router(cfg-call-home)# profile profile1
```

Enters the Call Home destination profile configuration submode for the specified destination profile.

Step 5 **subscribe-to-alert-group all**

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group all
```

Subscribes to all available alert groups using the lowest severity.

You can subscribe to alert groups individually by specific type, as described in Step 6 through Step 11.

Note
This command subscribes to the syslog debug default severity. This causes a large number of syslog messages to generate. You should subscribe to alert groups individually, using appropriate severity levels and patterns when possible.

Step 6 **subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group configuration
periodic daily 12:00
```

Subscribes this destination profile to the Configuration alert group. The Configuration alert group can be configured for periodic notification, as described in Periodic notification, on page 208.

Step 7 **subscribe-to-alert-group environment** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major
```

Subscribes this destination profile to the Environment alert group. The Environment alert group can be configured to filter messages based on severity, as described in Message severity threshold, on page 208.

Step 8 **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic monthly 1 12:00
```

Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification, as described in Periodic notification, on page 208.

Step 9 **subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major
```

Subscribes this destination profile to the Syslog alert group. The Syslog alert group can be configured to filter messages based on severity, as described in Message severity threshold, on page 208.

You can specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message is sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it in quotes (""). You can specify up to five patterns for each destination profile.

Step 10 **subscribe-to-alert-group crash**

Example:

```
Router(cfg-call-home-profile)# [no | default]
subscribe-to-alert-group crash
```

Subscribes to the Crash alert group in user profile. By default, TAC profile subscribes to the Crash alert group and cannot be unsubscribed.

Step 11 **subscribe-to-alert-group snapshot periodic** {**daily** *hh:mm* | **hourly** *mm* | **interval** *mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00
```

Subscribes this destination profile to the Snapshot alert group. The Snapshot alert group can be configured for periodic notification, as described in Periodic notification, on page 208.

By default, the Snapshot alert group has no command to run. You can add commands into the alert group, as described in Configure a snapshot command list, on page 209. In doing so, the output of the commands added in the Snapshot alert group will be included in the snapshot message.

Step 12 **exit**

Example:

```
Router(cfg-call-home-profile)# exit
```

Exits the Call Home destination profile configuration submode.

Periodic notification

When you subscribe a destination profile to the Configuration, Inventory, or Snapshot alert group, you can choose to receive the alert group messages asynchronously or periodically at a specified time. The sending period can be set to one of these options:

- Daily—Specifies the time of day to send, using an hour:minute format *hh:mm*, with a 24-hour clock (for example, 14:30).
- Weekly—Specifies the day of the week and time of day in the format *day hh:mm*, where the day of the week is spelled out (for example, Monday).
- Monthly—Specifies the numeric date, from 1 to 31, and the time of day, in the format *date hh:mm*.
- Interval—Specifies the interval at which the periodic message is sent, from 1 to 60 minutes.
- Hourly—Specifies the minute of the hour at which the periodic message is sent, from 0 to 59 minutes.

Note Hourly and by interval periodic notifications are available for the Snapshot alert group only.

Message severity threshold

When you subscribe a destination profile to the Environment or Syslog alert group, you can set a threshold for the sending of alert group messages based on the level of severity of the message. Any message with a value lower than the destination profile specified threshold is not sent to the destination.

The severity threshold is configured using the keywords listed in the following table. The severity threshold ranges from catastrophic (level 9, highest level of urgency) to debugging (level 0, lowest level of urgency). If no severity threshold is configured for the Syslog or Environment alert groups, the default is debugging (level 0). The Configuration and Inventory alert groups do not allow severity configuration; severity is always set as normal.

Note Call Home severity levels are not the same as system message logging severity levels.

Table 15: Severity and Syslog level mapping

Level	Keyword	Syslog level	Description
9	catastrophic	—	Network-wide catastrophic failure.
8	disaster	—	Significant network impact.
7	fatal	Emergency (0)	System is unusable.
6	critical	Alert (1)	Critical conditions, immediate attention needed.
5	major	Critical (2)	Major conditions.
4	minor	Error (3)	Minor conditions.
3	warning	Warning (4)	Warning conditions.
2	notification	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	normal	Information (6)	Normal event signifying return to normal state.
0	debugging	Debug (7)	Debugging messages.

Configure a snapshot command list

To configure a snapshot command list, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 [**no** | **default**] **alert-group-config snapshot**

Example:

```
Router(cfg-call-home)# alert-group-config snapshot
```

Enters snapshot configuration mode.

The **no** or **default** command will remove all snapshot command.

Step 4 [**no** | **default**] **add-command** *command string*

Example:

```
Router(cfg-call-home-snapshot)# add-command “show version”
```

Adds the command to the Snapshot alert group. The **no** or **default** command removes the corresponding command.

- *command string*—IOS command. Maximum length is 128.

Step 5 **exit**

Example:

```
Router(cfg-call-home-snapshot)# exit
```

Exits and saves the configuration.

Configure general e-mail options

To use the e-mail message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) e-mail server address. You can configure the from and reply-to e-mail addresses, and you can specify up to four backup e-mail servers.

Note these guidelines when configuring general e-mail options:

- Backup e-mail servers can be defined by repeating the **mail-server** command using different priority numbers.
- The **mail-server priority** number parameter can be configured from 1 to 100. The server with the highest priority (lowest priority number) is tried first.

To configure general e-mail options, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **mail-server** [{*ipv4-address* | *ipv6-address*} | *name*] **priority** *number*

Example:

```
Router(cfg-call-home)# mail-server stmp.example.com priority 1
```

Assigns an e-mail server address and its relative priority among configured e-mail servers.

Provide either of these:

- The e-mail server’s IP address.

- The e-mail server's fully qualified domain name (FQDN) of 64 characters or less.

Assign a priority number between 1 (highest priority) and 100 (lowest priority).

Step 4 **sender from** *email-address*

Example:

```
Router(cfg-call-home)# sender from username@example.com
```

(Optional) Assigns the e-mail address that appears in the from field in Call Home e-mail messages. If no address is specified, the contact e-mail address is used.

Step 5 **sender reply-to** *email-address*

Example:

```
Router(cfg-call-home)# sender reply-to username@example.com
```

(Optional) Assigns the e-mail address that appears in the reply-to field in Call Home e-mail messages.

Step 6 **source-interface** *interface-name*

Example:

```
Router(cfg-call-home)# source-interface loopback1
```

Assigns the source interface name to send call-home messages.

- *interface-name*—Source interface name. Maximum length is 64.

Note
For HTTP messages, use the **ip http client source-interface** *interface-name* command in global configuration mode to configure the source interface name. This allows all HTTP clients on the device to use the same source interface.

Step 7 **vrf** *vrf-name*

Example:

```
Router(cfg-call-home)# vrf vpn1
```

(Optional) Specifies the VRF instance to send call-home e-mail messages. If no vrf is specified, the global routing table is used.

Note
For HTTP messages, if the source interface is associated with a VRF, use the **ip http client source-interface** *interface-name* command in global configuration mode to specify the VRF instance that will be used for all HTTP clients on the device.

Example

This example shows the configuration of general e-mail parameters, including a primary and secondary e-mail server:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# mail-server smtp.example.com priority 1
Router(cfg-call-home)# mail-server 192.0.2.1 priority 2
Router(cfg-call-home)# sender from username@example.com
Router(cfg-call-home)# sender reply-to username@example.com
Router(cfg-call-home)# source-interface loopback1
Router(cfg-call-home)# vrf vpn1
Router(cfg-call-home)# exit
Router(config)#
```

Specify rate limit for sending Call Home messages

To specify the rate limit for sending Call Home messages, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **rate-limit** *number*

Example:

```
Router(cfg-call-home)# rate-limit 40
```

Specifies a limit on the number of messages sent per minute.

- *number*—Range is 1 to 60. The default is 20.

Specify HTTP proxy server

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*

Example:

```
Router(cfg-call-home)# http-proxy 192.0.2.1 port 1
```

Specifies the proxy server for the HTTP request.

Enable AAA authorization to run IOS commands for Call Home messages

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **aaa-authorization**

Example:

```
Router(cfg-call-home)# aaa-authorization
```

Enables AAA authorization.

Note
By default, AAA authorization is disabled for Call Home.

Step 4 **aaa-authorization** [**username** *username*]

Example:

```
Router(cfg-call-home)# aaa-authorization username user
```

Specifies the username for authorization.

- **username** *username*—Default username is callhome. Maximum length is 64.

Configure syslog throttling

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 [**no**] **syslog-throttling**

Example:

```
Router(cfg-call-home)# syslog-throttling
```

Enables or disables call-home syslog message throttling and avoids sending repetitive call-home syslog messages.

Note
By default, syslog message throttling is enabled.

Configure Call Home data privacy

The data-privacy command scrubs data, such as IP addresses, from running configuration files to protect the privacy of customers. Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data. Currently, the **show** command output is not being scrubbed except for configuration messages in the outputs for the **show running-config all** and the**show startup-config data** commands.

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **data-privacy** {**level** {**normal** | **high**} | **hostname**}

Example:

```
Router(cfg-call-home)# data-privacy level high
```

Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal.

Note
Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data.

- **normal**—Scrubs all normal-level commands.
- **high**—Scrubs all normal-level commands plus the IP domain name and IP address commands.
- **hostname**—Scrubs all high-level commands plus the hostname command.

Note
Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.

Send Call Home communications manually

You can manually send several types of Call Home communications. To send Call Home communications, perform the tasks in this section. This section contains these subsections:

- Send a Call Home Test Message Manually, on page 215
- Send Call Home alert group messages manually, on page 216
- Submit Call Home analysis and report requests, on page 217
- Manually send command output message for one command or a command list, on page 218

Send a Call Home Test Message Manually

You can use the **call-home test** command to send a user-defined Call Home test message.

To manually send a Call Home test message, perform these step:

Procedure

call-home test [*"test-message"*] **profile** *name*

Example:

```
Router# call-home test profile profile1
```

Sends a test message to the specified destination profile. The user-defined test message text is optional but must be enclosed in quotes (“”) if it contains spaces. If no user-defined message is configured, a default message is sent.

Send Call Home alert group messages manually

You can use the **call-home send** command to manually send a specific alert group message.

Note these guidelines when manually sending a Call Home alert group message:

- Only the crash, snapshot, configuration, and inventory alert groups can be sent manually.
- When you manually trigger a crash, snapshot, configuration, or inventory alert group message and you specify a destination profile name, a message is sent to the destination profile regardless of the profile’s active status, subscription status, or severity setting.
- When you manually trigger a crash, snapshot, configuration, or inventory alert group message and do not specify a destination profile name, a message is sent to all active profiles that have either a normal or periodic subscription to the specified alert group.

To manually trigger Call Home alert group messages, perform these steps:

Procedure

Step 1 **call-home send alert-group snapshot** [**profile** *name*]

Example:

```
Router# call-home send alert-group snapshot profile profile1
```

Sends a snapshot alert group message to one destination profile if specified, or to all subscribed destination profiles.

Step 2 **call-home send alert-group crash** [**profile** *name*]

Example:

```
Router# call-home send alert-group crash profile profile1
```

Sends a crash alert group message to one destination profile if specified, or to all subscribed destination profiles.

Step 3 **call-home send alert-group configuration** [**profile** *name*]

Example:

```
Router# call-home send alert-group configuration profile profile1
```

Sends a configuration alert group message to one destination profile if specified, or to all subscribed destination profiles.

Step 4 **call-home send alert-group inventory** [**profile** *name*]

Example:

```
Router# call-home send alert-group inventory profile profile1
```

Sends an inventory alert group message to one destination profile if specified, or to all subscribed destination profiles.

Submit Call Home analysis and report requests

You can use the **call-home request** command to submit information about your system to Cisco to receive helpful analysis and report information specific to your system. You can request a variety of reports, including security alerts, known bugs, best practices, and command references.

Note these guidelines when manually sending Call Home analysis and report requests:

- If a **profile** *name* is specified, the request is sent to the profile. If no profile is specified, the request is sent to the Cisco TAC profile. The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.
- The **ccoid** *user-id* is the registered identifier of the Smart Call Home user. If the *user-id* is specified, the response is sent to the e-mail address of the registered user. If no *user-id* is specified, the response is sent to the contact e-mail address of the device.
- Based on the keyword specifying the type of report requested, the following information is returned:
  - **config-sanity**—Information on best practices as related to the current running configuration.
  - **bugs-list**—Known bugs in the running version and in the currently applied features.
  - **command-reference**—Reference links to all commands in the running configuration.
  - **product-advisory**—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect the devices in your network.

To submit a request for analysis and report information from the Cisco Output Interpreter tool, perform these steps:

Procedure

Step 1 **call-home request output-analysis** *"show-command"* [**profile** *name*] [**ccoid** *user-id*]

Example:

```
Router# call-home request output-analysis "show diag" profile TG
```

Sends the output of the specified show command for analysis. The show command must be contained in quotes ("").

Step 2 **call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*]

Example:

```
Router# call-home request config-sanity profile TG
```

Sends the output of a predetermined set of commands such as the **show running-config all**, **show version** or **show module** commands, for analysis. In addition, the **call home request product-advisory** sub-command includes all inventory alert group commands. The keyword specified after **request** specifies the type of report requested.

Example

This example shows a request for analysis of a user-specified **show** command:

```
Router# call-home request output-analysis "show diag" profile TG
```

Manually send command output message for one command or a command list

You can use the **call-home send** command to execute an IOS command or a list of IOS commands and send the command output through HTTP or e-mail protocol.

Note these guidelines when sending the output of a command:

- The specified IOS command or list of IOS commands can be any run command, including commands for all modules. The command must be contained in quotes (“”).
- If the e-mail option is selected using the “email” keyword and an e-mail address is specified, the command output is sent to that address. If neither the e-mail nor the HTTP option is specified, the output is sent in long-text format with the specified service request number to the Cisco TAC (attach@cisco.com).
- If neither the “email” nor the “http” keyword is specified, the service request number is required for both long-text and XML message formats and is provided in the subject line of the e-mail.
- If the HTTP option is specified, the CiscoTac-1 profile destination HTTP or HTTPS URL is used as the destination. The destination e-mail address can be specified so that Smart Call Home can forward the message to the e-mail address. The user must specify either the destination e-mail address or an SR number but they can also specify both.

To execute a command and send the command output, perform these step:

Procedure

call-home send {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*]

Example:

```
Router# call-home send “show version;show running-config;show inventory” email support@example.com
msg-format xml
```

Executes the CLI or CLI list and sends output via e-mail or HTTP.

- {*cli command* | *cli list*}—Specifies the IOS command or list of IOS commands (separated by ‘;’). It can be any run command, including commands for all modules. The commands must be contained in quotes (“”).
- **email** *email* **msg-format {long-text | xml}**—If the **email** option is selected, the command output will be sent to the specified e-mail address in long-text or XML format with the service request number in the subject. The e-mail

address, the service request number, or both must be specified. The service request number is required if the e-mail address is not specified (default is attach@cisco.com for long-text format and callhome@cisco.com for XML format).

- **http** {**destination-email-address** *email*}—If the **http** option is selected, the command output will be sent to Smart Call Home backend server (URL specified in TAC profile) in XML format.

  destination-email-address *email* can be specified so that the backend server can forward the message to the e-mail address. The e-mail address, the service request number, or both must be specified.

- **tac-service-request** *SR#*—Specifies the service request number. The service request number is required if the e-mail address is not specified.

Example

This example shows how to send the output of a command to a user-specified e-mail address:

```
Router# call-home send “show diag” email support@example.com
```

This example shows the command output sent in long-text format to attach@cisco.com, with the SR number specified:

```
Router# call-home send “show version; show run” tac-service-request 123456
```

This example shows the command output sent in XML message format to callhome@cisco.com:

```
Router# call-home send “show version; show run” email callhome@cisco.com msg-format xml
```

This example shows the command output sent in XML message format to the Cisco TAC backend server, with the SR number specified:

```
Router# call-home send “show version; show run” http tac-service-request 123456
```

This example shows the command output sent to the Cisco TAC backend server through the HTTP protocol and forwarded to a user-specified email address:

```
Router# call-home send “show version; show run” http destination-email-address
user@company.com
```

Configure Diagnostic Signatures

The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customers networks.

Information about Diagnostic Signatures

Diagnostic Signatures

Diagnostic signatures (DS) for the Call Home system provides a flexible framework that allows the defining of new events and corresponding CLIs that can analyze these events without upgrading the Cisco software.

Diagnostic Signature provides the ability to define more types of events and trigger types than the standard Call Home feature supports. The Diagnostic Signature subsystem downloads and processes files on a device as well as handles callbacks for diagnostic signature events.

The Diagnostic Signature feature downloads digitally signed signatures that are in the form of files to devices. DS files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

DS files contain XML data to specify the event description, and these files include CLI commands or scripts to perform required actions. These files are digitally signed by Cisco or a third party to certify their integrity, reliability, and security.

The structure of a DS file can be in one of these formats:

- Metadata-based simple signature that specifies the event type and contains other information that can be used to match the event and perform actions such as collecting information by using the CLI. The signature can also change configurations on the device as a workaround for certain bugs.
- Embedded Event Manager (EEM) Tool Command Language (Tcl) script-based signature that specifies new events in the event register line and additional action in the Tcl script.
- Combination of both the formats above.

The basic information contained in a DS file:

- **ID (unique number)**—Unique key that represents a DS file that can be used to search a DS.
- **Name (ShortDescription)**—Unique description of the DS file that can be used in lists for selection.
- **Description**—Long description about the signature.
- **Revision**—Version number, which increments when the DS content is updated.
- **Event & Action**—Defines the event to be detected and the action to be performed after the event happens.

Prerequisites for Diagnostic Signatures

Before you download and configure diagnostic signatures (DSs) on a device, you must ensure that these conditions are met:

- You must assign one or more DSs to the device. For more information on how to assign DSs to devices, see Download Diagnostic Signatures, on page 221.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. You must install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.

Note If you configure the trustpool feature, the CA certificate is not required.

Download Diagnostic Signatures

To download the diagnostic signature (DS) file, you require the secure HTTP (HTTPS) protocol. If you have already configured an email transport method to download files on your device, you must change your assigned profile transport method to HTTPS to download and use DS.

Cisco software uses a PKI Trustpool Management feature, which is enabled by default on devices, to create a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs). The trustpool feature installs the CA certificate automatically. The CA certificate is required for the authentication of the destination HTTPS servers.

There are two types of DS update requests to download DS files: regular and forced-download. Regular download requests DS files that were recently updated. You can trigger a regular download request either by using a periodic configuration or by initiating an on-demand CLI. The regular download update happens only when the version of the requested DS is different from the version of the DS on the device. Periodic download is only started after there is any DS assigned to the device from DS web portal. After the assignment happens, the response to the periodic inventory message from the same device will include a field to notify device to start its periodic DS download/update. In a DS update request message, the status and revision number of the DS is included such that only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSes. You can trigger the forced-download update request only by initiating an on-demand CLI. In a force-download update request, the latest version of the DS file is downloaded irrespective of the current DS file version on the device.

The DS file is digitally signed, and signature verification is performed on every downloaded DS file to make sure it is from a trusted source.

Diagnostic Signature Workflow

The diagnostic signature feature is enabled by default in Cisco software. The workflow for using diagnostic signatures:

- Find the DS(es) you want to download and assign them to the device. This step is mandatory for regular periodic download, but not required for forced download.
- The device downloads all assigned DS(es) or a specific DS by regular periodic download or by on-demand forced download.
- The device verifies the digital signature of every single DS. If verification passes, the device stores the DS file into a non-removable disk, such as bootflash or hard disk, so that DS files can be read after the device is reloaded. On the router, the DS file is stored in the bootflash:/call home directory.
- The device continues sending periodic regular DS download requests to get the latest revision of DS and replace the older one in device.

- The device monitors the event and executes the actions defined in the DS when the event happens.

Diagnostic Signature events and actions

The events and actions sections are the key areas used in diagnostic signatures. The event section defines all event attributes that are used for event detection. The action section lists all actions which should be performed after the event happens, such as collecting show command outputs and sending them to Smart Call Home to parse.

Diagnostic Signature event detection

Event detection in a DS is defined in two ways: single event detection and multiple event detection.

Single event detection

In single event detection, only one event detector is defined within a DS. The event specification format is in one of these two types:

- DS event specification type: syslog, periodic, configuration, Online Insertion Removal (OIR) immediate, and call home are the supported event types, where “immediate” indicates that this type of DS does not detect any events, its actions are performed once it is downloaded, and the call-home type modifies the current CLI commands defined for existing alert-group.
- The Embedded Event Manager (EEM) specification type: supports any new EEM event detector without having to modify the Cisco software.

  Other than using EEM to detect events, a DS is triggered when a Tool Command Language (Tcl) script is used to specify event detection types.

Multiple event detection

Multiple event detection involves defining two or more event detectors, two ore more corresponding tracked object states, and a time period for the events to occur. The specification format for multiple event detection can include complex event correlation for tracked event detectors. For example, three event detectors (syslog, OIR, and IPSLA) are defined during the creation of a DS file. The correlation that is specified for these event detectors is that the DS will execute its action if both syslog and OIR events are triggered simultaneously, or if IPSLA is triggered alone.

Diagnostic Signature actions

The diagnostic signature (DS) file consists of various actions that must be initiated when an event occurs. The action type indicates the kind of action that will be initiated in response to a certain event.

Variables are elements within a DS that are used to customize the files.

DS actions are categorized into the following four types:

- call-home
- command
- emailto
- script

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message uses “diagnostic-signature” as its message type and DS ID as the message sub-type.

The commands defined for the DS action type initiate CLI commands that can change configuration of the device, collect show command outputs, or run any EXEC command on the device. The DS action type script executes Tcl scripts.

Diagnostic Signature variables

Variables are referenced within a DS and are used to customize the DS file. All DS variable names have the prefix ds_ to separate them from other variables. The supported DS variable types are:

- System variable: variables assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two system variables: ds_hostname and ds_signature_id.
- Environment variable: values assigned manually by using the **environment** *variable-name variable-value* command in call-home diagnostic-signature configuration mode. Use the **show call-home diagnostic-signature** command to display the name and value of all DS environment variables. If the DS file contains unresolved environment variables, this DS will stay in pending status until the variable gets resolved.
- Prompt variable: values assigned manually by using the **call-home diagnostic-signature install** *ds-id* command in privileged EXEC mode. If you do not set this value, the status of the DS indicates pending.
- Regular expression variable: values assigned from a regular expression pattern match with predefined CLI command outputs. The value is assigned during the DS run.
- Syslog event variable: values assigned during a syslog event detection in the DS file. This variable is valid only for syslog event detection.

How to configure Diagnostic Signatures

- Configure the Call Home Service for Diagnostic Signatures, on page 223
- Configure Diagnostic Signatures, on page 225

Configure the Call Home Service for Diagnostic Signatures

Configure the Call Home Service feature to set attributes such as the contact email address where notifications related with diagnostic signatures (DS) are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from.

You can also create a new user profile, configure correct attributes and assign it as the DS profile. For periodic downloads, the request is sent out just following full inventory message. By changing the inventory periodic configuration, the DS periodic download also gets rescheduled.

Note The predefined CiscoTAC-1 profile is enabled as a DS profile by default and we recommend that you use it. If used, you only need to change the destination transport-method to the **http** setting.

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 **service call-home**

Example:

```
Router(config)# service call-home
```

Enables Call Home service on a device.

Step 3 **call-home**

Example:

```
Router(config)# call-home
```

Enters call-home configuration mode for the configuration of Call Home settings.

Step 4 **contact-email-addr** *email-address*

Example:

```
Router(cfg-call-home)# contact-email-addr userid@example.com
```

(Optional) Assigns an email address to be used for Call Home customer contact.

Step 5 **mail-server** {*ipv4-addr* | *name*} **priority** *number*

Example:

```
Router(cfg-call-home)# mail-server 10.1.1.1 priority 4
```

(Optional) Configures a Simple Mail Transfer Protocol (SMTP) email server address for Call Home. This command is only used when sending email is part of the actions defined in any DS.

Step 6 **profile** *profile-name*

Example:

```
Router(cfg-call-home)# profile user1
```

Configures a destination profile for Call Home and enters call-home profile configuration mode.

Step 7 **destination transport-method** {**email** | **http**}

Example:

```
Router(cfg-call-home-profile)# destination transport-method http
```

Specifies a transport method for a destination profile in the Call Home.

Note
To configure diagnostic signatures, you must use the **http** option.

Step 8 **destination address** {**email** *address* | **http** *url*}

Example:

```
Router(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Configures the address type and location to which call-home messages are sent.

Note
To configure diagnostic signatures, you must use the **http** option.

Step 9 **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
```

Configures a destination profile to send messages for the Inventory alert group for Call Home.

- This command is used only for the periodic downloading of DS files.

Step 10 **exit**

Example:

```
Router(cfg-call-home-profile)# exit
```

Exits call-home profile configuration mode and returns to call-home configuration mode.

What to do next

Set the profile configured in the previous procedure as the DS profile and configure other DS parameters.

Configure Diagnostic Signatures

Before you begin

Configure the Call Home feature to set attributes for the Call Home profile. You can either use the default CiscoTAC-1 profile or use the newly-created user profile.

Procedure

Step 1 **call-home**

Example:

```
Router(config)# call-home
```

Enters call-home configuration mode for the configuration of Call Home settings.

Step 2 **diagnostic-signature**

Example:

```
Router(cfg-call-home)# diagnostic-signature
```

Enters call-home diagnostic signature mode.

Step 3 **profile** *ds-profile-name*

Example:

```
Router(cfg-call-home-diag-sign)# profile user1
```

Specifies the destination profile on a device that DS uses.

Step 4 **environment** *ds_env-var-name* *ds-env-var-value*

Example:

```
Router(cfg-call-home-diag-sign)# environment ds_env1 envarval
```

Sets the environment variable value for DS on a device.

Step 5 **end**

Example:

```
Router(cfg-call-home-diag-sign)# end
```

Exits call-home diagnostic signature mode and returns to privileged EXEC mode.

Step 6 **call-home diagnostic-signature** [{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*]

Example:

```
Router# call-home diagnostic-signature download 6030
```

Downloads, installs, and uninstalls diagnostic signature files on a device.

Step 7 **show call-home diagnostic-signature** [*ds-id* {**actions** | **events** | **prerequisite** | **prompt** | **variables** | **failure** | **statistics** | **download**}]

Example:

```
Router# show call-home diagnostic-signature actions
```

Displays the call-home diagnostic signature information.

Configuration Examples for Diagnostic Signatures

The following example shows how to enable the periodic downloading request for diagnostic signature (DS) files. This configuration will send download requests to the service call-home server daily at 2:30 p.m. to check for updated DS files. The transport method is set to HTTP.

```
Router> enable
Router# configure terminal
Router(config)# service call-home
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr userid@example.com
Router(cfg-call-home)# mail-server 10.1.1.1 priority 4
Router(cfg-call-home)# profile user-1
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
Router(cfg-call-home-profile)# exit
Router(cfg-call-home)# diagnostic-signature
Router(cfg-call-home-diag-sign)# profile user1
Router(cfg-call-home-diag-sign)# environment ds_env1 envarval
Router(cfg-call-home-diag-sign)# end
```

The following is sample output from the **show call-home diagnostic-signature** command for the configuration displayed above:

```
outer# show call-home diagnostic-signature

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: user1 (status: ACTIVE)
Environment variable:
ds_env1: abc
Downloaded DSes:
DS ID    DS Name                         Revision Status     Last Update (GMT+00:00)
-------- ------------------------------- -------- ---------- -------------------
6015     CronInterval                    1.0      registered 2013-01-16 04:49:52
6030     ActCH                           1.0      registered 2013-01-16 06:10:22
6032     MultiEvents                     1.0      registered 2013-01-16 06:10:37
6033     PureTCL                         1.0      registered 2013-01-16 06:11:48
```

Display Call Home Configuration Information

You can use variations of the **show call-home** command to display Call Home configuration information.

Procedure

Step 1 **show call-home**

Example:

```
Router# show call-home
```

Displays the Call Home configuration in summary.

Step 2 **show call-home detail**

Example:

```
Router# show call-home detail
```

Displays the Call Home configuration in detail.

Step 3 **show call-home alert-group**

Example:

```
Router# show call-home alert-group
```

Displays the available alert groups and their status.

Step 4 **show call-home mail-server status**

Example:

```
Router# show call-home mail-server status
```

Checks and displays the availability of the configured e-mail server(s).

Step 5 **show call-home profile** {**all** | *name*}

Example:

```
Router# show call-home profile all
```

Displays the configuration of the specified destination profile. Use the **all** keyword to display the configuration of all destination profiles.

Step 6 **show call-home statistics** [**detail** | **profile** *profile_name*]

Example:

```
Router# show call-home statistics
```

Displays the statistics of Call Home events.

Examples

Call Home information in summary

Call Home information in detail

Available Call Home alert groups

E-mail server status information

Information for all destination profiles

Information for a user-defined destination profile

Call Home statistics

These examples show the sample output when using different options of the **show call-home** command.

```
Router# show call-home
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.0.2.1 Priority: 1
    Mail-server[2]: Address: 209.165.202.254 Priority: 2
    http proxy: 192.0.2.2:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show clock

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1
Router#
```

```
Router# show call-home detail
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.0.2.1 Priority: 1
    Mail-server[2]: Address: 209.165.202.254 Priority: 2
    http proxy: 192.0.2.2:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show clock

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info
```

```
Profiles:

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#

Router# show call-home alert-group
Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info
Router#

Router# show call-home mail-server status
Please wait. Checking for mail server status ...

    Mail-server[1]: Address: 192.0.2.1 Priority: 1 [Not Available]
    Mail-server[2]: Address: 209.165.202.254 Priority: 2 [Available]
Router#
```

```
Router# show call-home profile all

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#

Router# show call-home profile campus-noc
Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Router#
```

```
Router# show call-home statistics
Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   3                    3                    0
    Config      3                    3                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total Failed    0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total Ratelimit
      -dropped  0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Last call-home message sent time: 2011-09-26 23:26:50 GMT-08:00
Router#
```

Default Call Home settings

The table lists the default Call Home settings.

Table 16: Default Call Home settings

Parameters	Default
Call Home feature status	Disabled
User-defined profile status	Active
Predefined Cisco TAC profile status	Inactive
Transport method	E-mail
Message format type	XML
Destination message size for a message sent in long text, short text, or XML format	3,145,728
Alert group status	Enabled
Call Home message severity threshold	Debug
Message rate limit for messages per minute	20
AAA Authorization	Disabled
Call Home syslog message throttling	Enabled
Data privacy level	Normal

Alert Group trigger events and commands

Call Home trigger events are grouped into alert groups, with each alert group assigned commands to execute when an event occurs. The command output is included in the transmitted message. The following table lists the trigger events included in each alert group, including the severity level of each event and the executed commands for the alert group.

Table 17: Call Home Alert Groups, Events, and Actions

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Crash	SYSTEM_ CRASH	–	–	Events related to software crash. The following commands are executed: **show version** **show logging** **show region** **show inventory** **show stack** **crashinfo file** (this command shows the contents of the crashinfo file)
–	TRACEBACK	–	–	Detects software traceback events. The following commands are executed: **show version** **show logging** **show region** **show stack**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Configuration	–	–	–	User-generated request for configuration or configuration change event. The following commands are executed: **show platform** **show inventory** **show running-config all** **show startup-config** **show version**
Environmental	–	–	–	Events related to power, fan, and environment sensing elements such as temperature alarms. The following commands are executed: **show environment** **show inventory** **show platform** **show logging**
–	–	SHUT	0	Environmental Monitor initiated shutdown.
–	–	ENVCRIT	2	Temperature or voltage measurement exceeded critical threshold.
–	–	BLOWER	3	Required number of fan trays is not present.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
–	–	ENVWARN	4	Temperature or voltage measurement exceeded warning threshold.
–	–	RPSFAIL	4	Power supply may have a failed channel.
–	ENVM	PSCHANGE	6	Power supply name change.
–	–	PSLEV	6	Power supply state change.
–	–	PSOK	6	Power supply now appears to be working correctly.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Inventory	–	–	–	

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
				Inventory status should be provided whenever a unit is cold-booted or when FRUs are inserted or removed. This is considered a noncritical event, and the information is used for status and entitlement. Commands executed for all Inventory messages sent in anonymous mode and for Delta Inventory message sent in full registration mode: **show diag all eeprom detail** **show version** **show inventory oid** **show platform** Commands executed for Full Inventory message sent in full registration mode: **show platform** **show diag all eeprom detail** **show version** **show inventory oid** **show bootflash: all** **show data-corruption** **show interfaces** **show file systems** **show memory statistics**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
				show process memory **show process cpu** **show process cpu history** **show license udi** **show license detail** **show buffers**
–	HARDWARE_ REMOVAL	REMCARD	6	Card removed from slot %d, interfaces disabled.
–	HARDWARE_ INSERTION	INSCARD	6	Card inserted in slot %d, interfaces administratively shut down.
Syslog	–	–	–	Event logged to syslog. The following commands are executed: **show inventory** **show logging**
–	SYSLOG	LOG_EMERG	0	System is unusable.
–	SYSLOG	LOG_ALERT	1	Action must be taken immediately.
–	SYSLOG	LOG_CRIT	2	Critical conditions.
–	SYSLOG	LOG_ERR	3	Error conditions.
–	SYSLOG	LOG_WARNING	4	Warning conditions.
–	SYSLOG	LOG_NOTICE	5	Normal but signification condition.
–	SYSLOG	LOG_INFO	6	Informational.
–	SYSLOG	LOG_DEBUG	7	Debug-level messages.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Test	–	TEST	–	User-generated test message. The following commands are executed: **show platform** **show inventory** **show version**

Message Contents

This section consists of tables which list the content formats of alert group messages.

The table lists the content fields of a short text message.

Table 18: Format for a short text message

Data Item	Description
Device identification	Configured device name
Date/time stamp	Time stamp of the triggering event
Error isolation message	Plain English description of triggering event
Alarm urgency level	Error level such as that applied to a system message

The table shows the content fields that are common to all long text and XML messages. The fields specific to a particular alert group message are inserted at a point between the common fields. The insertion point is identified in the table.

Table 19: Common Fields for all long text and XML messages

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD HH:MM:SS GMT+HH:MM*.	CallHome/EventTime
Message name	Name of message. Specific event names are listed in the Alert Group trigger events and commands, on page 233.	For short text message only
Message type	Specifically “Call Home”.	CallHome/Event/Type

Data Item (Plain Text and XML)	**Description (Plain Text and XML)**	**Call-Home Message Tag (XML Only)**
Message subtype	Specific type of message: full, delta, test	CallHome/Event/SubType
Message group	Specifically “reactive”. Optional because default is “reactive”.	For long-text message only
Severity level	Severity level of message (see Message severity threshold, on page 208).	Body/Block/Severity
Source ID	Product type for routing through the workflow engine. This is typically the product family name.	For long-text message only
Device ID	Unique device identifier (UDI) for end device generating message. This field should be empty if the message is nonspecific to a fabric switch. The format is *type@Sid@serial*. • *type* is the product model number from backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. Example: CISCO3845@C@12345678	CallHome/CustomerData/ ContractData/DeviceId
Customer ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ ContractData/CustomerId
Contract ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ ContractData/CustomerId
Site ID	Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.	CallHome/CustomerData/ ContractData/CustomerId

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Server ID	If the message is generated from the fabric switch, this is the unique device identifier (UDI) of the switch. • *type* is the product model number from backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. Example: CISCO3845@C@12345678	For long text message only.
Message description	Short text describing the error.	CallHome/MessageDescription
Device name	Node that experienced the event. This is the host name of the device.	CallHome/CustomerData/ SystemInfo/NameName
Contact name	Name of person to contact for issues associated with the node experiencing the event.	CallHome/CustomerData/ SystemInfo/Contact
Contact e-mail	E-mail address of person identified as contact for this unit.	CallHome/CustomerData/ SystemInfo/ContactEmail
Contact phone number	Phone number of the person identified as the contact for this unit.	CallHome/CustomerData/ SystemInfo/ContactPhoneNumber
Street address	Optional field containing street address for RMA part shipments associated with this unit.	CallHome/CustomerData/ SystemInfo/StreetAddress
Model name	Model name of the router. This is the “specific model as part of a product family name.	CallHome/Device/Cisco_Chassis/Model
Serial number	Chassis serial number of the unit.	CallHome/Device/Cisco_Chassis/ SerialNumber
Chassis part number	Top assembly number of the chassis.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name=“PartNumber”

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
System object ID	System Object ID that uniquely identifies the system.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name="sysObjectID"
System description	System description for the managed element.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name="sysDescr"

The table shows the inserted fields specific to a particular alert group message.

Note These fields may be repeated if multiple commands are executed for this alert group.

Table 20: Inserted fields specific to a particular Alert Group message

Command output name	Exact name of the issued command.	/aml/Attachments/Attachment/Name
Attachment type	Attachment type. Usually "inline".	/aml/Attachments/Attachment@type
MIME type	Normally "text" or "plain" or encoding type.	/aml/Attachments/Attachment/ Data@encoding
Command output text	Output of command automatically executed (see Alert Group trigger events and commands, on page 233).	/mml/attachments/attachment/atdata

The table shows the inserted content fields for reactive messages (system failures that require a TAC case) and proactive messages (issues that might result in degraded system performance).

Table 21: Inserted fields for a reactive or proactive Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/ HardwareVersion
Supervisor module software version	Top-level software version	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= "SoftwareVersion"
Affected FRU name	Name of the affected FRU generating the event message	CallHome/Device/Cisco_Chassis/ Cisco_Card/Model
Affected FRU serial number	Serial number of affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/SerialNumber
Affected FRU part number	Part number of affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/PartNumber

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
FRU slot	Slot number of FRU generating the event message	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of affected FRU	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU software version	Software version(s) running on affected FRU	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString

The table shows the inserted content fields for an inventory message.

Table 22: Inserted fields for an inventory event message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/HardwareVersion
Supervisor module software version	Top-level software version	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“SoftwareVersion”
FRU name	Name of the affected FRU generating the event message	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
FRU s/n	Serial number of FRU	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
FRU part number	Part number of FRU	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU slot	Slot number of FRU	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of FRU	CallHome/Device/Cisco_Chassis/CiscoCard/HardwareVersion
FRU software version	Software version(s) running on FRU	CallHome/Device/Cisco_Chassis /Cisco_Card/SoftwareIdentity/VersionString

CHAPTER 16

Managing Cisco Enhanced Services and Network Interface Modules

The router supports Cisco Enhanced Services Modules (SMs) and Cisco Network Interface Modules (NIMs). The modules are inserted into the router using an adapter, or carrier card, into various slots. For more information, see the following documents:

- Hardware Installation Guide for Cisco 8300 Series Secure Routers

These sections are included in this chapter:

Information about Cisco Service Modules and Network Interface Modules

The router configures, manages, and controls the supported Cisco Service Modules (SMs), Network Interface Modules (NIMs) and PIM (Pluggable Interface Modules) using the module management facility built in its architecture. This new centralized module management facility provides a common way to control and monitor all the modules in the system regardless of their type and application. All Cisco Enhanced Service and Network Interface Modules supported on your router use standard IP protocols to interact with the host router. Cisco IOS software uses alien data path integration to switch between the modules.

- Modules supported, on page 246

- Network Interface Modules and Enhanced Service Modules, on page 246

Modules supported

For information about the interfaces and modules supported by the Cisco 8300 Series Secure Routers, see Hardware Installation Guide for Cisco 8300 Series Secure Routers.

Network Interface Modules and Enhanced Service Modules

For more information on the supported Network Interface Modules and Service Modules, refer to the Cisco 8300 Series Secure Routers datasheet.

Implement SMs and NIMs on your platforms

Download the module firmware

Module firmware must be loaded to the router to be able to use a service module. For more information, see Installing a firmware subpackage, on page 104.

The modules connect to the RP via the internal eth0 interface to download the firmware. Initially, the module gets an IP address for itself via BOOTP. The BOOTP also provides the address of the TFTP server used to download the image. After the image is loaded and the module is booted, the module provides an IP address for the running image via DHCP.

Install SMs and NIMs

For more information, see "Installing and Removing NIMs and SMs" in the Hardware Installation Guide for Cisco 8300 Series Secure Routers.

Access your module through a console connection or Telnet

Before you can access the modules, you must connect to the host router through the router console or through Telnet. After you are connected to the router, you must configure an IP address on the Gigabit Ethernet interface connected to your module. Open a session to your module using the **hw-module session** command in privileged EXEC mode on the router.

To establish a connection to the module, connect to the router console using Telnet or Secure Shell (SSH) and open a session to the switch using the **hw-module session** *slot/subslot* command in privileged EXEC mode on the router.

Use these configuration examples to establish a connection:

- The example shows how to open a session from the router using the **hw-module session** command:

```
Router# hw-module session slot/card
Router# hw-module session 0/1 endpoint 0

Establishing session connect to subslot 0/1
```

- The example shows how to exit a session from the router, by pressing **Ctrl-A** followed by **Ctrl-Q** on your keyboard:

```
type ^a^q
picocom v1.4

port is        : /dev/ttyDASH2
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : ascii_xfr -s -v -l10
receive_cmd is : rz -vv
```

Online insertion and removal

The router supports online insertion and removal (OIR) of Cisco Enhanced Services Modules and Cisco Network Interface Modules. You can perform these tasks using the OIR function:

Note The router supports OIR of a module, but does not support the hot removal and insertion of a module. Ensure to stop the traffic on these module, before insertion or removal.

- Prepare for online removal of a module, on page 247
- Deactivate a module, on page 247
- Deactivating modules and Interfaces in different command modes, on page 248
- Reactivate a module, on page 249
- Verify the deactivation and activation of a module, on page 249

Prepare for online removal of a module

The router supports the OIR of a module, independent of removing another module installed in your router. This means that an active module can remain installed in your router, while you remove another module from one of the subslots. If you are not planning to immediately replace a module, ensure that you install a blank filler plate in the subslot.

Deactivate a module

A module must be deactivated before removing it from the router. To perform a graceful deactivation, use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode.

Note When you are preparing for an OIR of a module, it is not necessary to independently shut down each of the interfaces before deactivating the module. The **hw-module subslot** *slot/subslot* **stop** command in EXEC mode automatically stops traffic on the interfaces and deactivates them along with the module in preparation for OIR. Similarly, you do not have to independently restart any of the interfaces on a module after OIR.

The example shows how to use the **show facility-alarm status** command to verify if any critical alarm is generated when a module is removed from the system:

```
Router# show facility-alarm status
System Totals  Critical: 18  Major: 0  Minor: 0

Source                      Time                    Severity      Description [Index]
------                      ------                  --------      -------------------

Power Supply Bay 1          Sep 28 2020 10:02:34    CRITICAL      Power Supply/FAN Module
Missing [0]
POE Bay 0                   Sep 28 2020 10:02:34    INFO          Power Over Ethernet Module
 Missing [0]
POE Bay 1                   Sep 28 2020 10:02:34    INFO          Power Over Ethernet Module
 Missing [0]
GigabitEthernet0/0/2       Sep 28 2020 10:02:46   INFO          Physical Port Administrative
 State Down [2]
GigabitEthernet0/0/3       Sep 28 2020 10:02:46   INFO          Physical Port Administrative
 State Down [2
xcvr container 0/0/4        Sep 28 2020 10:02:46    INFO          Transceiver Missing - Link
 Down [1]
TenGigabitEthernet0/0/5    Sep 28 2020 10:02:54   CRITICAL      Physical Port Link Down [1]
TenGigabitEthernet0/1/0    Sep 28 2020 10:03:26   INFO         Physical Port Administrative
 State Down [2]
GigabitEthernet1/0/0       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down [1]
GigabitEthernet1/0/1       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down [1]
GigabitEthernet1/0/2       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down [1]
GigabitEthernet1/0/3       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down [1]
GigabitEthernet1/0/4       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down [1]
GigabitEthernet1/0/5       Sep 28 2020 10:07:35   CRITICAL      Physical Port Link Down [1]
TwoGigabitEthernet1/0/16   Sep 28 2020 10:07:35   INFO         Physical Port Administrative
 State Down [2]
TwoGigabitEthernet1/0/17   Sep 28 2020 10:07:35   INFO         Physical Port Administrative
 State Down [2]
TwoGigabitEthernet1/0/18   Sep 28 2020 10:07:35   INFO         Physical Port Administrative
 State Down [2]
TwoGigabitEthernet1/0/19   Sep 28 2020 10:07:35   INFO         Physical Port Administrative
 State Down [2]
xcvr container 1/0/20       Sep 28 2020 10:04:00    INFO          Transceiver Missing - Link
 Down [1]
xcvr container 1/0/21       Sep 28 2020 10:04:00    INFO          Transceiver Missing - Link
 Down [1]1]
```

Note A critical alarm (Active Card Removed OIR Alarm) is generated even if a module is removed after performing graceful deactivation.

Deactivating modules and Interfaces in different command modes

You can deactivate a module and its interfaces using the **hw-module subslot** command in one of these modes:

1. **hw-module subslot** *slot*/*subslot* **shutdown unpowered**

   If you choose to deactivate your module and its interfaces by executing the **hw-module subslot** *slot/subslot* **shutdown unpowered** command in global configuration mode, you are able to change the configuration in such a way that no matter how many times the router is rebooted, the module does not boot. This command is useful when you need to shut down a module located in a remote location and ensure that it does not boot automatically when the router is rebooted.

   ```
   Router(config)# hw-module subslot 0/2 shutdown unpowered
   ```

   Deactivates the module located in the specified slot and subslot of the router, where:

   - *slot*—Specifies the chassis slot number where the module is installed.
   - *subslot*—Specifies the subslot number of the chassis where the module is installed.
   - **shutdown**—Shuts down the specified module.
   - **unpowered**—Removes all interfaces on the module from the running configuration and the module is powered off.

2. **hw-module subslot** *slot*/*subslot* [**reload** | **stop** | **start**]

   If you choose to use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode, you cause the module to gracefully shut down. The module is rebooted when the **hw-module subslot** *slot/subslot* **start** command is executed.

   ```
   Router# hw-module subslot 0/2 stop
   ```

   Deactivates the module in the specified slot and subslot, where:

   - *slot*—Specifies the chassis slot number where the module is installed.
   - *subslot*—Specifies the subslot number of the chassis where the module is installed.
   - **reload**—Stops and restarts the specified module.
   - **stop**—Removes all interfaces from the module and the module is powered off.
   - **start**—Powers on the module similar to a physically inserted module in the specified slot. The module firmware reboots and the entire module initialization sequence is executed in the IOSd and Input/Output Module daemon (IOMd) processes.

Reactivate a module

If, after deactivating a module using the **hw-module subslot** *slot/subslot* **stop** command, you want to reactivate it without performing an OIR, use one of these commands (in privileged EXEC mode):

- **hw-module subslot** *slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

Verify the deactivation and activation of a module

When you deactivate a module, the corresponding interfaces are also deactivated. This means that these interfaces will no longer appear in the output of the **show interface** command.

1. To verify the deactivation of a module, enter the **show hw-module subslot all oir** command in privileged EXEC configuration mode.

   Observe the "Operational Status" field associated with the module that you want to verify. In this example, the module located in subslot 1 of the router is administratively down.

   ```
   Router# show hw-module subslot all oir

     Module                  Model                Operational Status
   ----------------------- -------------------- ------------------------

   subslot 0/0             4M-2xSFP+            ok

   subslot 0/1             C-NIM-8M             ok
   subslot 0/4             VDSP-CC              ok
   ```

2. To verify activation and proper operation of a module, enter the **show hw-module subslot all oir** command and observe "ok" in the **Operational Status** field as shown in the following example:

   ```
   Router# show hw-module subslot all oir

    Module                  Model               Operational Status
   ----------------------- -------------------- ------------------------

   subslot 0/0             4M-2xSFP+            ok

   subslot 0/1             C-NIM-8M             ok
   subslot 0/4             VDSP-CC              ok
   ```

Manage modules and interfaces

The router supports various modules. For a list of supported modules, see Modules supported, on page 246. The module management process involves bringing up the modules so that their resources can be utilized. This process consists of tasks such as module detection, authentication, configuration by clients, status reporting, and recovery.

For a list of small-form-factor pluggable (SFP) modules supported on your router, see the "Installing and Upgrading Internal Modules and FRUs" section in the Hardware Installation Guide for Cisco 8300 Series Secure Routers.

The following sections provide additional information on managing the modules and interfaces:

- Manage module interfaces, on page 250

Manage module interfaces

After a module is in service, you can control and monitor its module interface. Interface management includes configuring clients with **shut** or **no shut** commands and reporting on the state of the interface and the interface-level statistics.

Configuration examples

This section provides examples of deactivating and activating modules.

Deactivating a module configuration: Example

You can deactivate a module to perform OIR of that module. The following example shows how to deactivate a module (and its interfaces) and remove power to the module. In this example, the module is installed in subslot 0 of the router.

```
Router(config)# hw-module subslot 1/0 shutdown unpowered
```

Activating a module configuration: Example

You can activate a module if you have previously deactivated it. If you have not deactivated a module and its interfaces during OIR, then the module is automatically reactivated upon reactivation of the router.

The following example shows how to activate a module. In this example, the module is installed in subslot 0, located in slot 1 of the router:

```
Router(config)# no hw-module subslot 1/0 shutdown unpowered
```

CHAPTER 17

Cellular IPv6 address

This chapter provides an overview of the IPv6 addresses and describes how to configure Cellular IPv6 address on Cisco 8300 Series Secure Routers.

This chapter includes this section:

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:CDBA:0000:0000:0000:0000:3257:9652
- 2001:CDBA::3257:9652 (zeros can be omitted)

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:cdba::3257:9652 /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 8300 Series Secure Routers support the following address types:

- Link-Lock address , on page 254
- Global address, on page 254

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.

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.

Configure Cellular IPv6 address

To configure the cellular IPv6 address, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 **ipv6 unicast-routing**

Example:

```
Router(config)# ipv6 unicast-routing
```

Enables forwarding of IPv6 unicast data packets.

Step 3 **interface Cellular** {**type** | **number**}

Example:

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

Specifies the cellular interface.

Step 4 ip address negotiated

Example:

```
Router(config-if)# ip address negotiated
```

Specifies that the IP address for a particular interface is dynamically obtained.

Step 5 load-interval***seonds***

Example:

```
Router(config-if)# load-interval 30
```

Specifies the length of time for which data is used to compute load statistics.

Step 6 dialer in-band

Example:

```
Router(config-if)# dialer in-band
```

Enables DDR and configures the specified serial interface to use in-band dialing.

Step 7 dialer idle-timeout ***seonds***

Example:

```
Router(config-if)# dialer idle-timeout 0
```

Specifies the dialer idle timeout period.

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 or ipv6 enable

Example:

```
Router(config-if)# ipv6 address autoconfig
```

or

```
Router(config-if)# ipv6 enable
```

Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.

Step 11 **dialer-listdialer-groupprotocolprotocol-name** {**permit** |deny|**list** |*access-list-number* | *access-group* }

Example:

```
Router(config)# dialer-list 1 protocol ipv6 permit
```

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.

Step 12 **ipv6 route** *ipv6-prefix/prefix-length 128*

Example:

```
Router(config)#ipv6 route 2001:1234:1234::3/128 Cellular0/1/0
```

Step 13 **End**

Example:

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

Exits to global configuration mode.

Examples

This example shows the Cellular IPv6 configuration for NIM-LTEA-EA and NIM-LTEA-LA modules.

```
Router(config)# interface Cellular0/1/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
lte dialer-group 1
no peer default ip address
ipv6 address autoconfig
!
interface Cellular0/1/1
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer-group 1
no peer default ip address
ipv6 address autoconfig
```

This example shows the Cellular IPv6 configuration for P-LTEAP18-GL, P-LTEA-XX, and P-LTE-XX modules.

```
Router(config)# interface Cellular0/2/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
lte dialer-group 1
no peer default ip address
ipv6 enable
!
interface Cellular0/2/1
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer-group 1
no peer default ip address
ipv6 enable
```

CHAPTER 18

Radio Aware Routing

Radio-Aware Routing (RAR) is a mechanism that uses radios to interact with the routing protocol OSPFv3 to signal the appearance, disappearance, and link conditions of one-hop routing neighbors.

In a large mobile networks, connections to the routing neighbors are often interrupted due to distance and radio obstructions. When these signals do not reach the routing protocols, protocol timers are used to update the status of a neighbor. Routing protocols have lengthy timer, which is not recommended in mobile networks.

Benefits of Radio Aware Routing

The Radio Aware Routing feature offers these benefits:

- Provides faster network convergence through immediate recognition of changes.
- Enables routing for failing or fading radio links.
- Allows easy routing between line-of-sight and non-line-of-sight paths.
- Provides faster convergence and optimal route selection so that delay-sensitive traffic, such as voice and video, is not disrupted
- Provides efficient radio resources and bandwidth usage.
- Reduces impact on the radio links by performing congestion control in the router.
- Allows route selection based on radio power conservation.
- Enables decoupling of the routing and radio functionalities.
- Provides simple Ethernet connection to RFC 5578, R2CP, and DLEP compliant radios.

Restrictions and Limitations

The Radio Aware Routing feature has these restrictions and limitations:

- The DLEP and R2CP protocols are not supported on Cisco 8300 Series Secure Routers.
- Multicast traffic is not supported in aggregate mode.
- Cisco High Availability (HA) technology is not supported.

License Requirements

This feature is made available with the AppX license.

System components

The Radio Aware Routing (RAR) feature is implemented using the MANET (Mobile adhoc network) infrastructure comprising of different components such as PPPoE, Virtual multipoint interface (VMI), QoS, routing protocol interface and RAR protocols.

Point-to-Point Protocol over Ethernet or PPPoE

PPPoE is a well-defined communication mechanism between the client and the server. In the RAR implementation, radio takes the role of the PPPoE client and router takes the role of the PPPoE server. This allows a loose coupling of radio and router, while providing a well-defined and predictable communication mechanism.

As PPPoE is a session or a connection oriented protocol, it extends the point-to-point radio frequency (RF) link from an external radio to an IOS router.

PPPoE extensions

PPPoE extensions are used when the router communicates with the radio. In the Cisco IOS implementation of PPPoE, each individual session is represented by virtual access interface (connectivity to a radio neighbor) on which, QoS can be applied with these PPPoE extensions.

RFC5578 provides extensions to PPPoE to support credit-based flow control and session-based real time link metrics, which are very useful for connections with variable bandwidth and limited buffering capabilities (such as radio links).

Virtual Multipoint Interface (VMI)

Though PPPoE Extensions provides the most of the setup to communicate between a router and a radio, VMI addresses the need to manage and translate events that higher layers (example, routing protocols) consume. In addition, VMI operates in the Bypass mode.

In Bypass mode, every Virtual Access Interface (VAI) representing a radio neighbor is exposed to routing protocols OSPFv3 and EIGRP, so that, the routing protocol directly communicates with the respective VAI for both unicast and multicast routing protocol traffic.

In Aggregae mode, VMI is exposed to the routing protocols (OSPF) so that the routing protocols can leverage VMI for their optimum efficiency. When the network neighbors are viewed as a collection of networks on a point-to-multipoint link with broadcast and multicast capability at VMI, VMI helps in aggregating the multiple virtual access interfaces created from PPPoE. VMI presents a single multi access layer 2 broadcast capable interface. The VMI layer handles re-directs unicast routing protocol traffic to the appropriate P2P link (Virtual-Access interface), and replicats any Multicast/Broadcast traffic that needs to flow. Since the routing protocol communicates to a single interface, the size of the topology database is reduced, without impacting the integrity of the network.

QoS Provisioning on PPPoE Extension Session

The following example describes QoS provisioning on PPPoE extension session:

```
policy-map rar_policer
 class class-default
  police 10000 2000 1000 conform-action transmit  exceed-action drop  violate-action drop
policy-map rar_shaper
 class class-default
  shape average percent 1

interface Virtual-Template2
 ip address 192.0.2.7 255.255.255.0
 no peer default ip address
 no keepalive
 service-policy input rar_policer
end
```

Example: Configure the RAR feature in bypass mode

This example is an end-to-end configuration of RAR in the bypass mode:

Note Before you being the RAR configuration, you must first configure the **subscriber authorization enable** command to bring up the RAR session. Without enbaling authorization, the Point-to-Point protocol does not recognize this as a RAR session and may not tag *manet_radio* in presentation of a PPPoE Active Discovery Initiate (PADI). By default, bypass mode does not appears in the configuration. It appears only if the mode is configured as bypass.

Configure a Service for RAR

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

Configure Broadband

```
bba-group pppoe VMI2
 virtual-template 2
service profile rar-lab
!
interface GigabitEthernet0/0/0
```

```
 description Connected to Client1
  negotiation auto
  pppoe enable group VMI2
!
```

Configure a Service for RAR

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

Configuration in Bypass Mode

- IP Address Configured under Virtual-Template Explicitly

  ```
  interface Virtual-Template2
  ip address 192.0.2.7 255.255.255.0
  no ip redirects
  peer default ip address pool PPPoEpool2
  ipv6 enable
  ospfv3 1 network manet
  ospfv3 1 ipv4 area 0
  ospfv3 1 ipv6 area 0
  no keepalive
  service-policy input rar_policer Or/And
  service-policy output rar_shaper
  ```

- VMI Unnumbered Configured under Virtual Template

  ```
  interface Virtual-Template2
  ip unnumbered vmi2
  no ip redirects
  peer default ip address pool PPPoEpool2
  ipv6 enable
  ospfv3 1 network manet
  ospfv3 1 ipv4 area 0
  ospfv3 1 ipv6 area 0
  no keepalive
  service-policy input rar_policer Or/And
  service-policy output rar_shaper
  ```

Configure the Virtual Multipoint Interface in Bypass Mode

```
interface vmi2 //configure the virtual multi interface
ip address 192.0.2.5 255.255.255.0
physical-interface GigabitEthernet0/0/0
mode bypass
```

```
interface vmi3//configure the virtual multi interface
 ip address 192.0.2.6 255.255.255.0
 physical-interface GigabitEthernet0/0/1
mode bypass
```

Configure OSPF Routing

```
router ospfv3 1
 router-id 192.0.2.1
```

```
!
 address-family ipv4 unicast
  redistribute connected metric 1 metric-type 1
  log-adjacency-changes
 exit-address-family
 !
 address-family ipv6 unicast
  redistribute connected metric-type 1
  log-adjacency-changes
 exit-address-family
!
ip local pool PPPoEpool2 192.0.2.8 192.0.2.4
```

Example: Configuring the RAR feature in aggregate mode

This example is an end-to-end configuration of RAR in the aggregate mode:

Note Before you being the RAR configuration, you must first configure the **subscriber authorization enable** command to bring up the RAR session. Without enabling authorization, the Point-to-Point protocol does not recognize this as a RAR session and may not tag *manet_radio* in PADI.

Configure a Service for RAR

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

Configure Broadband

```
bba-group pppoe VMI2
 virtual-template 2
service profile rar-lab

!
interface GigabitEthernet0/0/0
 description Connected to Client1
  negotiation auto
  pppoe enable group VMI2

!
```

Configure a Service for RAR

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

Configuration in Aggregate Mode

```
interface Virtual-Template2
ip unnumbered vmi2
no ip redirects
no peer default ip address
ipv6 enable
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

Configure the Virtual Multipoint Interface in Aggregate Mode

```
interface vmi2 //configure the virtual multi interface
ip address 192.0.2.8 255.255.255.0
physical-interface GigabitEthernet0/0/0
mode aggregate
```

```
interface vmi3//configure the virtual multi interface
 ip address 192.0.2.4 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 1
 physical-interface GigabitEthernet0/0/1
mode aggregate
```

Configure OSPF Routing

```
router ospfv3 1
 router-id 192.0.2.1
!
 address-family ipv4 unicast
  redistribute connected metric 1 metric-type 1
  log-adjacency-changes
 exit-address-family
 !
 address-family ipv6 unicast
  redistribute connected metric-type 1
  log-adjacency-changes
 exit-address-family
!
ip local pool PPPoEpool2 192.0.2.4 192.0.2.8
ip local pool PPPoEpool3 192.0.2.6 192.0.2.2
```

Verify RAR Session Details

To retrieve RAR session details, use these show commands:

```
Router#show pppoe session packets all
Total PPPoE sessions 2

session id: 9
local MAC address: 006b.f10e.a5e0, remote MAC address: 0050.56bc.424a
virtual access interface: Vi2.1, outgoing interface: Gi0/0/0
    1646 packets sent, 2439363 received
    176216 bytes sent, 117250290 received

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 32928     PADG Timer index: 0
 PADG last rcvd Seq Num: 17313
 PADG last nonzero Seq Num: 17306
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33308  rcvd: 17313
 PADC xmit: 17313  rcvd: 19709
 In-band credit pkt xmit: 7 rcvd: 2434422
 Last credit packet snapshot
  PADG xmit: seq_num = 32928, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 32928, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17313, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17313, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


session id: 10
local MAC address: 006b.f10e.a5e1, remote MAC address: 0050.56bc.7dcb
virtual access interface: Vi2.2, outgoing interface: Gi0/0/1
    1389302 packets sent, 1852 received
    77869522 bytes sent, 142156 received

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 18787     PADG Timer index: 0
 PADG last rcvd Seq Num: 18784
 PADG last nonzero Seq Num: 18768
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 18787  rcvd: 18784
 PADC xmit: 18784  rcvd: 18787
 In-band credit pkt xmit: 1387764 rcvd: 956
 Last credit packet snapshot
  PADG xmit: seq_num = 18787, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 18787, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18784, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 18784, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 1


Router#show pppoe session packets
Total PPPoE sessions 2

SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
9       2439391         1651            117252098       176714
10      1858            1389306         142580          77869914


Router#show vmi counters
Interface vmi2: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =       4280
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Interface vmi3: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =       2956
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Interface vmi4: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =          0
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Router#


Router#show vmi neighbor details
1 vmi2 Neighbors
      1 vmi3 Neighbors
      0 vmi4 Neighbors
      2 Total Neighbors

vmi2   IPV6 Address=FE80::21E:E6FF:FE43:F500
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.6, Uptime=05:15:01
       Output pkts=89, Input pkts=0
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=9
       INTERFACE STATS:
          VMI Interface=vmi2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33038     PADG Timer index: 0
 PADG last rcvd Seq Num: 17423
 PADG last nonzero Seq Num: 17420
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33418  rcvd: 17423
 PADC xmit: 17423  rcvd: 19819
 In-band credit pkt xmit: 7 rcvd: 2434446
 Last credit packet snapshot
  PADG xmit: seq_num = 33038, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33038, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17423, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17423, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


vmi3   IPV6 Address=FE80::21E:7AFF:FE68:6100
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.10, Uptime=05:14:55
       Output pkts=6, Input pkts=0
       METRIC DATA: Total rcvd=1, Avg arrival rate (ms)=0
          CURRENT: MDR=128000 bps, CDR=128000 bps
                   Lat=0 ms, Res=100, RLQ=100, load=0
          MDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
          CDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
          Latency  Max=0, Min=0, Avg=0 (ms)
          Resource Max=100%, Min=100%, Avg=100%
          RLQ      Max=100, Min=100, Avg=100
          Load     Max=0%, Min=0%, Avg=0%
       Transport PPPoE, Session ID=10
       INTERFACE STATS:
          VMI Interface=vmi3,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/1,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 18896     PADG Timer index: 0
 PADG last rcvd Seq Num: 18894
 PADG last nonzero Seq Num: 18884
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 18896  rcvd: 18894
 PADC xmit: 18894  rcvd: 18896
 In-band credit pkt xmit: 1387764 rcvd: 961
 Last credit packet snapshot
  PADG xmit: seq_num = 18896, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 18896, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18894, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 18894, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 1


Router#show vmi neighbor details vmi 2
              1 vmi2 Neighbors

vmi2   IPV6 Address=FE80::21E:E6FF:FE43:F500
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.4, Uptime=05:16:03
       Output pkts=89, Input pkts=0
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=9
       INTERFACE STATS:
          VMI Interface=vmi2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33100     PADG Timer index: 0
 PADG last rcvd Seq Num: 17485
 PADG last nonzero Seq Num: 17449
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)  [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33480  rcvd: 17485
 PADC xmit: 17485  rcvd: 19881
 In-band credit pkt xmit: 7 rcvd: 2434460
 Last credit packet snapshot
  PADG xmit: seq_num = 33100, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33100, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17485, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17485, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


Router#show platform hardware qfp active feature ess session
Current number sessions: 2
Current number TC flow: 0
Feature Type: A=Accounting D=Policing(DRL) F=FFR M=DSCP Marking L=L4redirect P=Portbundle
T=TC

   Session    Type      Segment1      SegType1      Segment2      SegType2 Feature Other
----------------------------------------------------------------------------------------
        21     PPP 0x0000001500001022    PPPOE 0x0000001500002023    LTERM -------
        24     PPP 0x0000001800003026    PPPOE 0x0000001800004027    LTERM -------
```

```
Router#show platform software subscriber pppoe_fctl evsi 21
PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33215     PADG Timer index: 0
 PADG last rcvd Seq Num: 17600
 PADG last nonzero Seq Num: 17554
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33595  rcvd: 17600
 PADC xmit: 17600  rcvd: 19996
 In-band credit pkt xmit: 7 rcvd: 2434485
 Last credit packet snapshot
  PADG xmit: seq_num = 33215, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33215, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17600, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17600, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534

BQS buffer statistics
 Current packets in BQS buffer: 0
 Total en-queue packets: 0 de-queue packets: 0
 Total dropped packets: 0

Internal flags: 0x0
```

```
Router#show platform hardware qfp active feature ess session id 21
Session ID: 21

  EVSI type: PPP
  SIP Segment ID: 0x1500001022
  SIP Segment type: PPPOE
  FSP Segment ID: 0x1500002023
  FSP Segment type: LTERM
  QFP if handle: 16
  QFP interface name: EVSI21
  SIP TX Seq num: 0
  SIP RX Seq num: 0
  FSP TX Seq num: 0
  FSP RX Seq num: 0
  Condition Debug: 0x00000000
    session
```

```
Router#show ospfv3 neighbor

          OSPFv3 1 address-family ipv4 (router-id 192.0.2.3)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.0.2.1           0   FULL/  -        00:01:32    19              Virtual-Access2.1

          OSPFv3 1 address-family ipv6 (router-id 192.0.2.3)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.0.2.1          0   FULL/  -        00:01:52    19              Virtual-Access2.1
Router#
```

```
Router#sh ip route

Codes: L - local, 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, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.0.2.8/8 is variably subnetted, 3 subnets, 2 masks
C        192.0.2.5/24 is directly connected, Virtual-Access2.1
O        192.0.2.6/32 [110/1] via 192.0.2.22, 00:00:03, Virtual-Access2.1
L        192.0.2.7/32 is directly connected, Virtual-Access2.1
      192.0.2.12/32 is subnetted, 1 subnets
C        192.0.2.20 is directly connected, Virtual-Access2.1
```

Troubleshoot Radio Aware Routing

To troubleshoot the RAR, use these debug commands:

- **debug pppoe errors**
- **debug pppoe events**
- **debug ppp error**
- **debug vmi error**
- **debug vmi neighbor**
- **debug vmi packet**
- **debug vmi pppoe**
- **debug vmi registries**
- **debug vmi multicast**
- **debug vtemplate cloning**
- **debug vtemplate event**
- **debug vtemplate error**
- **debug plat hard qfp ac feature subscriber datapath pppoe detail**

CHAPTER 19

Support for Software Media Termination Point

The Support for Software Media Termination Point (MTP) feature bridges the media streams between two connections, allowing Cisco Unified Communications Manager (CUCM) to relay the calls that are routed through SIP or H.323 endpoints through Skinny Client Control Protocol (SCCP) commands. These commands allow CUCM to establish an MTP for call signaling.

Finding feature information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Information about support for Software Media Termination Point

This feature extends the software MTP support to the Cisco Unified Border Element (Enterprise). Software MTP is an essential component of large-scale deployments of Cisco UCM. This feature enables new capabilities so that the Cisco UBE can function as an Enterprise Edge Cisco Session Border Controller for large-scale deployments that are moving to SIP trunking.

Prerequisites for Software Media Termination Point

- For the software MTP to function properly, codec and packetization must be configured the same way on both in call legs and out call legs.

Restrictions for Software Media Termination Point

- RSVP Agent is not supported in software MTP.
- Software MTP for repacketization is not supported.
- Call Threshold is not supported for standalone software MTP.
- Per-call debugging is not supported.
- Multiple concurrent Synchronisation Sources (SSRCs) with the same destination IP and port are not supported.

SRTP-DTMF Interworking

From Cisco IOS XE 17.10.1a, Secure Real-time Transport Protocol (SRTP) Dual-Tone Multi-Frequency (DTMF) interworking is supported with Software MTP in pass through mode. SMTP supports DTMF Interworking for nonsecure calls, and this feature adds support for SRTP DTMF interworking for secure calls.

CUCM support for this feature is expected to be implemented in a later release.

Restrictions for SRTP-DTMF Interworking

- The SRTP-DTMF Interworking feature supports only the codec-passthrough format.
- The SRTP-DTMF Interworking feature does not support multiple concurrent Synchronised Sources (SSRCs) with the same destination IP and port.
- The calls that support SRTP-DTMF Interworking may have a minor performance impact as compared to calls supported on nonsecure DTMF interworking.

Supported Platforms for SRTP-DTMF Interworking

From Cisco IOS XE 17.10.1a, the following platforms support SRTP DTMF interworking with SMTP:

- Cisco 4461 Integrated Services Router (ISR)
- Cisco Catalyst 8200 Edge Series Platforms
- Cisco Catalyst 8300 Edge Series Platforms
- Cisco 8300 Series Secure Routers
- Cisco Catalyst 8000V Edge Software

Configuring Support for Software Media Termination Point

Perform the following tasks to enable and configure the support for Software Media Termination Point feature.

Procedure

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 **sccp local** *interface-type interface-number* [**port** *port-number*]

Example:

```
Router(config)# sccp local gigabitethernet0/0/0
```

Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco UCM.

- *interface type*: Can be an interface address or a virtual-interface address such as Ethernet.
- *interface number*: Interface number that the SCCP application uses to register with Cisco UCM.
- (Optional) **port** *port-number*: Port number used by the selected interface. Range is 1025 to 65535. Default is 2000.

Step 4 **sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number*

Example:

```
Router(config)# sccp ccm 10.1.1.1 identifier 1 version 7.0+
```

Adds a Cisco UCM server to the list of available servers and sets the following parameters:

- *ipv4-address*: IP version 4 address of the Cisco UCM server.
- *ipv6-address*: IP version 6 address of the Cisco UCM server.
- *dns*: DNS name.
- **identifier**: Specifies the number that identifies the Cisco UCM server. Range is 1 to 65535.
- **port** *port-number* (Optional): Specifies the TCP port number. Range is 1025 to 65535. Default is 2000.
- **version** *version-number*: Cisco UCM version. Valid versions are 3.0, 3.1, 3.2, 3.3, 4.0, 4.1, 5.0.1, 6.0, and 7.0+. There is no default value.

Step 5 **sccp**

Example:

```
Router(config)# sccp
```

Enables the Skinny Client Control Protocol (SCCP) and its related applications (transcoding and conferencing).

Step 6 **sccp ccm group** *group-number*

Example:

```
Router(config)# sccp ccm group 10
```

Creates a Cisco UCM group and enters SCCP Cisco UCM configuration mode.

- *group-number*: Identifies the Cisco UCM group. Range is 1 to 50.

Step 7 **associate ccm** *identifier-number* **priority** *number*

Example:

```
Router(config-sccp-ccm)# associate ccm 10 priority 3
```

Associates a Cisco UCM with a Cisco UCM group and establishes its priority within the group:

- *identifier-number*: Identifies the Cisco UCM. Range is 1 to 65535. There is no default value.
- **priority** *number*: Priority of the Cisco UCM within the Cisco UCM group. Range is 1 to 4. There is no default value. The highest priority is 1.

Step 8 **associate profile** *profile-identifier* **register** *device-name*

Example:

```
Router(config-sccp-ccm)# associate profile 1 register MTP0011
```

Associates a DSP farm profile with a Cisco UCM group:

- *profile-identifier*: Identifies the DSP farm profile. Range is 1 to 65535. There is no default value.
- **register** *device-name*: Device name in Cisco UCM. A maximum of 15 characters can be entered for the device name.

Step 9 **dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]

Example:

```
Router(config-sccp-ccm)# dspfarm profile 1 mtp
```

Enters DSP farm profile configuration mode and defines a profile for DSP farm services:

- *profile-identifier*: Number that uniquely identifies a profile. Range is 1 to 65535. There is no default.
- **conference**: Enables a profile for conferencing.
- **mtp**: Enables a profile for MTP.
- **transcode**: Enables a profile for transcoding.
- **security**(Optional): Enables a profile for secure DSP farm services. For more information on configuration examples, see section #unique_264 unique_264_Connect_42_GUID-5FB6A48E-204C-45AA-AE63-413B075A7871, on page 273.

Step 10 **trustpoint** *trustpoint-label*

Example:

```
Router(config-dspfarm-profile)# trustpoint dspfarm
```

(Optional) Associates a trustpoint with a DSP farm profile.

Step 11 **codec** *codec*

Example:

```
Router(config-dspfarm-profile)# codec g711ulaw
```

Specifies the codecs supported by a DSP farm profile.

- codec-type: Specifies the preferred codec. Enter ? for a list of supported codecs

  Repeat this step for each supported codec.

Step 12 **maximum sessions** {**hardware** | **software**} *number*

Example:

```
Router(config-dspfarm-profile)# maximum sessions software 10
```

Specifies the maximum number of sessions that are supported by the profile.

- **hardware**: Number of sessions that MTP hardware resources can support.
- **software**: Number of sessions that MTP software resources can support.
- *number*: Number of sessions that are supported by the profile. Range is 0 to x. Default is 0. The x value is determined at run time depending on the number of resources available with the resource provider.

Step 13 **associate application sccp**

Example:

```
Router(config-dspfarm-profile)# associate application sccp
```

Associates SCCP to the DSP farm profile.

Step 14 **no shutdown**

Example:

```
Router(config-dspfarm-profile)# no shutdown
```

Changes the status of the interface to the UP state.

Examples: Support for Software Media Termination Point

The following example shows a sample configuration for the Support for Software Media Termination Point feature:

```
sccp local GigabitEthernet0/0/1
sccp ccm 10.13.40.148 identifier 1 version 6.0
```

```
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/0/1
 associate ccm 1 priority 1
 associate profile 6 register RR_RLS6
!
 dspfarm profile 6 mtp
 codec g711ulaw
 maximum sessions software 100
 associate application SCCP
!
!
gateway
media-inactivity-criteria all
timer receive-rtp 400
```

The following example shows a sample configuration for the SRTP-DTMF Interworking feature-with secure dspfarm profile:

```
sccp local GigabitEthernet0/0/0
sccp ccm 172.18.151.125 identifier 1 version 7.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/0/0
 associate ccm 1 priority 1
 associate profile 1 register Router
!
dspfarm profile 1 mtp security
 trustpoint IOSCA
 codec g711ulaw
 codec pass-through
 tls-version v1.2
 maximum sessions software 5000
 associate application SCCP
```

Note SR-TP traffic can pass through an SMTP resource when the dspfarm profile is provisioned with codec pass-through, and if it does not have TLS and security-related configuration. For traffic flows that require SRTP-DTMF interworking support, the SMTP dspfarm profile must include the **security** keyword and the TLS and codec pass-through configuration. This dspfarm resource profile can also pass through SRTP traffic independent of SRTP-DTMF interworking support.

Verifying Software Media Termination Point Configuration

To verify and troubleshoot this feature, use the following **show** commands.

- To verify information about SCCP, use the **show sccp** command:

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.13.40.157, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.13.40.148, Port Number: 2000
```

```
                Priority: N/A, Version: 6.0, Identifier: 1
                Trustpoint: N/A
```

- To verify information about the DSPfarm profile, use the **show dspfarm profile** command:

```
Router# show dspfarm profile 6

Dspfarm Profile Configuration
 Profile ID = 6, Service = MTP, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Number of Resource Configured : 100
 Number of Resource Available : 100
 Hardware Configured Resources : 0
 Hardware Available Resources : 0
 Software Resources : 100
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
```

- To verify information about the secure DSPfarm profile status, use the **show dspfarm profile** command and check that the secure service mode is set:

```
Router# show dspfarm profile 2
Dspfarm Profile Configuration
 Profile ID = 2, Service = MTP, Resource ID = 2
 Profile Service Mode : secure
 Trustpoint : IOSCA
 TLS Version  : v1.2
 TLS Cipher   : AES128-SHA
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Total Number of Resources Configured : 8000
 Total Number of Resources Available : 8000
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Hardware Configured Resources : 0
 Hardware Resources Out of Service: 0
 Software Configured Resources : 8000
 Number of Hardware Resources Active : 0
 Number of Software Resources Active : 0
 Codec Configuration: num_of_codecs:2
 Codec : pass-through, Maximum Packetization Period : 0
 Codec : g711ulaw, Maximum Packetization Period : 30
```

- To display statistics for the SCCP connections, use the **show sccp connections** command:

```
Router# show sccp connections

sess_id   conn_id    stype  mode       codec    ripaddr        rport   sport
16808048  16789079    mtp   sendrecv   g711u    10.13.40.20    17510   7242
16808048  16789078    mtp   sendrecv   g711u    10.13.40.157   6900    18050
```

For SMTP secure DTMF, the **show sccp connections** command displays the codec type (pass-th), the s-type (s-mtp), and information about the DTMF method (rfc2833_pthru):

```
Router# show sccp connections

sess_id   conn_id   stype   mode     codec    sport  rport   ripaddr conn_id_tx   dtmf_method
16791234  16777308  s-mtp   sendrecv  pass_th  8006   24610   172.18.153.37
rfc2833_pthru
16791234  16777306  s-mtp   sendrecv  pass_th  8004   17576   172.18.154.2
rfc2833_report

Total number of active session(s) 1, and connection(s) 2
```

- To display information about RTP connections, use the **show rtpspi call** command:

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId  dstCallId   Mode      LocalRTP  RmtRTP  LocalIP     RemoteIP    SRTP
1    22      19         Snd-Rcv   7242      17510   0x90D080F   0x90D0814    0
2    19      22         Snd-Rcv   18050     6900    0x90D080F   0x90D080F    0
```

If SRTP DTMF interworking is active, the SRTP field shows a non-zero value:

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId  dstCallId   Mode      LocalRTP  RmtRTP  LocalIP     RemoteIP    SRTP
1   13      14          Snd-Rcv   8024      18270   0xA7A5355   0xAC129A02   1
2   14      13          Snd-Rcv   8026      24768   0xA7A5355   0xAC129925   1
```

- To display information about VoIP RTP connections, use the **show voip rtp connections** command:

```
Router# show voip rtp connections
VoIP RTP Port Usage Information
Max Ports Available: 30000, Ports Reserved: 100, Ports in Use: 102
Port range not configured, Min: 5500, Max: 65499
VoIP RTP active connections :
No. CallId    dstCallId  LocalRTP  RmtRTP    LocalIP         RemoteIP
1     114       117        19822    24556   10.13.40.157     10.13.40.157
2     115       116        24556    19822   10.13.40.157     10.13.40.157
3     116       115        19176    52625   10.13.40.157     10.13.40.20
4     117       114        16526    52624   10.13.40.157     10.13.40.20
```

- Additional, more specific, **show** commands that can be used include the following:
  - **show sccp connection callid**
  - **show sccp connection connid**
  - **show sccp connection sessionid**
  - **show rtpspi call callid**
  - **show rtpspi stat callid**
  - **show voip rtp connection callid**
  - **show voip rtp connection type**
  - **show platform hardware qfp active feature sbc global**

- To isolate specific problems, use the **debug sccp** command:
  - **debug sccp** [**all** | **config** | **errors** | **events** | **keepalive** | **messages** | **packets** | **parser** | **tls**]

Feature Information for Support for Software Media Termination Point

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 23: Feature Information for Support for Software Media Termination Point

Feature Name	Releases	Feature Information
Support for Software Media Termination Point	Cisco IOS XE Release 2.6 S	Software Media Termination Point (MTP) provides the capability for Cisco Unified Communications Manager (Cisco UCM) to interact with a voice gateway via Skinny Client Control Protocol (SCCP) commands. These commands allow the Cisco UCM to establish an MTP for call signaling.
Support for Secure Real-time Transport Protocol (SRTP) Dual-Tone Multi-Frequency (DTMF) Interworking	Cisco IOS XE Dublin 17.10.1a	The Secure Real-time Transport Protocol (SRTP) Dual-Tone Multi-Frequency (DTMF) feature provides support for DTMF interworking between Secure Software MTP in pass-through mode only and CUCM.

CHAPTER 20

Troubleshooting

Troubleshooting

Troubleshoot using system reports

System reports

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
2. IOSd core file and IOS crashinfo file if there was an IOSd process crash
3. Tracelogs
4. System process information
5. Bootup logs
6. 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 bundling makes it convenient to get a crash snapshot in one place. The file can also be moved off the box for analysis.

The 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
```

Sample system report

See this sample report with the file name `Router1_RP_0-system-report_20210204-163559-UTC`

Here, 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
```

APPENDIX A

Unsupported commands

The Cisco 8300 Series Secure Routers contain a series of commands with the **logging** or **platform** keywords that either produce no output or produce output that is not useful for customer purposes. Such commands that are not useful for customer purposes are considered as unsupported commands. You will not find any further Cisco documentation for the unsupported commands.

This is a list of unsupported commands for the Cisco 8300 Series Secure Routers:

- backplaneswitchport
- clear logging onboard slot f0 dram
- clear logging onboard slot f0 voltage
- clear logging onboard slot f0 temperature
- show logging onboard slot f0 dram
- show logging onboard slot f0 serdes
- show logging onboard slot f0 status
- show logging onboard slot f0 temperature
- show logging onboard slot f0 uptime
- show logging onboard slot f0 uptime latest
- show logging onboard slot f0 voltage
- show logging onboard slot 0 dram
- show logging onboard slot 0 serdes
- show logging onboard slot 0 status
- show logging onboard slot 0 temperature
- show logging onboard slot 0 uptime
- show logging onboard slot 0 uptime latest
- show logging onboard slot 0 voltage
- show platform software adjacency r0 special

- show platform software adjacency rp active special
- show platform hardware backplaneswitch-manager RP active summary
- show platform hardware backplaneswitch-manager RP active subslot GEO statistics
- show platform software backplaneswitch-manager RP [active [detail]]
- show platform hardware backplaneswitch-manager [R0 [status] | RP]
- show platform hardware backplaneswitch-manager RPactive CP statistics
- platform hardware backplaneswitch-manager rp active subslot GEO statistics
- show platform software ethernet rp active l2cp
- show platform software ethernet rp active l2cp interface GigabitEthernet0
- show platform software ethernet rp active loopback
- show platform software ethernet rp active vfi
- show platform software ethernet r0 vfi
- show platform software ethernet r0 vfi id 0
- show platform software ethernet r0 vfi name GigabitEthernet0
- show platform software ethernet r0 l2cp
- show platform software ethernet r0 l2cp interface GigabitEthernet0
- show platform software ethernet r0 bridge-domain statistics
- show platform software flow r0 exporter name GigabitEthernet0
- show platform software flow r0 exporter statistics
- show platform software flow r0 global
- show platform software flow r0 flow-def
- show platform software flow r0 interface
- show platform software flow r0 ios
- show platform software flow r0 monitor
- show platform software flow r0 sampler
- show platform hardware qfp active classification feature-manager label GigabitEthernet 0 0
- show platform software interface f0 del-track
- show platform software interface fp active del-track
- show platform software rg r0 services
- show platform software rg r0 services rg-id 0
- show platform software rg r0 services rg-id 0 verbose
- show platform software rg r0 services verbose

- show platform software rg r0 statistics
- show platform software rg rp active services
- show platform software rg rp active services rg-id 0
- show platform software rg rp active services rg-id 0 verbose
- show platform software rg rp active statistics
- show platform hardware slot 0 dram statistics
- show platform hardware slot f0 dram statistics
- show platform hardware slot 0 eobc interface primary rmon
- show platform hardware slot 0 eobc interface primary status
- show platform hardware slot 0 eobc interface standby rmon
- show platform hardware slot 0 eobc interface standby status
- show platform hardware slot f0 eobc interface primary rmon
- show platform hardware slot f0 eobc interface primary status
- show platform hardware slot f0 eobc interface standby rmon
- show platform hardware slot f0 eobc interface standby status
- show platform hardware slot f0 sensor consumer
- show platform hardware slot f0 sensor producer