Catalyst 8200 and Catalyst 8300 Edge Software Configuration Guide

First Published: 2026-05-04

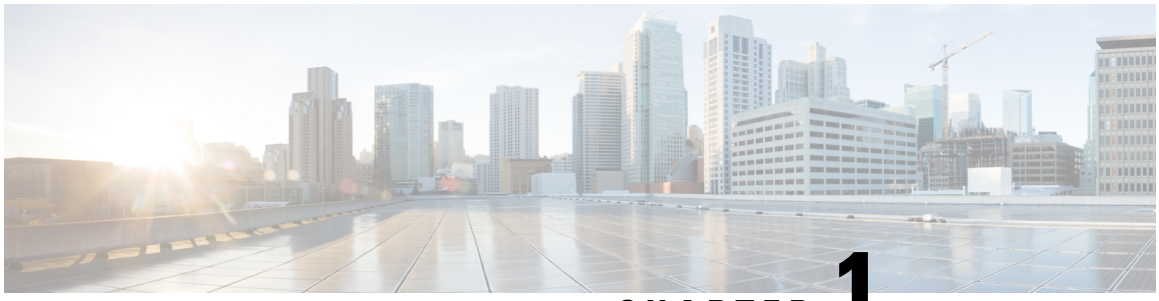
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Reference wapper Preface topic here

Reference Preface Map here

Reference wapper Preface topic here



CHAPTER 1

Overview of Catalyst 8200 and Catalyst 8300 Series Edge Platforms

Information on Cisco Catalyst 8300 and 8200 Series Edge Platforms

The Cisco Catalyst 8300 and 8200 Series Edge Platforms are a series of cloud edge platforms that are

- 5G-ready, cloud edge platforms designed for accelerated services
- cloud edge platforms designed for accelerated services, multi-layer security
- cloud-native agility, and edge intelligence to accelerate your journey to cloud.

These platforms are designed for medium-sized and large enterprise branch offices and support both Cisco IOS XE and Cisco IOS XE SD-WAN functionality.

Cisco Catalyst 8300 and 8200 Series Edge Platforms with Cisco IOS XE SD-WAN Software deliver Cisco secure, cloud-scale SD-WAN solution for the branch. The Cisco Catalyst 8300 and 8200 Series Edge Platforms are built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises. The platform provides a higher WAN port density and the capability for a redundant power supply.

The Cisco Catalyst 8300 and 8200 Series Edge Platforms have a wide variety of interface options to choose from, ranging from lower and higher module density with backward compatibility to a variety of existing WAN, LAN, LTE, voice, and compute modules. Powered by Cisco IOS XE, fully programmable software architecture, and API support, these platforms can facilitate automation at scale to achieve zero-touch IT capability while migrating workloads to the cloud. They also come with Trustworthy Solutions 2.0 infrastructure, which secures the platforms against threats and vulnerabilities, provides integrity verification and remediation of threats.

The Cisco Catalyst 8300 and 8200 Series Edge Platforms are suited for medium-sized and large enterprise branch offices for high WAN IPsec performance with integrated SD-WAN services.

Cisco Catalyst 8300 and 8200 Series Edge Platforms target these use-cases:

- Enterprise Branch office, Managed Service Provider CPE, Internet Gateway for Direct Internet Access (DIA), Secure Access Service Edge (SASE) cloud platform with SD-WAN
- Next-generation Software Defined (SD) Branch routing platforms

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 Amsterdam 17.3 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 switches from autonomous to controller mode, the startup configuration and the NVRAM information (including certificates) are erased. This action is equivalent to a 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, ensure that the device configuration is set to auto-boot.

Switch between controller and autonomous modes using bootstrap configuration files

On a device that already runs a Cisco IOS XE non SD-WAN image, after installing Cisco IOS XE Release 17.3.2 or later image, the device boots up in autonomous mode.

On a device that already runs a Cisco IOS XE SD-WAN image, after installing Cisco IOS XE Release17.3.1r or later image, the device boots up in controller mode.

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.

These are the Cisco Catalyst 8300 and 8200 Series Edge Platforms models:

- C8300-2N2S-4T2X
- C8300-2N2S-6T
- C8300-1N1S-4T2X
- C8300-1N1S-6T
- C8200-1N-4T
- C8200L-1N-4T

Supported modules and features on Cisco 8300 and 8200 Series Edge Platforms

This table provides the supported modules and features on Cisco Catalyst 8300 and 8200 Series Edge Platforms.

Table 1: Supported Modules and Features on Cisco 8300 and 8200 Series Edge Platformsup table title

Features	Cisco 8300	Cisco 8200	Cisco 8200L
Service Plane Applications (UTD, AppQoE, and TcpOpt)	Yes	No	No
CPU Core	8 Core C8300-2N2S-4T2X supports 12 Core	8 Core	4 Core
CPU Memory	8 G	8 G	4 G
Backplane Support	10 G	10 G	1 G

Default Configuration

Default configuration indicates the tasks performed by the device during the boot up process.

When you boot up the device in autonomous mode, the device looks for a file named `c8000.cfg` in the bootflash. If the file is not found in the bootflash, the device then looks for `ciscortr.cfg` file. 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.

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.

Configure Global Parameters

Global parameters refer to configuration settings that apply to the entire router, influencing its overall operation and behavior rather than being specific to a single interface or feature. To manually define Gigabit Ethernet interfaces, follow these steps, beginning from global configuration mode.

Procedure

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.

Configure Gigabit Ethernet Interfaces

A Gigabit Ethernet Interface is a physical network interface used to connect devices in a local area network (LAN) for significantly improved throughput.To manually configure Gigabit Ethernet interfaces, follow these steps, beginning from global configuration mode.

Procedure

Step 1 **interfacegigabitethernet***slot/bay/port*

Example:

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

Enters the configuration mode for a Gigabit Ethernet interface on the device.

Step 2 **ip address***ip-addressmask*

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 **noshutdown**

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.

Configure a Loopback Interface

A loopback interface is a virtual network interface that is implemented entirely in software and is not associated with any physical hardware. It allows a device to send and receive data packets to itself, facilitating internal communication and diagnostics without involving external network components.This task explains how to configure a loopback interface.

Procedure

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-addressmask*

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** command.

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.

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
```

Verifying Loopback Interface Configuration

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

```
Router#
show interface loopback 0
Loopback0 is up, line protocol is up
Hardware is Loopback
Internet address is 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 the following 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
```

Dynamic Allocation of Cores

Dynamic allocation of cores provide flexibility for users to leverage the CPU cores for different services or for CEF/IPSec performances. The Catalyst 8000 Series Edge platforms are equipped with a minimum of eight 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 17.4 onwards, you can use the **platform resource { service-plane-heavy | data-plane-heavy }** command to adjust the cores across service plane and data plane. However, you have to reboot the device for the configured profile to take effect.

These are the list of Catalyst 8000 Series Edge platforms that support changing the core allocations dynamically:

- C8300-2N1S-6T
- C8300-2N1S-4T2X
- C8300-2N2S-6T
- C8300-2N2S-4T2X
- C8200-1N-4T

Configure Command-Line Access

Command-line access refers to the method of interacting with the device's operating system through a text-based interface known as the Command-Line Interface (CLI). This interface allows users to enter commands directly to configure, manage, and troubleshoot the device. The CLI in Cisco IOS XE provides a powerful and flexible way to control the device, supporting a wide range of commands for various functions. To configure parameters to control access to the device, use 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 here specifies a console terminal for access.

Step 2 **password***password*

Example:

```
Router(config-line)#password 5dr4Hepw3
```

Specifies a unique password for the console terminal line.

Step 3 **login**

Example:

```
Router(config-line)#login
```

Enables password checking at terminal session login.

Step 4 **exec-timeout***minutes* [*seconds*]

Example:

```
Router(config-line)#

 exec-timeout 5 30
Router(config-line)#
```

Sets the interval during which the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, adds seconds to the interval value.

The example provided here shows a timeout of 5 minutes and 30 seconds. Entering a timeout of **0 0** specifies never to time out.

Step 5 **exit**

Example:

```
Router(config-line)#exit
```

Exits line configuration mode to re-enter global configuration mode.

Step 6 **line** [| **console**| **tty**| **vty**] *line-number*

Example:

```
Router(config)#

 line vty 0 4
Router(config-line)#
```

Specifies a virtual terminal for remote console access.

Step 7 **password***password*

Example:

```
Router(config-line)#password aldf2ad1
```

Specifies a unique password for the virtual terminal line.

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.

This configuration shows the command-line access commands.

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

```
!
line console 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (

 default
)
stopbits 1 (

 default
)
line vty 0 4
password secret
login
!
```

Configure 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.

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.

Configure Routing Information Protocol

This task covers details on configuring Routing Information Protocol that helps routers determine the most efficient path for data packets to travel across a network.

Procedure

Step 1 **routerrip**

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 **noauto-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.

This completes the configuration of Routing Information Protocol.

What to do next

Verify the Routing Information Protocol configuration is complete.

Use the **show running-config** command from privileged EXEC mode.

```
    !
    Router#
    show running-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
    :
    :
    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
```

Configure Enhanced Interior Gateway Routing Protocol

This task covers details on configuring Enhanced Interior Gateway Routing Protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol designed to automate routing decisions and configuration within a computer network, facilitating the efficient and reliable exchange of routing information between routers.

Procedure

Step 1 **router eigrp** *as-number*

Example:

```
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.

This completes the configuration of EIGRP.

What to do next

Verify that EIGRP configuration is complete:

This 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 the following:

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

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D     192.0.2.3/8 [90/409600] via 192.0.2.2, 00:00:02, Ethernet0/0
```

Configure Routing Information Protocol

This task covers details on configuring Routing Information Protocol that helps routers determine the most efficient path for data packets to travel across a network.

Procedure

Step 1 **routerrip**

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 **noauto-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.

This completes the configuration of Routing Information Protocol.

What to do next

Verify the Routing Information Protocol configuration is complete.

Use the **show running-config** command from privileged EXEC mode.

```
    !
    Router#
    show running-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
    :
    :
    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
```

Configure Enhanced Interior Gateway Routing Protocol

This task covers details on configuring Enhanced Interior Gateway Routing Protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol designed to automate routing decisions and configuration within a computer network, facilitating the efficient and reliable exchange of routing information between routers.

Procedure

Step 1 **router eigrp** *as-number*

Example:

```
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.

This completes the configuration of EIGRP.

What to do next

Verify that EIGRP configuration is complete:

This 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 the following:

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

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D     192.0.2.3/8 [90/409600] via 192.0.2.2, 00:00:02, Ethernet0/0
```

Cisco IOS XE software

Access Cisco IOS XE software

Use the console port to access the command line interface directly or when using Telnet.

Console connections

The CON port is an EIA or 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.

Connect to the console port

Use this procedure when you need direct access to device configuration via the console port.

Procedure

Step 1 Configure your terminal emulation software with these settings.

- 9600 bits per second (bps),
- eight data bits,
- no parity, and
- no flow control

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

Your terminal displays the device's console output, allowing direct access to device configuration.

Access the console interface

Use the console interface to directly manage and configure the router.

Follow these steps to access the console interface:

Procedure

Step 1 Enter the following command.

```
Router> enable
```

Step 2 If the enable password has not been configured, proceed to Step 3. Otherwise, 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. Enter the commands to complete your tasks.

Step 3 If you enter the **setup** command, refer to *Using Cisco Setup Command Facility* .

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

```
Router# quit
```

You successfully access and exit the privileged EXEC mode in the console interface.

Access the device console using SSH

Secure Shell is a protocol that provides a secure remote access connection to network devices. To enable SSH support on the device, access the device console using SSH as described in these steps.

Before you begin

Ensure the device is reachable via IP and supports SSH.

Install SSH client software on your management workstation.

Procedure

Step 1 Configure the device host name.

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

Here, *host name* is the device host name 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 for your device.

```
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.

You will establish a secure SSH session to the device console.

Remote CLI access methods

This section provides procedures to access the CLI from a remote console using Telnet.

- Enable console access to the device via Telnet

- Access a console interface using Telnet

Enable console access to the device via Telnet

This section describes the necessary steps and configuration requirements for enabling remote access to a device console using Telnet.

Before you begin

Ensure the device is configured to support remote access using Telnet over a TCP or IP network.

Configure the device's virtual terminal lines with the **line vty** command.

Set the vty lines to require user login and specify a password to secure remote access. For details about the **line vty** command, refer the Cisco IOS Terminal Services Command Reference document.

Use this task to set up remote console access for network management.

Procedure

Step 1 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 on the vty lines.

Step 2 To ensure login is not disabled on the lines when using AAA authentication, configure the list with the **login authentication** command and also define the login list with the **aaa authentication login** 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.

Step 3 Ensure the device has a configured hostname or an IP address before attempting Telnet access.

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.

The device is now configured to allow remote console access via Telnet using password or AAA authentication.

Access a console interface using Telnet

Use this procedure when you need to manage a device from your terminal or PC via Telnet.

Follow these steps to access the console interface:

Before you begin

Ensure Telnet is enabled on the device.

Procedure

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

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

Here, *host* refers to 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
When you use 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
```

You are connected to the console interface of the remote device.

USB serial console ports

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. Refer to the 'Connecting to a Console Terminal or Modem' section for detailed instructions.

- Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platform
- Hardware Installation Guide for Cisco Catalyst 8200 Series Edge Platforms

Keyboard shortcuts

A keyboard shortcut is a key combination or sequence that

- allows commands to be entered without regard to case sensitivity,
- enables the use of abbreviated commands and parameters, and
- requires that abbreviations contain enough unique letters to distinguish them from any other available commands or parameters.

This 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.

History buffer

The history buffer is a CLI feature that:

- stores the last 20 commands you entered,
- enables history substitution so you can access previous commands without retyping them, and
- uses special abbreviated commands to quickly recall and reuse stored entries.

This 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 you are in EXEC mode, lists the last few commands you entered.

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

Command modes

A command mode is a CLI access level that

- determines which IOS XE commands are available,
- secures and isolates different configuration functions, and
- defines the privileges assigned to each user or process within the operating system.

Cisco IOS XE provides the same command modes as traditional Cisco IOS and supports these modes only in autonomous mode. You access Cisco IOS XE software through the CLI, which divides commands into several modes. The commands available to you always depend on your current mode. When you enter a question mark (**?**) at the CLI prompt, you can see a list of commands available in that 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.

This 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>`	Enter the **logout** command.
Privileged EXEC	From user EXEC mode, enter the **enable** command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, enter the **configure terminal** command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, enter 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 ui command. To return to privileged EXEC mode, enter the **end** command.

Command Mode	Access Method	Prompt	Exit Method
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, enter the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon#>`	To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded.

Diagnostic mode

A diagnostic mode is a device operation state that

- offers a comprehensive user interface for troubleshooting, surpassing the limited access methods of previous devices
- enables diagnosis and troubleshooting of Cisco IOS problems even when the Cisco IOS process is not functioning properly, and
- provides diagnostic commands that are also accessible in privileged EXEC mode when the device is operating normally.

The device enters diagnostic mode in several scenarios. If the IOS process fails, your device might boot into diagnostic mode automatically, or it may reset first based on device configuration. Additionally, if a user-configured access policy uses the **transport-map** command to direct access into diagnostic mode, the device follows this policy. The device also enters diagnostic mode when it receives a break signal (such as **Ctrl-C** or **Ctrl-Shift-6**) during access, provided it is configured to do so in response to the break

Additional reference information

In diagnostic mode, you have have access to a subset of commands from user EXEC mode. These commands allow users 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 to or from the device using remote access methods such as FTP, TFTP, and SCP.

CLI help commands

Use these CLI commands to access help or list available options and arguments.

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. To get help that is specific to a command mode, a command, a keyword, or an argument, use one of the following commands.

Table 5: Help Commands

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

Command help options and symbols

The Cisco IOS XE software provides command-line help so you can enter commands accurately.

- Entering a question mark (**?**) at the CLI prompt or after part of a command displays a list of 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 ?**.
- Command help output shows optional or required arguments, along with brief descriptions.
- The **<cr>** symbol indicates that pressing **Enter** will complete the command.
- If **<cr>** appears at the end of help output, all previous options are optional. If **<cr>** is not displayed, further arguments or keywords are required.
- The **<cr>** symbol refers to the carriage return key, which is labeled **Enter** on most modern keyboards. On older keyboards, the carriage return key is the **Return** key.

Table 6: 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 from '>' to '#', for example, for example, `Router>` to `Router#`

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

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

Command	Comment

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  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)#`
	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.

`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`
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

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

Command	Comment

`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.

CLI command forms

A CLI command form is a configuration command variation that:

- typically has a **no** form to disable a function and a standard form to enable or re-enable a function,
- often includes a default form that resets the command to its default setting using the **default** keyword, and
- is fully documented in Cisco IOS Software command reference publications, which explain the syntax and functions of the standard, **no**, and **default** forms.

Additional reference information

The Cisco IOS software command reference publications document the syntax and effects of both the **no** and **default** forms for configuration commands. To see available **default** commands on your system, enter **default ?** in the appropriate command mode.

Note To disable IP routing (which is enabled by default), use the **no ip routing** command.To re-enable IP routing, use the **ip routing** command.

To reset a command to its default setting, use the default command-name syntax.

Save configuration changes

To ensure your configuration changes are retained after a software reload or power outage, you must save the running configuration to the startup configuration. This task writes your current settings to NVRAM, making them persistent across device reboots.

Before you begin

Make sure you have the necessary privileges to execute configuration commands in the CLI.

Follow these steps to save configuration changes:

Procedure

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.

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.

Your configuration changes are saved to NVRAM and retained across device reboots or power loss.

Configuration files

A configuration file is a data file that stores and manages the operational settings of a Cisco router. Key details about configuration file storage and maintenance include:

- The startup configuration file resides in the NVRAM: file system.
- The running configuration files are stored in the system: file system.
- Maintains a consistent storage arrangement across different Cisco router platforms.

Additional reference information

Users should routinely back up the startup configuration file on any Cisco router. Copy the startup configuration file from NVRAM to another file system on the router and to a network server to back it up. TA backup makes it easy for you to recover the startup configuration file if the file in NVRAM becomes unusable.

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

To learn more about managing configuration files, refer the “Managing Configuration Files” section in the Cisco IOS XE Configuration Fundamentals Configuration Guide.

Filtering output from the show and more commands

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

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

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

The output matches certain lines of information in the configuration file.

Example

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

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

Save configuration changes before powering off

Ensure you save any configuration changes you want to keep by using the **copy running-config startup-config** command before powering off the device.

If you power off the device by switching the power supply to Off without saving, you will lose any changes made to the running configuration since the last save to NVRAM. When you power the device back on, it loads the configuration stored in NVRAM. Only saved settings are retained after startup.

Cisco software images

The Cisco IOS XE Software is packaged in feature sets consisting of software images that provide the following benefits:

- contains a group of feature sets that are available for a specific platform depends on which Cisco software images are included in a release.
- is distributed in multiple feature sets for various deployment needs, and
- supports designated Cisco platforms.

Additional reference information

To identify which software images are available for a particular platform, or whether a feature is present in a given image, use the Cisco Feature Navigator or see the Release Notes for Cisco IOS XE.

Cisco feature navigators

A Cisco feature navigator is an online tool that

- provides details about platform support for Cisco devices,
- enables you to identify which Cisco IOS XE software images support specific features, and
- facilitates software image and feature set searches without requiring a Cisco.com account.

Additional reference information

To find information about platform support details and software image support, refer to the Cisco Feature Navigator.

Software advisor

The Software advisor tool is a Cisco resource that:

- allows you to check if a feature is supported in a specific Cisco IOS XE release,
- helps you locate the software documentation for a given feature, and
- enables you to verify the minimum software requirements of Cisco IOS XE software based on the hardware installed on your device.

Cisco provides the Software Advisor tool, which is available in the Tools and Resources section.

Release notes

The Release Notes document for Cisco Catalyst 8000 Series Edge Platforms is a release-specific resource that:

- provides memory recommendations for the platform,
- lists open and resolved severity 1 and 2 caveats, and
- focuses on the current release without offering cumulative feature information from previous releases

For cumulative feature information, refer to the Cisco Feature Navigator at http://www.cisco.com/go/cfn/.

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.

Best practice for CLI session management

Follow these best practices to ensure secure and effective CLI session management:

- Configure inactivity timeouts to automatically close idle CLI sessions and enhance security.
- Lock your CLI session to prevent others from making configuration changes at the same time.
- Reserve enough system capacity for CLI session access so that you and other administrators can always access the system, even under high load.

Configure 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. Set 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"`.

The device automatically ends the CLI session after the specified period of inactivity, increasing security by preventing unauthorized access to unattended sessions.

Lock a CLI session

Use this task to lock your CLI session when stepping away, requiring a temporary password for re-entry.

Before you begin

To configure a temporary password on a CLI session, first configure the line using the **lockable** command, and then use the **lock** command in EXEC mode. When the line is configured as **lockable**, you can use the **lock** command to assign a temporary password.

Procedure

Step 1 `Router# configure terminal`

Enters global configuration mode.

Step 2 Enter the line where 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
```

Your CLI session is locked. Accessing the session again requires the temporary password you set.

Software Installation

A consolidated package is a bootable image used for installing software on a router that

- comprises a bundle of modular software units, known as subpackages,
- allows each subpackage to independently control a distinct set of router functions, and
- facilitates individual subpackage upgrades and typically results in reduced boot times.

Upgrade software during a scheduled maintenance window to minimize service disruption. The router must be rebooted to apply the software upgrade.

ROMMON images

A ROMMON image is a software package that

- Is utilized by the ROMmon software on a router.
- Operates independently from the consolidated package typically used to boot the router, and
- Can be upgraded separately to update the router's ROMmon software.

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.

For detailed information on ROMmon, refer to the Hardware Installation Guide for the Cisco Catalyst 8000 Series Edge Platforms.

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

File systems

This table lists the file systems available on the Cisco Catalyst 8000 Series Edge Platform.

Table 7: Device File Systems

File System	Description
bootflash:	Boot flash memory file system.
flash:	Alias to the boot flash memory file system above.
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.
usb0: USB 3.0 Type-A usb1: USB 3.0 Type-B	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 describes the autogenerated files and directories that may be created. It also explains how to manage the files in these directories.

Table 8: Autogenerated Files

File or Directory	Description
crashinfo files	Crash info 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 at bootup. You can erase the .core files in this directory without impacting device functionality. However, do not erase the directory itself.

File or Directory	Description
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.
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 are not part of device operations and can be erased without affecting device 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.

Configuration register for autoboot

The configuration register can be used to change behavior. This includes control over the device's boot process. Set the configuration register to 0x0 to boot into ROM, by using one of these 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

Manage and configure a device to run using a consolidated package

You can manage and configure a device using cope and boot commands.

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:/

          81921   drwx           237568   Jul 8 2020 11:17:27 -07:00  tracelogs
          98305   drwx             4096  Jun 24 2020 17:26:48 -07:00  license_evlog
          237569  drwx             4096  Jun 24 2020 17:26:48 -07:00  core
          131073  drwx             4096  Jun 24 2020 17:26:45 -07:00  onep
          16      -rw-               30  Jun 24 2020 17:26:38 -07:00
throughput_monitor_params
          13      -rw-           134458  Jun 24 2020 17:26:37 -07:00  memleak.tcl
          401409  drwx             4096  Jun 24 2020 17:26:23 -07:00  .dbpersist
          15      -rwx             1314  Jun 24 2020 17:26:21 -07:00  trustidrootx3_ca.ca
          14      -rw-            20109  Jun 24 2020 17:26:21 -07:00  ios_core.p7b
          73729   drwx             4096  Jun 24 2020 17:26:19 -07:00  gs_script
          12      -rw-              182  Jun 24 2020 17:26:19 -07:00  mode_event_log
          221185  drwx             4096  Jun 24 2020 17:26:13 -07:00  .prst_sync
          212993  drwx             4096  Jun 24 2020 17:25:59 -07:00  .ssh
          368641  drwx             4096  Jun 24 2020 17:25:55 -07:00  .rollback_timer
          376833  drwx             4096  Jun 24 2020 17:25:55 -07:00  .installer
          458753  drwx             4096  Jun 24 2020 17:25:47 -07:00  sysboot
          11      -rw-        696368193  Jun 24 2020 17:15:13 -07:00

          Router# copy tftp: bootflash:Address or name of remote host []? 203.0.113.2
        Source filename []? /auto/tftp-ngio/test/c8000be-universalk9.17.03.01prd14.SPA.bin

          Destination filename [c8000be-universalk9.17.03.01prd14.SPA.bin]?
          Accessing
```

```
tftp://203.0.113.2//auto/tftp-ngio/test/c8000be-universalk9.17.03.01prd14.SPA.bin...
          %Error opening
tftp://203.0.113.2//auto/tftp-ngio/test/c8000be-universalk9.17.03.01prd14.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/c8000be-universalk9.17.03.01prd14.SPA.bin]?

          Destination filename [c8000be-universalk9.17.03.01prd14.SPA.bin]?
          Accessing
tftp://203.0.113.2//auto/tftp-ngio/test/c8000be-universalk9.17.03.01prd14.SPA.bin...
          Loading /auto/tftp-ngio/test/c8000be-universalk9.17.03.01prd14.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
c8000be-universalk9.17.03.01prd14.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:c8000be-universalk9.17.03.01prd14.SPA.bin
          Router(config)# config-reg 0x2102
          Router(config)# exit
          Router# show run | include boot
          boot-start-marker
          boot system flash bootflash:c8000be-universalk9.17.03.01prd14.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

An example to configure a device to boot the consolidated package via TFTP using the boot command.

```
Router#configure terminal
                     Enter configuration commands, one per line.  End with CNTL/Z.
                     Router(config)#boot system
tftp://10.81.116.4/auto/cebu-tftpboot/test/release/rommon/bin/test-17-3-2r
                     Router(config)#config-register 0x2102
                     Router(config)#exit
                     Router#
                     *Jul  7 01:43:52.098: %SYS-5-CONFIG_I: Configured from console by
console
                     Router#show run | include boot
                     boot-start-marker
                     boot system bootflash:c8000be-universalk9.17.03.01prd14.SPA.bin
                     boot system
tftp://10.81.116.4/auto/mcebu-tftpboot/test/release/rommon/bin/test-17-3-1r
                     boot-end-marker
                     license boot level network-essentials
                     diagnostic bootup level minimal
                     Router#copy running-config startup-config
                     Destination filename [startup-config]?
                     Building configuration...
                     [OK]
                     Router#reload
                     Proceed with reload? [confirm]

                     *Jul  7 01:55:28.639: %SYS-5-RELOAD:
                     Reload requested by console. Reload Reason: Reload Command.Jul  7
01:55:36.715: %PMAN-5-EXITACvp: Process manager is exiting: process exit with reload chassis
 code
                     Initializing Hardware ...

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

```
                        System Bootstrap, Version 1RU-20191104, DEVELOPMENT SOFTWARE
                        Copyright (c) 1994-2019  by cisco Systems, Inc.


                        Current image running: Boot ROM1

                        Last reset cause: LocalSoft
                        C8300-1N1S-6T platform with 8388608 Kbytes of main memory


                        ........
                        Located c8000be-universalk9.17.03.01prd14.SPA.bin

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

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

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

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

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

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


                        Package header rev 3 structure detected
                        IsoSize = 655712256
                        Calculating SHA-1 hash...Validate package: SHA-1 hash:
                        calculated DF67D179:DAB875C9:D61FB9E7:2E25B30B:48E86BFC
                        expected   DF67D179:DAB875C9:D61FB9E7:2E25B30B:48E86BFC
                        RSA Signed RELEASE Image Signature Verification Successful.
                        Image validated


                        RSA Signed RELEASE Image Signature Verification Successful.
                        Image validated
                        Jul  7 01:58:19.327: %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 [Amsterdam], c8000be Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.1prd8, RELEASE SOFTWARE (fc1)
                        Technical Support: http://www.cisco.com/techsupport
```

```
                        Copyright (c) 1986-2020 by Cisco Systems, Inc.
                        Compiled Tue 19-May-20 12:00 by mcpre


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


                        PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
                       LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE,

                        AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE
                        "SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL
                        ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF
YOU
                        ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

                        Your use of the Software is subject to the Cisco End User License
Agreement
                        (EULA) and any relevant supplemental terms (SEULA) found at

http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

                       You hereby acknowledge and agree that certain Software and/or features
 are
                        licensed for a particular term, that the license to such Software
and/or
                       features is valid only for the applicable term and that such Software
 and/or
                        features may be shut down or otherwise terminated by Cisco after
expiration
                        of the applicable license term (e.g., 90-day trial period). Cisco
reserves
                        the right to terminate any such Software feature electronically or
by any
                        other means available. While Cisco may provide alerts, it is your
sole
                       responsibility to monitor your usage of any such term Software feature
 to
                        ensure that your systems and networks are prepared for a shutdown of
 the
                        Software feature.

                        All TCP AO KDF Tests Pass
                        cisco C8300-1N1S-6T (1RU) processor with 3763047K/6147K bytes of
memory.
                        Processor board ID FDO2320A0CF
                        Router operating mode: Autonomous
                        6 Gigabit Ethernet interfaces
                        32768K bytes of non-volatile configuration memory.
                        8388608K bytes of physical memory.
                        7090175K bytes of flash memory at bootflash:.
                        28884992K bytes of M.2 USB at harddisk:.

                       Dspfarm profile 7 :: No resource, check voice card or dspfarm service
 is not configured
                        Press RETURN to get started!
                        Router>show version
                        Cisco IOS XE Software, Version 17.03.01prd8
                        Cisco IOS Software [Amsterdam], c8000be Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.1prd8, RELEASE SOFTWARE (fc1)
                        Technical Support: http://www.cisco.com/techsupport
                        Copyright (c) 1986-2020 by Cisco Systems, Inc.
                        Compiled Tue 19-May-20 12:00 by mcpre
```

```
                    Cisco IOS-XE software, Copyright (c) 2005-2020 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: (c)


                    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 Package License Information:

                    ------------------------------------------------------------------
                    Technology     Type         Technology-package Technology-package
                    Current            Next Reboot
                    ------------------------------------------------------------------
                    Smart License  Perpetual    network-essentials network-essentials
                    Smart License  Subscription None              None

                    The current crypto throughput level is 1000000 kbps


                    cisco C8300-1N1S-6T (1RU) processor with 3763047K/6147K bytes of
memory.
                    Processor board ID FDO2320A0CF
                    Router operating mode: Autonomous
```

```
6 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
7090175K bytes of flash memory at bootflash:.
28884992K bytes of M.2 USB at harddisk:.

Configuration register is 0x2102
```

Install the software using install commands

From Cisco IOS XE Cupertino 17.7.1a, Cisco Catalyst 8000 Edge platforms are shipped in install mode by default. Users can boot the platform, and upgrade or downgrade to Cisco IOS XE software versions using a set of **install** commands.

Restrictions

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

Install software using install commands

This 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.

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**.

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.
install activate	**install activate**	Activates the package added using the **install add** command. • Use the **show install summary** command to see which image is inactive. This image will get activated. • System reloads on executing this command. Confirm if you want to proceed with the activation. Use this command with the **prompt-level none** keyword to automatically ignore any confirmation prompts.

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

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

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

Table 11: List of show Commands

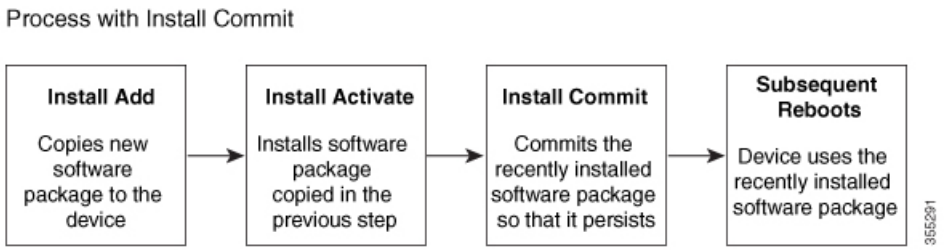
Command	Syntax	Purpose
show install log	**show install log**	Provides the history and details of all install operations that have been performed since the platform was booted.
show install package	**show install package** <*filename*>	Provides details about the .pkg/.bin file that is specified.
show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

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

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:

Figure 1: Process with install commit



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.

Boot 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 convert 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 **installadd filelocation:***filename* [**activate commit**]

Example:

```
Device#install add file
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin activate
 commit
```

Copies the software install package from a local or remote location (through FTP, HTTP, HTTPs, or TFTP) to the platform and extracts the individual components of the .package file into subpackages and packages.conf files. It also performs a validation and compatibility check for the platform and image versions, activates the package, and commits the package to make it persistent across reloads.

The platform reloads after this command is run.

Step 3 **exit**

Example:

```
Device#exit
```

Exits privileged EXEC mode and returns to user EXEC mode.

Platform is upgraded to new version.

Three-step install

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 **installadd filelocation:***filename*

Example:

```
Device#install add file
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
```

Copies the software install package from a remote location (through FTP, HTTP, HTTPs, or TFTP) to the platform, and extracts the individual components of the .package file into subpackages and packages.conf files.

Step 3 **showinstall 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 **installactivate** [**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 **installabort**

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 **installcommit**

Example:

```
Device#install commit
```

Commits the new package installation and makes the changes persistent over reloads.

Step 7 **installrollback tocommitted**

Example:

```
Device#install rollback to committed
```

(Optional) Rolls back the platform to the last committed state.

Step 8 **installremove** { **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 **showinstall 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.

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.

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 these 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 you issue the **install commit** command, the installation process terminates. The platform then 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 example for software installation using install commands

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:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
 activate commit
          install_add_activate_commit: START Thu Oct 28 21:57:21 UTC 2021

          System configuration has been modified.
          Press Yes(y) to save the configuration and proceed.
          Press No(n) for proceeding without saving the configuration.
          Press Quit(q) to exit, you may save configuration and re-enter the command.
[y/n/q]y
          Building configuration...

          [OK]Modified configuration has been saved

          *Oct 28 21:57:39.818: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted
private config file
         *Oct 28 21:57:39.925: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
 install one-shot
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bininstall_add_activate_commit:
 Adding PACKAGE
          install_add_activate_commit: Checking whether new add is allowed ....

          --- Starting Add ---
          Performing Add on Active/Standby
          [1] Add package(s) on R0
          [1] Finished Add on R0
          Checking status of Add on [R0]
          Add: Passed on [R0]
          Finished Add

          Image added. Version: 17.07.01.0.1515
          install_add_activate_commit: Activating PACKAGE
          Following packages shall be activated:

/bootflash/c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg


/bootflash/c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg


/bootflash/c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg


/bootflash/c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg


/bootflash/c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg


/bootflash/c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

```
/bootflash/c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

/bootflash/c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

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

          --- Starting Activate ---
          Performing Activate on Active/Standby

          *Oct 28 22:05:49.484: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [1] Activate package(s)
 on R0
          [1] Finished Activate on R0
          Checking status of Activate on [R0]
          Activate: Passed on [R0]
          Finished Activate

          --- Starting Commit ---
          Performing Commit on Active/Standby
          [1] Commit package(s) on R0

          Building configuration...
          [1] Finished Commit on R0
          Checking status of Commit on [R0]
          Commit: Passed on [R0]
          Finished Commit

          [OK]
          *Oct 28 22:06:55.375: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted
```

```
private config fileSend model notification for install_add_activate_commit before reload
          Install will reload the system now!
          SUCCESS: install_add_activate_commit  Thu Oct 28 22:07:22 UTC 2021

          Router#
          *Oct 28 22:07:22.661: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install one-shot PACKAGE
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.binOct
 28 22:07:26.864: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action
 requested

          □

          Press RETURN to get started!
```

This is an example of downgrading in install mode.

```
Router# install add file
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
          install_add: START Thu Oct 28 22:36:43 UTC 2021

         *Oct 28 22:36:44.526: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
 install add
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bininstall_add:
 Adding PACKAGE
          install_add: Checking whether new add is allowed ....

          --- Starting Add ---
          Performing Add on Active/Standby
          [1] Add package(s) on R0
          [1] Finished Add on R0
          Checking status of Add on [R0]
          Add: Passed on [R0]
          Finished Add

          Image added. Version: 17.07.01.0.1601
          SUCCESS: install_add  Thu Oct 28 22:40:25 UTC 2021

          Router#
          *Oct 28 22:40:25.971: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install add PACKAGE
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin

          Router# 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
          [0|install_op_boot(INFO, )]: cleanup_trap  remote_invocation 0 operation
install_op_boot .. 0 .. 0
          [1|display_install_log]: START Thu Oct 28 22:12:11 UTC 2021
          [2|install_add]: START Thu Oct 28 22:36:43 UTC 2021
          [2|install_add(INFO, )]: Set INSTALL_TYPE to PACKAGE
          [2|install_add(CONSOLE, )]: Adding PACKAGE
          [2|install_add(CONSOLE, )]: Checking whether new add is allowed ....
          [2|install_add(INFO, )]: check_add_op_allowed: Install type PACKAGE
          [remote|install_add]: START Thu Oct 28 22:37:12 UTC 2021
          [remote|install_add]: END SUCCESS  Thu Oct 28 22:40:10 UTC 2021
          [remote|install_add(INFO, )]: cleanup_trap  remote_invocation 1 operation
install_add .. 0 .. 0
          [2|install_add(INFO, )]: Remote output from R0
          [2|install_add(INFO, )]: install_add: START Thu Oct 28 22:37:12 UTC 2021
          Expanding image file:
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
          Verifying parameters
          Expanding superpackage
```

```
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
          ... parameters verified
          Validating package type
          ... package type validated
          Copying package files

c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
        c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
        c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

        c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          WARNING: A different version of provisioning file packages.conf already exists
in bootflash:
          WARNING: The provisioning file from the expanded bundle will be saved as
          WARNING: bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_0.conf
          ... package files copied
          SUCCESS: Finished expanding all-in-one software package.
          Image file expanded
          SUCCESS: install_add  Thu Oct 28 22:40:10 UTC 2021
          [2|install_add]: END SUCCESS  Thu Oct 28 22:40:25 UTC 2021
          [2|install_add(INFO, )]: cleanup_trap  remote_invocation 0 operation install_add
 .. 0 .. 0
          [3|COMP_CHECK]: START Thu Oct 28 22:40:26 UTC 2021
          [3|COMP_CHECK]: END FAILED exit(1)  Thu Oct 28 22:40:27 UTC 2021
          [3|COMP_CHECK(INFO, )]: cleanup_trap  remote_invocation 0 operation COMP_CHECK
.. 1 .. 1
          [4|install_activate]: START Thu Oct 28 22:42:53 UTC 2021
          [4|install_activate(INFO, require user prompt)]: install_cli
```

```
          [4|install_activate(CONSOLE, )]: Activating PACKAGE
          [4|install_activate(INFO, )]: Acquiring transaction lock...
          [4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
          [4|install_activate(INFO, )]: tmp_global_trans_lock:
/tmp/tmp_install_global_trans_lock
          [4|install_activate(INFO, )]: tmp lock does not exist:
/tmp/tmp_install_global_trans_lock
          [4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
          [4|install_activate(INFO, )]: tmp_global_trans_lock:
/tmp/tmp_install_global_trans_lock
          [4|install_activate(INFO, )]: local_trans_lock:
/bootflash/.installer/install_local_trans_lock
          [4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
          [4|install_activate(INFO, )]: validate_lock: lock_duration is 7200
          [4|install_activate(INFO, )]: install type stored in lock PACKAGE, install type
PACKAGE, install operation install_activate
          [4|install_activate(INFO, )]: lock duration: 7200
          [4|install_activate(INFO, )]: extend trans lock done.
/bootflash/.installer/install_global_trans_lock
          [4|install_activate(INFO, require user prompt)]: install_cli
          [4|install_activate( FATAL)]: Cannot proceed activate because of user input
          [4|install_activate(INFO, )]: cleanup_trap  remote_invocation 0 operation
install_activate .. 6 .. 0
          [5|install_add]: START Thu Oct 28 22:45:48 UTC 2021
          [5|install_add(INFO, )]: Set INSTALL_TYPE to PACKAGE
          [5|install_add(CONSOLE, )]: Adding PACKAGE
          [5|install_add(CONSOLE, )]: Checking whether new add is allowed ....
          [5|install_add(INFO, )]: check_add_op_allowed: Install type PACKAGE
          [5|install_add( FATAL)]: Super package already added. Add operation not allowed.
 install remove inactive can be used to discard added packages

          Router# install activate
          install_activate: START Thu Oct 28 23:57:57 UTC 2021
          install_activate: Activating PACKAGE

         *Oct 28 23:57:57.823: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
 install activateFollowing packages shall be activated:

/bootflash/c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


/bootflash/c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


/bootflash/c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


/bootflash/c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


/bootflash/c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


/bootflash/c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


/bootflash/c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
```

```
/bootflash/c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

/bootflash/c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg


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

          --- Starting Activate ---
          Performing Activate on Active/Standby

          *Oct 29 00:04:19.400: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [1] Activate package(s)
 on R0
          --- Starting list of software package changes ---
          Old files list:
          Modified
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

          Modified
c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

          Modified
c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

```
          Modified
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

          Modified
c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
          Modified
c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
         Modified c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

          New files list:
          Added
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

          Added
c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

          Added
c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

          Added
```

```
c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
          Added
c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
         Added c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

          Finished list of software package changes
          [1] Finished Activate on R0
          Checking status of Activate on [R0]
          Activate: Passed on [R0]
          Finished Activate

          Send model notification for install_activate before reload
          Install will reload the system now!
          SUCCESS: install_activate  Fri Oct 29 00:05:09 UTC 2021

          Router#
          *Oct 29 00:05:09.504: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install activate PACKAGEOct 29 00:05:14.494: %PMAN-5-EXITACTION: R0/0: pvp: Process
 manager is exiting: reload action requested

          Initializing Hardware ...

          Checking for PCIe device presence...done
          System integrity status: 0x610

          System Bootstrap, Version 17.3(4.1r), RELEASE SOFTWARE
          Copyright (c) 1994-2021 by cisco Systems, Inc.

          Current image running   : Boot ROM1
          Last reset cause        : LocalSoft
          C8300-2N2S-6T platform with 8388608 Kbytes of main memory

          □

          Press RETURN to get started!

          □

          Router# install commit
          install_commit: START Fri Oct 29 00:13:58 UTC 2021
          install_commit: Committing PACKAGE

          --- Starting Commit ---
          Performing Commit on Active/Standby

         *Oct 29 00:13:59.552: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
 install commit  [1] Commit package(s) on R0
          [1] Finished Commit on R0
          Checking status of Commit on [R0]
          Commit: Passed on [R0]
          Finished Commit

          SUCCESS: install_commit  Fri Oct 29 00:14:03 UTC 2021

          Router#
          *Oct 29 00:14:03.712: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install commit PACKAGE
```

This is an example of the three-step installation.

```
ROUTER# install activate file bootflash:c8000be-universalk9.17.06.01a.SPA.bin activate
commit

          install_add_activate_commit: START Fri Dec 10 18:07:17 GMT 2021
```

```
          *Dec 10 18:07:18.405 GMT: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine:
Started install one-shot
bootflash:c8000be-universalk9.17.06.01a.SPA.bininstall_add_activate_commit: Adding PACKAGE
          install_add_activate_commit: Checking whether new add is allowed ....

          --- Starting Add ---
          Performing Add on Active/Standby
          [1] Add package(s) on R0
          [1] Finished Add on R0
          Checking status of Add on [R0]
          Add: Passed on [R0]
          Finished Add

          Image added. Version: 17.06.01a.0.298
          install_add_activate_commit: Activating PACKAGE
          Following packages shall be activated:
          /bootflash/c8000be-rpboot.17.06.01a.SPA.pkg
          /bootflash/c8000be-mono-universalk9.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_sm_nim_adpt.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_sm_dsp_sp2700.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_sm_async.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_sm_1t3e3.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_sm_10g.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_prince.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_nim_xdsl.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_nim_ssd.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_nim_shdsl.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_nim_ge.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_nim_cwan.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_nim_bri_st_fw.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_nim_async.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_ngwic_t1e1.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_dsp_tilegx.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_dsp_sp2700.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_dsp_analogbri.17.06.01a.SPA.pkg
          /bootflash/c8000be-firmware_dreamliner.17.06.01a.SPA.pkg

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

          --- Starting Activate ---
          Performing Activate on Active/Standby
          [1] Activate package(s) on R0
          [1] Finished Activate on R0
          Checking status of Activate on [R0]
          Activate: Passed on [R0]
          Finished Activate

          --- Starting Commit ---
          Performing Commit on Active/Standby
          [1] Commit package(s) on R0
          Building configuration...

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

          [OK]
          *Dec 10 18:14:57.782 GMT: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted
 private config fileSend model notification for install_add_activate_commit before reload
          /usr/binos/conf/install_util.sh: line 164: /bootflash/.prst_sync/reload_info: No
 such file or directory
          /usr/binos/conf/install_util.sh: line 168: /bootflash/.prst_sync/reload_info: No
 such file or directory
```

```
          cat: /bootflash/.prst_sync/reload_info: No such file or directory
          Install will reload the system now!
          SUCCESS: install_add_activate_commit  Fri Dec 10 18:15:23 GMT 2021

          ROUTER#
         *Dec 10 18:15:23.955 GMT: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
 Completed install one-shot PACKAGE bootflash:c8000be-universalk9.17.06.01a.SPA.binDec 10
18:15:27.708: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action
requested

          Initializing Hardware ...

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

          System Bootstrap, Version 17.3(5r), RELEASE SOFTWARE
          Copyright (c) 1994-2021 by cisco Systems, Inc.

          Current image running: Boot ROM0

          Last reset cause: LocalSoft
          ROUTER platform with 8388608 Kbytes of main memory

          □

          Press RETURN to get started!

          □

          ROUTER#
          ROUTER# show version
          Cisco IOS XE Software, Version 17.06.01a
         Cisco IOS Software [Bengaluru], c8000be Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
 Version 17.6.1a, RELEASE SOFTWARE (fc2)
          Technical Support: http://www.cisco.com/techsupport
          Copyright (c) 1986-2021 by Cisco Systems, Inc.
          Compiled Sat 21-Aug-21 03:27 by mcpre

          Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc.
          All rights reserved.  Certain components of Cisco IOS-XE software are
          licensed under the GNU General Public License ("GPL") Version 2.0.  The
          software code licensed under GPL Version 2.0 is free software that comes
          with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
          GPL code under the terms of GPL Version 2.0.  For more details, see the
          documentation or "License Notice" file accompanying the IOS-XE software,
          or the applicable URL provided on the flyer accompanying the IOS-XE
          software.

          ROM: 17.3(5r)

          ROUTER uptime is 0 minutes
          Uptime for this control processor is 2 minutes
          System returned to ROM by LocalSoft
          System image file is "bootflash:packages.conf"
          Last reload reason: LocalSoft

          This product contains cryptographic features and is subject to United
          States and local country laws governing import, export, transfer and
          use. Delivery of Cisco cryptographic products does not imply
          third-party authority to import, export, distribute or use encryption.
          Importers, exporters, distributors and users are responsible for
          compliance with U.S. and local country laws. By using this product you
          agree to comply with applicable laws and regulations. If you are unable
```

```
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Technology Package License Information:

------------------------------------------------------------------
Technology     Type         Technology-package Technology-package
Current            Next Reboot
------------------------------------------------------------------
Smart License  Perpetual    None               None
Smart License  Subscription None               None

The current crypto throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco ROUTER (1RU) processor with 3747220K/6147K bytes of memory.
Processor board ID FDO2521M27S
Router operating mode: Autonomous
5 Gigabit Ethernet interfaces
2 2.5 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
7573503K bytes of flash memory at bootflash:.
1875361792K bytes of NVMe SSD at harddisk:.
16789568K bytes of USB flash at usb0:.

Configuration register is 0x2102
```

This is an example of terminating a software installation.

```
Router# install abort
install_abort: START Fri Oct 29 02:42:51 UTC 2021

This install abort would require a reload. Do you want to proceed? [y/n]
*Oct 29 02:42:52.789: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install aborty
--- Starting Abort ---
Performing Abort on Active/Standby

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

Send model notification for install_abort before reload
Install will reload the system now!
SUCCESS: install_abort  Fri Oct 29 02:44:47 UTC 2021

Router#
*Oct 29 02:44:47.866: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install abort PACKAGEOct 29 02:44:51.577: %PMAN-5-EXITACTION: R0/0: pvp: Process
 manager is exiting: reload action requested
```

```
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610

System Bootstrap, Version 17.3(4.1r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running   : Boot ROM1
Last reset cause        : LocalSoft
C8300-2N2S-6T platform with 8388608 Kbytes of main memory

□

Press RETURN to get started!

□
```

These are sample outputs for show commands:

```
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

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    17.07.01.0.1515

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

Device#show install
packagebootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin

            Package:
c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
            Size: 831447859
            Timestamp: 2021-10-23 17:08:14 UTC
            Canonical path:
/bootflash/c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin


            Raw disk-file SHA1sum:
            5c4e7617a6c71ffbcc73dcd034ab58bf76605e3f
            Header size:     1192 bytes
            Package type:    30000
            Package flags:   0
            Header version:  3

            Internal package information:
            Name: rp_super
            BuildTime: 2021-10-21_13.00
            ReleaseDate: 2021-10-21_03.11
            BootArchitecture: i686
            RouteProcessor: radium
            Platform: C8000BE
            User: mcpre
            PackageName: universalk9
```

```
            Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
            CardTypes:

            Package is bootable from media and tftp.
            Package contents:

            Package:
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
            Size: 2966620
            Timestamp: 2021-10-21 20:10:44 UTC

            Raw disk-file SHA1sum:
            501d59d5f152ca00084a0da8217bf6f6b95dddb1
            Header size:     1116 bytes
            Package type:    40000
            Package flags:   0
            Header version:  3

            Internal package information:
            Name: firmware_nim_ge
            BuildTime: 2021-10-21_13.00
            ReleaseDate: 2021-10-21_03.11
            BootArchitecture: none
            RouteProcessor: radium
            Platform: C8000BE
            User: mcpre
            PackageName: firmware_nim_ge
            Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
            CardTypes:

            Package is not bootable.
            Package:
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
            Size: 10204252
            Timestamp: 2021-10-21 20:10:43 UTC

            Raw disk-file SHA1sum:
            a57bed4ddecfd08af3b456f69d11aaeb962865ea
            Header size:     1116 bytes
            Package type:    40000
            Package flags:   0
            Header version:  3

            Internal package information:
            Name: firmware_prince
            BuildTime: 2021-10-21_13.00
            ReleaseDate: 2021-10-21_03.11
            BootArchitecture: none
            RouteProcessor: radium
            Platform: C8000BE
            User: mcpre
            PackageName: firmware_prince
            Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
            CardTypes:

            Package is not bootable.

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    17.07.01.0.1515
```

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

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    17.07.01.0.1515

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

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

To 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.

Upgrade firmware on NIMs

To upgrade the firmware on a Network Interface Module (NIM), perform these steps:

Before you begin

When you boot the device in packages.conf mode with the Cisco IOS XE image (super package) during the installation period, you can upgrade or downgrade the firmware without reloading the device. You need to follow the steps described in Installing a Firmware Subpackage section before proceeding with the firmware upgrade.

If you do not boot the device in packages.conf mode with the Cisco IOS XE image, you need to follow the below prerequisites before proceeding with the firmware upgrade:

- Copy the firmware subpackage (NIM firmware) into bootflash:/mydir.
- Send a request to the platform software package expand file boot flash:/mydir/<IOS-XE image> to expand the super package.
- Reload the hardware module subslot to boot the module with the new firmware.
- Verify that the module is booted up with the new firmware using the s**how platform software subslot x/y module firmware** command.

Procedure

Step 1 copy Cisco IOS XE image into bootflash: **mydir** .

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 2 **requestplatformsoftwarepackageexpandfile***bootflash:/mydir /<IOS-XE image* to expand super package.

Example:

```
Router#

 request platform software package expand file
bootflash:/mydir/c8000be-universalk9.03.14.00.S.155-1.S-std.SPA.bin
```

Expands the platform software package to super package.

Step 3 **reload** .

Example:

```
Router#reload
rommon >
```

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

Step 4 **bootbootflash:mydir//packages.conf** .

Example:

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

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

Step 5 **copy** NIM firmware subpackage to the folder **bootflash:mydir/** .

Example:

```
Router#copy bootflash:c8000be-firmware_nim_xdsl.2020-07-01_11.05_39n.SSA.pkg
bootflash:mydir/
```

Copies the NIM firmware subpackage into bootflash:mydir.

Step 6 **requestplatformsoftwarepackageinstall***rp 0 file bootflash:/mydir/<firmware subpackage>* .

Example:

```
Router#equest platform software package install rp 0 file
bootflash:mydir/c8000be-firmware_nim_xdsl.2020-07-01_11.05_39n.SSA.pkg
```

Installs the software package.

Step 7 **hw-module subslot x/yreload** to boot the module with the new firmware.

Example:

```
Router#hw-module subslot 0/2 reload
```

Reloads the hardware module subslot and boots the module with the new firmware.

Step 8 **showplatformsoftwaresubslot 0/2 module firmware** to verify that the module is booted up with the new firmware.

Example:

```
Router#show platform software subslot 0/2 module firmware
Pe
```

Displays the version of the newly installed firmware.

Firmware is upgraded on NIMs.

Examples: upgrade the firmware on NIMs

To perform firmware upgrade on NIMs

Examples

This example shows how to perform firmware upgrade in a device module:

```
            Router
          mkdir bootflash:mydir
Create directory filename [mydir]?
```

```
Created dir bootflash:/mydir
Router#c
Router#copy bootflash:c8000be-universalk9.17.03.01prd14.S-std.SPA.bin bootflash:mydir/
Destination filename [mydir/c8000be-universalk9.17.03.01prd14.S-std.SPA.bin]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCC
696368193 bytes copied in 478.600 secs (1455011 bytes/sec)
Router#
Router#
Router#dir bootflash:mydir
Directory of bootflash:/mydir/
632738  -rw-        425288648  Dec 12 2014 09:16:42 +00:00
c8000be-universalk9.17.03.01prd14.S-std.SPA.bin
7451738112 bytes total (474025984 bytes free)
Router#
Router#
           request platform software package
expand file bootflash:/mydir/c8000be-universalk9.17.03.01prd14.S-std.SPA.bin.S-std.SPA.bin
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.
Router#
           reload
Proceed with reload? [confirm]
Proceed with reload? [confirm]
*Jul  8 11:48:30.917 PDT: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
 Command.
*Jul  8 11:48:32.768 PDT: %IOSXE_INFRA-3-RELOAD_INFO_SAVE_FAIL: Unable to save reload
information: 23: Invalid argument.
Jul  8 11:48:38.652: %PMAN-TACTION: R0/0: pvp: Process manager is exiting: process exit
with reload chassis code
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
C8300-1N1S-4T2X platform with 8388608 Kbytes of main memory
rommon 1
           boot bootflash:mydir/packages.conf
File size is 0x000028f1
Located mydir/packages.conf
Image size
10481 inode num 632741, bks cnt 3 blk size 8*512
#
File size is 0x150ae3cc
Located mydir/c8000be-universalk9.17.03.01prd14.S-std.SPA.pkg
Image size 353035212 inode num 356929, bks cnt 86191 blk size 8*512
###################################################################
######################################################################
Boot image size = 353035212 (0x150ae3cc) bytes
Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
  calculated 8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3
  expected   8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3
RSA Signed RELEASE Image Signature Verification Successful.
Package Load Test Latency : 3799 msec
```

```
Image validated
Dec 12 09:28:50.338 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 61864 kB] - Please clean up files on bootflash.
            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 [Amsterdam], c8000be Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version
 17.3.1prd14, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Tue 16-Jun-20 23:44 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco c8000be1-X/K9 (2RU) processor with 1681388K/6147K bytes of memory.
Processor board ID FTX1736AJUT
2 Ethernet interfaces
4 Gigabit Ethernet interfaces
2 ATM interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of flash memory at bootflash:.
Press RETURN to get started!
*Dec 12 09:28:58.922:
%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = esg Next reboot level = appxk9 and License = appxk9
*Dec 12 09:28:58.943:
%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = esg Next reboot level = ipbasek9 and License = ipbasek9
*Dec 12 09:28:58.981:
%Cat_THROUGHPUT-6-LEVEL: Throughput level has been set to 1000000 kbps
*Dec 12 09:29:13.302: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*Dec 12 09:28:51.438: %CMRP-3-PFU_MISSING:cmand:  The platform does not detect a power
supply in slot 1
*Dec 12 09:29:01.256: %CMLIB-6-THROUGHPUT_VALUE:cmand:  Throughput license found, throughput
```

```
 set to 1000000 kbps
*Dec 12 09:29:03.223: %CPPHA-7-START:cpp_ha:  CPP 0 preparing ucode
*Dec 12 09:29:03.238: %CPPHA-7-START:cpp_ha:  CPP 0 startup init
*Dec 12 09:29:11.335: %CPPHA-7-START:cpp_ha:  CPP 0 running init
*Dec 12 09:29:11.645: %CPPHA-7-READY:cpp_ha:  CPP 0 loading and initialization complete
*Dec 12 09:29:11.711: %IOSXE-6-PLATFORM:cpp_cp:
Process CPP_PFILTER_EA_EVENT__API_CALL__REGISTER
*Dec 12 09:29:16.280:
%IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO:
Management vrf Mgmt-intf created with ID 1, ipv4 table-id 0x1, ipv6 table-id 0x1E000001
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state to up
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state to up
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to down
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state to up
*Dec 12 09:29:17.521: %SYS-5-LOG_CONFIG_CHANGE: Buffer logging disabled
*Dec 12 09:29:18.867: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 12 09:29:18.870:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled
*Dec 12 09:29:18.870:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*Dec 12 09:29:18.871:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/2, interfaces disabled
*Dec 12 09:29:18.873:
%SPA_OIR-6-OFFLINECARD: SPA (c8000be-X-4x1GE) offline in subslot 0/0
*Dec 12 09:29:18.874: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VA-B) offline in subslot 0/1
*Dec 12 09:29:18.874: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
*Dec 12 09:29:18.876: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F0
*Dec 12 09:29:18.876: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0
*Dec 12 09:29:18.882: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0
*Dec 12 09:29:18.884: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/1
*Dec 12 09:29:18.884: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/2
*Dec 12 09:29:18.935: %SYS-5-RESTART: System restarted --
Cisco IOS Software, c8000be Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(1)S,
RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Nov-14 18:28 by mcpre
*Dec 12 09:29:18.895: %SPA-3-ENVMON_NOT_MONITORED:iomd:  Environmental monitoring
is not enabled for c8000be-X-4x1GE[0/0]
*Dec 12 09:29:19.878: %LINK-5-CHANGED: Interface GigabitEthernet0,
changed state to administratively down
*Dec 12 09:29:22.419: %SPA_OIR-6-ONLINECARD: SPA (c8000be-X-4x1GE) online in subslot 0/0
*Dec 12 09:29:22.610: %SYS-6-BOOTTIME: Time taken to reboot after reload =  194 seconds
*Dec 12 09:29:24.354: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to down
*Dec 12 09:29:24.415: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/2,
changed state to down
*Dec 12 09:29:24.417: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/3,
changed state to down
*Dec 12 09:29:30.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to up
*Dec 12 09:29:30.925: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/2,
changed state to up
*Dec 12 09:29:30.936: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/3,
changed state to up
*Dec 12 09:29:31.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
*Dec 12 09:29:31.930: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0/2, changed state to up
*Dec 12 09:29:31.936: %LINEPROTO-5-UPDOWN: Line protocol on
```

```
Interface GigabitEthernet0/0/3, changed state to up
*Dec 12 09:29:34.147: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 12 09:30:29.152: %SPA_OIR-6-ONLINECARD: SPA (NIM-VA-B) online in subslot 0/1
*Dec 12 09:30:29.470: %SPA_OIR-6-ONLINECARD: SPA (NIM-VAB-A) online in subslot 0/2
*Dec 12 09:30:31.152: %LINK-3-UPDOWN: Interface Ethernet0/1/0, changed state to down
*Dec 12 09:30:31.152: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to down
*Dec 12 09:30:31.470: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to down
*Dec 12 09:30:31.470: %LINK-3-UPDOWN: Interface ATM0/2/0, changed state to down
*Dec 12 09:31:03.074: %CONTROLLER-5-UPDOWN: Controller VDSL 0/2/0, changed state to up
*Dec 12 09:31:05.075: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to up
*Dec 12 09:31:06.076: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2/0,
changed state to up
*Dec 12 09:31:12.559: %CONTROLLER-5-UPDOWN: Controller VDSL 0/1/0, changed state to up
*Dec 12 09:31:20.188: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to up
*Dec 12 09:31:21.188: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/1/0,
changed state to up
Router>
Router>en
Password:
Router#
Router#show controller vdsl 0/2/0
Controller VDSL 0/2/0 is UP
Daemon Status:        UP
         XTU-R (DS)        XTU-C (US)
Chip Vendor ID:        'BDCM'             'BDCM'
Chip Vendor Specific:   0x0000             0xA41B
Chip Vendor Country:    0xB500             0xB500
Modem Vendor ID:    'CSCO'             '    '
Modem Vendor Specific:  0x4602             0x0000
Modem Vendor Country:   0xB500             0x0000
Serial Number Far:
Modem Version Near:     15.5(1)S
Modem Version Far:      0xa41b
Modem Status(L1):    TC Sync (Showtime!)
DSL Config Mode:    VDSL2
Trained Mode(L1):    G.993.2 (VDSL2) Profile 30a
TC Mode:        PTM
Selftest Result:    0x00
DELT configuration:    disabled
DELT state:        not running
Failed full inits:    0
Short inits:        0
Failed short inits:    0
Modem FW  Version:    4.14L.04
Modem PHY Version:    A2pv6F039h.d24o_rc1
Line 1:
         XTU-R (DS)        XTU-C (US)
Trellis:         ON             ON
SRA:              disabled         disabled
SRA count:          0             0
Bit swap:          enabled         enabled
Bit swap count:         9             0
Profile 30a:          enabled
Line Attenuation:      3.5 dB          0.0 dB
Signal Attenuation:      0.0 dB          0.0 dB
Noise Margin:         30.9 dB        12.4 dB
Attainable Rate:    200000 kbits/s         121186 kbits/s
Actual Power:        13.3 dBm         7.2 dBm
Per Band Status:           D1     D2     D3     U0     U1     U2     U3
Line Attenuation(dB):   0.9    1.5    5.5    N/A    0.1    0.9    3.8
Signal Attenuation(dB): 0.8    1.5    5.5    N/A    0.0    0.2    3.2
Noise Margin(dB):       31.1    31.0    30.9    N/A    12.3    12.4    12.5
Total FECC:        0             0
Total ES:        0             0
```

```
Total SES:        0             0
Total LOSS:        0             0
Total UAS:        51             51
Total LPRS:        0             0
Total LOFS:        0             0
Total LOLS:        0             0
        DS Channel1      DS Channel0    US Channel1      US Channel0
Speed (kbps):           NA          100014        NA          100014
SRA Previous Speed:      NA               0        NA               0
Previous Speed:          NA               0        NA               0
Reed-Solomon EC:      NA               0        NA               0
CRC Errors:          NA               0        NA               0
Header Errors:          NA               0        NA               0
Interleave (ms):      NA            9.00        NA            0.00
Actual INP:          NA            4.00        NA            0.00
Training Log :    Stopped
Training Log Filename :    flash:vdsllog.bin
Router#
Router#
Router#
           copy bootflash:c8000be-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
bootflash:mydir/
Destination filename [mydir/c8000be-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
6640604 bytes copied in 1.365 secs (4864911 bytes/sec)
Router#
Router#
           request platform software package install rp 0 file
bootflash:mydir/c8000be-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
Found c8000be-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
--- Starting ISSU compatiblity verficiation ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatiblity verficiation
--- Starting impact testing ---
Checking operational impact of change
Finished impact testing
--- Starting list of software package changes ---
Old files list:
```

```
Removed c8000be-firmware_nim_xdsl.03.14.00.S.155-1.S-std.SPA.pkg
New files list:
Added c8000be-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
Finished list of software package changes
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
--- Starting analysis of software changes ---
Finished analysis of software changes
--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
Finding latest command set
Finding latest command shortlist lookup file
Finding latest command shortlist file
Assembling CLI output libraries
Assembling CLI input libraries
Skipping soft links for firmware upgrade
Skipping soft links for firmware upgrade
Assembling Dynamic configuration files
Applying interim IPC and database definitions
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19
/release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
Replacing running software
Replacing CLI software
Restarting software
Applying final IPC and database definitions
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
Generating software version information
Notifying running software of updates
Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
Finished update running software
SUCCESS: Finished installing software.
Router#
Router#show platform software subslot 0/2 module firmware
Avg Load info
-----------------------------------------
1.83 1.78 1.44 3/45 607
Kernel distribution info
-----------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2
(Buildroot 2011.11) ) #3 SMP PREEMPT Fri Nov 7 09:26:19 IST 2014
Module firmware versions
-----------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039h.d24o_rc1
Boot Loader: Secondry
-----------------------------------------
Version: 1.1
Modem Up time
-----------------------------------------
```

```
0D 0H 25M 38S
Router#
Router#
           hw-module subslot 0/2 reload
Proceed with reload of module? [confirm]
Router#
*Dec 12 09:55:59.645: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-VAB-A)
reloaded on subslot 0/2
*Dec 12 09:55:59.646: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
*Dec 12 09:55:59.647: %CONTROLLER-5-UPDOWN: Controller VDSL 0/2/0, changed state to down
*Dec 12 09:57:22.514: new extended attributes received from iomd(slot 0 bay 2 board 0)
*Dec 12 09:57:22.514: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-VAB-A)
reloaded on subslot 0/2
*Dec 12 09:57:22.515: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
Router#
Router#
*Dec 12 09:58:35.471: %SPA_OIR-6-ONLINECARD: SPA (NIM-VAB-A) online in subslot 0/2
*Dec 12 09:58:37.470: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to down
*Dec 12 09:58:37.470: %LINK-3-UPDOWN: Interface ATM0/2/0, changed state to down
Router#
Router#
           show platform software subslot 0/2 module firmware
Avg Load info
-----------------------------------------
0.84 0.23 0.08 1/45 598
Kernel distribution info
-----------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2 (Buildroot 2011.11) )
#6 SMP PREEMPT Mon Nov 17 10:51:41 IST 2014
Module firmware versions
-----------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039n.d24o_rc1
Boot Loader: Secondry
-----------------------------------------
Version: 1.1
Modem Up time
-----------------------------------------
0D 0H 0M 42S
Router#
```

Configure no service password-recovery

The Cisco IOS password recovery procedure allows you to gain access to ROMMON mode using the console and the Break key during system startup and reload. When the device software is loaded from ROMMON mode, the system updates the configuration with the new password.

The password recovery procedure allows anyone with console access to access the device and its network.

The No Service Password-Recovery feature prevents unauthorized users from using the service password-recovery procedure to access the device and network.

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

How to enable no service password-recovery

To enable no service password-recovery.

You can enable the No Service Password-Recovery in these 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.

Before you begin, make sure this feature is disabled prior to changing the device, including configurations, modules, software versions, or ROMMON versions, regardless of the significance.

Enable the configuration register boot bit to load the startup configuration by setting bit-8 to 0. To ignore the break key in Cisco IOS XE, set bit-6 to 0. Set the lowest four bits (3-0) to a value from 0x2 to 0xF to auto boot a Cisco IOS XE image. 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
C8300-1N1S-4T2X platform with 8388608 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 c8000be-universalk9.BLD_V153_3_S_XE310_THROTTLE_LATEST_20130623_234109.SSA.bin

Image size 395545216 inode num 26, bks cnt 96569 blk size 8*512
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 17.3(1r), RELEASE SOFTWARE
Copyright (c) 1994-2020  by cisco Systems, Inc.


Current image running: Boot ROM0

Last reset cause: LocalSoft
```

```
C8300-1N1S-4T2X platform with 8388608 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 c8000be-universalk9.BLD_V153_3_S_XE310_THROTTLE_LATEST_20130623_234109.SSA.bin

Image size 395545216 inode num 26, bks cnt 96569 blk size 8*512

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

Configuration Examples for No Service Password-Recovery

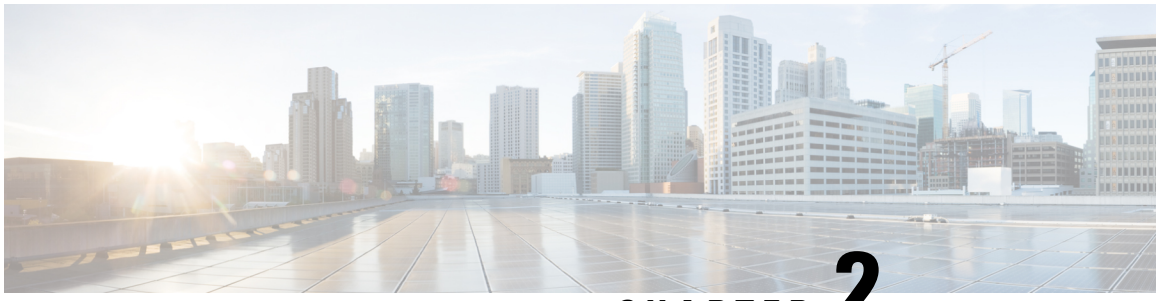
The example shows how to obtain the configuration register setting (which is set to autoboot), disable password recovery capability, and then verify that the configuration persists through a system reload:

```
Router# show version

Cisco Internetwork Operating System Software

IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)

TAC Support: http://www.cisco.com/tac

Copyright (c) 1986-2004 by Cisco Systems, Inc.

Compiled Wed 05-Mar-04 10:16 by xxx

Image text-base: 0x60008954, data-base: 0x61964000

ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)

...

125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).

8192K bytes of Flash internal SIMM (Sector size 256K).

Configuration register is 0x2102

Router# configure terminal

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)# exit

Router#

Router# reload

Proceed with reload? [confirm] yes

00:01:54: %SYS-5-RELOAD: Reload requested

System Bootstrap, Version 12.3...

Copyright (c) 1994-2004 by cisco Systems, Inc.

C7400 platform with 262144 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

...
```

This 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:

Do not execute this command without another plan for password recovery.

Are you sure you want to continue? [yes]: yes

..
```



CHAPTER 2

Device Management

Manage 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 these sections:

Use 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** .

Configure LAN Settings

LAN settings are configured for network devices primarily to manage and control the local network environment effectively. This process provides details on how to configure LAN settings for a device.

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** .

Configure Primary WAN Settings

The purpose of configuring WAN (Wide Area Network) settings on network devices is to establish and manage the connection between a local network and external networks.

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** .

Configure Secondary WAN Settings

The purpose of configuring secondary WAN settings on network devices is to provide an additional WAN connection that can serve as a backup or load-sharing link to the primary WAN. This secondary WAN connection enhances network reliability and availability by allowing failover in case the primary WAN link fails or experiences issues.

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 Secondary WAN Settings

The purpose of configuring secondary WAN settings on network devices is to provide an additional WAN connection that can serve as a backup or load-sharing link to the primary WAN. This secondary WAN connection enhances network reliability and availability by allowing failover in case the primary WAN link fails or experiences issues.

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** .

Using Web User Interface for day one setup

The purpose of the web user interface (Web UI) for devices is to provide an embedded, graphical user interface that simplifies device management by allowing users to provision, configure, monitor, and troubleshoot the device without requiring command-line interface (CLI) expertise. It enhances the user experience by offering an intuitive, GUI-based tool to build configurations and manage the device efficiently.

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.

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

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

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

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

Step 5 Click **Log In** .

Monitor and Troubleshoot Device Plug and Play (PnP) Onboarding using WebUI

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

- 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.

Procedure

Step 1 Enter the controller mode in WebUI

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.

Step 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.

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

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.

Step 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.

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

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

Step 6 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 Catalyst SD-WAN Manager. This file must contain details such as the vBond number, UUID, WAN interface, root CA and configuration.

Step 7 Click **Upload** .

Step 8 After your file is successfully uploaded, click **Submit.**

Step 9 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** .

Slot and subslot configuration

Best practice for multiple-rate SFP usage

- When using multiple-rate SFPs on the same interface (for example, 1G SFP or 10G SFP+ on a 10G port), verify compatibility with your platform.
- Ensure all member interfaces in a port-channel operate at the same speed and duplex.
- Use duplex interfaces of the same speed as member interfaces when configuring a port-channel.
- For more information about supported interfaces, see the corresponding data sheets.

Configure Gigabit Ethernet interfaces

This section outlines the process for configuring 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
```

Enter global configuration mode.

Step 3 **interface GigabitEthernet** *slot/subslot/port*

Example:

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

Configure a GigabitEthernet interface.

- **GigabitEthernet**—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
```

Assign 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
```

Select the negotiation mode.

- **auto**—Performs link autonegotiation.

Step 6 **end**

Example:

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

End the current configuration session and return to privileged EXEC mode.

The specified Gigabit Ethernet interface is now configured with the selected IP settings and link negotiation.

Interface configuration commands

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

Note Several platforms, NIMs, and SM cards support configuring multiple-rate SFPs on the same interface, such as 1-gigabit SFP or 10-gigabit SFP+ on a 10-gigabit port.

In port-channel bundles, all member interfaces should operate at the same speed and duplex settings. Refer to the corresponding datasheets for information on supported SFP rates by platform or interface.

```
Router# show running-config interface gigabitEthernet 0/0/0
Building configuration...
Current configuration : 71 bytes
!
interface gigabitEthernet0/0/0
no ip address
negotiation auto
end

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitEthernet 0/0/0
```

Commands for displaying interface summaries

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

The following command displays a list of all interfaces with traffic statistics and queue information.

```
Router# show platform software interface summary
  Interface                IHQ  IQD  OHQ  OQD  RXBS  RXPS  TXBS  TXPS  TRTL
-------------------------------------------------------------------------------
* GigabitEthernet0/0/0       0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/1       0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/2       0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/3       0    0    0    0     0     0     0     0     0
* Te0/0/4                    0    0    0    0     0     0     0     0     0
* Te0/0/5                    0    0    0    0     0      0    0     0     0
```

The following command provides a summarized view of interface states and key counters.

```
Router# show interfaces summary
   *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

Interface             IHQ  IQD    OHQ    OQD    RXBS    RXPS    TXBS    TXPS    TRTL
------------------------------------------------------------------------------------

* GigabitEthernet0/0/0 0    0      0      0      0       0       0       0       0
* GigabitEthernet0/0/1 0    0      0      0      0       0       0       0       0
* GigabitEthernet0/0/2 0    0      0      0      0       0       0       0       0
* GigabitEthernet0/0/3 0    0      0      0      0       0       0       0       0
* Te0/0/4              0    0      0      0      0       0       0       0       0
* Te0/0/5              0    0      0      0      0       0       0       0       0
```

The following command displays processor, memory, and CPU utilization for router platform components

```
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
```

Viewing information about an interface: Example

This example demonstrates how to display a brief summary of an interface's IP information and status, as well as the virtual interface bundle information, by using the **show ip interface brief** command.

```
Router# show ip interface brief
GigabitEthernet0/0/0   10.10.3.1       YES NVRAM  up         up
GigabitEthernet0/0/1   192.0.5.2       YES NVRAM  up         up
GigabitEthernet0/0/2   192.0.2.5       YES NVRAM  down       down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down       down
Te0/0/4                unassigned      YES NVRAM  down       down
Te0/0/5                10.20.4.8       YES NVRAM  down       down
Te0/1/0                unassigned      YES NVRAM  down       down
```

Cisco Service module and network interface modules

The router supports Cisco Services modules and Cisco network interface modules. The modules are inserted into the router using an adapter, or carrier card, into various slots. For more information, see the documents:

- Hardware Installation Guide for the Cisco Catalyst 8300 Series Edge Platform.
- Hardware Installation Guide for Cisco Catalyst 8200 Series Edge Platforms

Cisco service modules and network interface modules

The module management facility is an integrated feature in Cisco routers that centralizes the configuration, management, and control of various supported modules. The key points are:

- The router uses a built-in module management facility to configure, manage, and monitor all supported Cisco Service Modules, Network Interface Modules, and Pluggable Interface Modules, providing a unified approach regardless of module type or application.

- All Cisco Enhanced Service and Network Interface Modules communicate with the host router using standard IP protocols, ensuring interoperability and consistent management.
- Cisco IOS software utilizes alien data path integration to efficiently switch data between the different modules and the host router.

Supported modules

For information about the interfaces and modules supported by the Cisco Catalyst 8000 Edge Platform, see the Hardware Installation Guide for Cisco Catalyst 8000 Series Edge Platform.

Network interface and enhanced service modules

For more information about the supported Network Interface Modules and Service Modules, refer to the Cisco Catalyst 8300 Series Edge Platforms datasheet.

Module firmware process

Module firmware refers to the specialized software that must be loaded onto a router's service module to enable its intended functionality. The process involves the following steps:

- The service module connects to the router's Route Processor using the internal eth0 interface to initiate the firmware download process.
- The module acquires an IP address through BOOTP, which also supplies the address of the TFTP server from which the firmware image is downloaded.
- When the firmware image is loaded and the module is booted, DHCP assigns an IP address for the running image, so the module can operate within the network.

SM and NIM support for Cisco Catalyst 8200 and 8300 platforms

Note Cisco Catalyst 8200 Series Edge Platforms do not support service modules.

For procedures to install or remove NIMs and SMs, refer to the "Installing and Removing NIMs and SMs" in the Hardware Installation Guide for Cisco Catalyst 8300 Edge Platform and Hardware Installation Guide for Cisco Catalyst 8200 Series Edge Platforms.

Console and telnet connections

Console and telnet (along with Secure Shell, SSH) connections are network access methods used to establish communication with a host router. These methods enable administrators to remotely or locally access the router's CLI to manage and configure network modules.

- Connection method: Access is initiated by connecting to the host router either locally via the console port or remotely via telnet or SSH. These methods provide the initial network access channel to the router.
- Interface configuration: After establishing the connection to the router, an IP address must be configured on the Gigabit Ethernet interface that connects to the module. This step ensures proper network communication between the router and the module.

- Session establishment: Once the interface is configured, a session to the specific module is opened using the **hw-module session** *slot/subslot* command in privileged EXEC mode on the router. This command creates a direct management session to the module, allowing configuration and monitoring.

Examples

Use the following 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 capabilities

The router supports online insertion and removal of Cisco Enhanced Services Modules and Cisco Network Interface Modules.

Online module removals

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.

Module deactivation

Module deactivation is a process recommended before physically removing a module from a router to ensure a graceful shutdown and avoid potential issues. It involves stopping the module and its interfaces in a controlled manner. The key points of module deactivation are:

- Use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode to perform a graceful deactivation.
- When deactivating a module with this command, it is not necessary to manually shut down each interface. The command automatically deactivates all interfaces associated with the module
- Prepares the module for an Online Insertion and Removal procedure.

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.

Example

The following 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.

Deactivate a module and its interfaces in command modes

Use this task to safely shut down hardware modules in a router through either global configuration or EXEC mode, depending on your operational needs.

To deactivate a module and its interfaces, follow these steps:

Before you begin

Ensure you have determined the slot and subslot numbers for the target module.

Procedure

Step 1 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.

Step 2 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.

Step 3 To deactivate a module and all of its interfaces before removing the module, use one of the following commands in global configuration mode.

Step 4 **hw-module subslot** *slot*/*subslot* **shutdown unpowered**

Example:

```
Router# 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.

Step 5 **hw-module subslot** *slot*/*subslot* [**reload** | **stop** | **start**]

Example:

```
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.

The selected module and its interfaces are powered off and removed from the router configuration as specified by the chosen command and mode. The module will not boot until reactivated (if shutdown unpowered was used).

Deactivate and reactivate the SSD/HDD Carrier Card NIM

Perform these steps when you need to reseat, replace, or troubleshoot an SSD/HDD Carrier Card NIM in supported Cisco hardware.

Follow these steps to deactivate and reactivate an SSD/HDD Carrier Card NIM:

Before you begin

Ensure an SSD or HDD is installed in the Carrier Card NIM.

Only one Carrier Card NIM (SSD or HDD) is supported per bay. Installing another may cause file system corruption or module shutdown.

Deactivation may result in data loss; back up important data before proceeding.

Procedure

Step 1 **virtual-service** *name*

Example:

```
Router(config)# virtual-service my-kwaas-instance
```

Identifies the kWAAS service (by name), supported on your router, in preparation for the router to be shut down by the **no activate** command. We recommend that you use this command before reseating or replacing an SSD or HDD.

Step 2 **no activate**

Example:

```
Router(config-virt-serv)# no activate
```

Shuts down the kWAAS instance on your router. kWAAS services remain installed. The service will have to be reactivated after the HDD/SSD NIM (module) is restarted.

Step 3 **hw-module subslot** *slot*/*subslot* [**reload** | **stop** | **start**]

Example:

```
Router# hw-module subslot 0/2 stop
Proceed with stop of module? [confirm]
Router#
*Mar 6 15:13:23.997: %SPA_OIR-6-OFFLINECARD: SPA (NIM-SSD) offline in subslot 0/2
```

Deactivates or reactivates the module in the specified slot and subslot.

- *slot*—The chassis slot number where the module is installed.
- *subslot*—The subslot number of the chassis where the module is installed.
- **reload**—Deactivates and reactivates (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 IOMd processes.

Step 4 Wait for the EN (Enable) LED to turn off, and then remove the SSD/HDD Carrier Card NIM.

The SSD/HDD Carrier Card NIM is safely deactivated and can be physically removed or replaced, then reactivated for continued operation.

Module reactivation

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 the following commands (in privileged EXEC mode):

- **hw-module subslot***slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

Verify deactivation and activation of a module

This section outlines whether a module has been successfully deactivated or activated on the system.

Before you begin

Deactivating a module also deactivates its interfaces. As a result, these interfaces will not appear in the output of the **show interface** command.

Procedure

Step 1 Enter the **show hw-module subslot all oir** command in privileged EXEC mode to display the current operational status of all modules.

Example:

In the output, check the "Operational Status" field for the module of interest. If the status is "administratively down," the module is deactivated; if it shows "ok," the module is active.

Example:

```
Router# show hw-module subslot all oir

 Module                   Model                Operational Status
----------------------- -------------------- ------------------------
subslot 0/0              4x1G-2xSFP+          ok
subslot 0/1              C-NIM-1X             ok
subslot 1/0              SM-X-16G4M2X         ok

RadiumPP#
```

Step 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:

Example:

```
Router# show hw-module subslot all oir

 Module                   Model                Operational Status
----------------------- -------------------- ------------------------
```

```
subslot 0/0             4x1G-2xSFP+          ok
subslot 0/1             C-NIM-1X             ok
subslot 1/0             SM-X-16G4M2X         ok

RadiumPP#
Router# show platform hardware backplaneswitch-manager R0 status
slot  bay   port   enable   link status   speed(Mbps)   duplex   autoneg   pause_tx   pause_rx   mtu
-------------------------------------------------------------------------------------------------------
0      0     CP     True      Up           1000          Full    ENABLED    ENABLED    ENABLED
10240
1      0     GE1    True      Up           1000          Full    DISABLED   ENABLED    ENABLED
10240
1      0     GE0    True      Up           1000          Full    DISABLED   ENABLED    ENABLED
10240
2      0     GE1    True      Up           1000          Full    DISABLED   ENABLED    ENABLED
10240
2      0     GE0    True      Up           1000          Full    DISABLED   ENABLED    ENABLED
10240
0      1     GE1    True     Down          1000          Full    DISABLED   ENABLED    ENABLED
10240
0      1     GE0    True     Down          1000          Full    DISABLED   ENABLED    ENABLED
10240
0      2     GE1    True     Down          1000          Full    DISABLED   ENABLED    ENABLED
10240
0      2     GE0    True     Down          1000          Full    DISABLED   ENABLED    ENABLED
10240
0      3     GE1    True     Down          1000          Full    DISABLED   ENABLED    ENABLED
10240
0      3     GE0    True     Down          1000          Full    DISABLED   ENABLED    ENABLED
10240
0      4     GE1    True     Down          1000          Full    DISABLED   ENABLED    ENABLED
10240
0      4     GE0    True     Down          1000          Full    DISABLED   ENABLED    ENABLED
10240
0      0     FFP    True       Up         10000          Full    ENABLED    DISABLED   DISABLED
10240
slot  bay   port            mac    vid   modid     flags - Layer 2
-------------------------------------------------------------------------
0      0    FFP  2c54.2dd2.661b   2351       1              0x20
0      0    FFP  2c54.2dd2.661b   2352       1              0x20
0      0     CP  2c54.2dd2.661e   2351       0              0xC60
0      0     CP  2c54.2dd2.661e   2352       0              0x20
1      0    GE0  58bf.ea3a.00f6   2350       0              0x460
0      0    FFP  2c54.2dd2.661b   2350       1              0x20
1      0    GE0  58bf.ea3a.00f6   2352       0              0x20
0      0     CP  2c54.2dd2.661e   2350       0              0x20
1      0    GE0  58bf.ea3a.00f6   2351       0              0xC60
Port block masks: rows=from port, columns=to port, u=unknown unicast, m=unknown multicast, b=broadcast,
 A=all

           CP    FFP  1/0/1  1/0/0  2/0/1  2/0/0  0/1/1  0/1/0  0/2/1  0/2/0  0/3/1  0/3/0  0/4/1
0/4/0 drops
-------------------------------------------------------------------------------------------------------
CP          -     A     um     um     um     um     um     um     um     um     um     um     um
  um     1
FFP         A     -      -      -      -      -      -      -      -      -      -      -      -
   -     0
1/0/1      um    umb     -    umb    umb    umb    umb    umb    umb    umb    umb    umb    umb
 umb     0
1/0/0      um    umb    umb     -     umb    umb    umb    umb    umb    umb    umb    umb    umb
 umb     6
2/0/1      um    umb    umb    umb     -     umb    umb    umb    umb    umb    umb    umb    umb
 umb     0
2/0/0      um    umb    umb    umb    umb     -     umb    umb    umb    umb    umb    umb    umb
```

```
 umb      6
0/1/1       um     umb    umb     umb     umb     umb      -      umb     umb     umb     umb     umb     umb
 umb      0
0/1/0       um     umb    umb     umb     umb     umb     umb       -     umb     umb     umb     umb     umb
 umb      0
0/2/1       um     umb    umb     umb     umb     umb     umb      umb      -      umb     umb     umb     umb
 umb      0
0/2/0       um     umb    umb     umb     umb     umb     umb      umb     umb      -      umb     umb     umb
 umb      0
0/3/1       um     umb    umb     umb     umb     umb     umb      umb     umb     umb      -      umb     umb
 umb      0
0/3/0       um     umb    umb     umb     umb     umb     umb      umb     umb     umb     umb      -      umb
 umb      0
0/4/1       um     umb    umb     umb     umb     umb     umb      umb     umb     umb     umb     umb      -
 umb      0
0/4/0       um     umb    umb     umb     umb     umb     umb      umb     umb     umb     umb     umb     umb
   -      0

Port VLAN membership: [untagged vlan] U=untagged T=tagged <VLAN range begin>-<VLAN range end>

CP [2352] U:0001-0001 T:0002-2351 U:2352-2352 T:2353-4095
FFP [2352] T:0001-4095
1/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
1/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
2/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
2/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
0/1/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
0/1/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
0/2/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
0/2/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
0/3/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
0/3/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
0/4/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
0/4/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
```

You have verified the current operational state of the module, confirming deactivation or activation as required.

To verify interface connectivity for an active module, enter the **show platform hardware backplaneswitch-manager R0 status** command.

```
Router# show platform hardware backplaneswitch-manager rp active ffp statistics
Broadcom 10G port(e.g: FFP) status:
                           Rx pkts          Rx Bytes          Tx Pkts          Tx Bytes
-------------------------------------------------------------------------------------------
All                              0                 0                 0                 0
=64                              0                                   0
65~127                           0                                   0
128~255                          0                                   0
56~511                           0                                   0
512~1023                         0                                   0
1024~1518                        0                                   0
1519~2047                        0                                   0
2048~4095                        0                                   0
4096~9216                        0                                   0
9217~16383                       0                                   0
Max                              0                                   0
Good                             0                                   0
  CoS 0                                                              0                 0
  CoS 1                                                              0                 0
  CoS 2                                                              0                 0
  CoS 3                                                              0                 0
```

```
  CoS 4                                                 0                0
  CoS 5                                                 0                0
  CoS 6                                                 0                0
  CoS 7                                                 0                0
  Unicast                  0                            0
  Multicast                0                            0
  Broadcast                0                            0
  Control                  0
Errored
  FCS                      0                            0
  Undersize                0
  Ether len                0
  Fragment                 0                            0
  Jabber                   0
  MTU ck, good             0
  MTU ck, bad              0
  Tx underflow                                                          0
  err symbol               0
  frame err                0
  junk                     0
Drops
  CoS 0                                                 0                0
  CoS 1                                                 0                0
  CoS 2                                                 0                0
  CoS 3                                                 0                0
  CoS 4                                                 0                0
  CoS 5                                                 0                0
  CoS 6                                                 0                0
  CoS 7                                                 0                0
  STP                      0
  backpress                0
  congest                  0                  0
  purge/cell               0
  no destination           0
Pause PFC                  0                            0
  CoS 0                    0
  CoS 1                    0
  CoS 2                    0
  CoS 3                    0
  CoS 4                    0
  CoS 5                    0
  CoS 6                    0
  CoS 7                    0
```

Modules and interface management

Module management in a router refers to the process of:

- Identifying and verifying modules to ensure only authorized hardware or software components are activated.
- Expanding the router’s capabilities by providing additional network connections.
- Detecting modules, authenticating and configuring them for clients, monitoring status, and performing recovery actions to ensure optimal functionality.

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. It also involves reporting on the state of the interface and the interface-level statistics.

Module configurations

A module configuration is a process that

- defines how modules are activated or deactivated,
- controls power allocation to the module, and
- manages module interface status within a chassis.

Examples

Deactivating a module configuration

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 slot 1 subslot 1/0 shutdown unpowered
```

Activating a module configuration

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)# hw-module slot 1 subslot 1/0 start
```

Cellular IPv6 Addresses

An IPv6 addresses are network addresses that

- are 128-bit identifiers,
- represented as eight 16-bit hexadecimal fields separated by colons(:) and,
- can be compressed by omitting consecutive zero fields using double colons (::).

IPv6 addresses commonly contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress successive hexadecimal fields of zeros at any position in the address.

An IPv6 address prefix, in the format IPv6-prefix/ prefix-length, can be used to represent bit-wise contiguous blocks of addresses. The IPv6 prefix must use the format documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

The prefix length is a decimal value which indicates the number of high-order contiguous bits in the address that forms the prefix or the network portion. For example, 2001:cdba::3257:9652 /64 is a valid IPv6 prefix; here, /64 indicates the number of high-order bits comprising the prefix.

Examples of IPv6 addresses are:

- 2001:CDBA:0000:0000:0000:0000:3257:9652
- 2001:CDBA::3257:9652 (zeros can be omitted)

IPv6 Unicast Routing

An IPv6 unicast address is an IPv6 address type that

- identifies a single interface on a single node,
- ensures that packets sent to this address are delivered only to the specified interface, and
- is used for one-to-one communication in IPv6 networks.

The Cisco Catalyst 8300 Edge Platforms support Link-Local address and Global addresses unicast addresses.

Link-local addresses

Link-local addresses are IPv6 unicast addresses that

- are automatically configured on any IPv6-enabled interface,
- uses the link-local prefix FE80::/10 and a modified EUI-64 format interface identifier, and
- used for communication within the same local network link (subnet).

A link-local address is automatically configured on the cellular interface when an IPv6 address is enabled on an interface. After the data call is established, the cellular interface is updated with the host generated link-local address. This address consists of the link-local prefix FF80::/10 (1111 1110 10) and an auto-generated interface identifier from the USB hardware address.

Global addresses

Global IPv6 addresses are the IPv6 equivalent of public IPv4 addresses that

- uses a global routing prefix assigned by an Internet Service Provider (ISP),
- includes a subnet ID for network organization, and
- incorporates an interface ID derived from the device's hardware address.

The routing prefix is obtained from the PGW. The Interface Identifier is automatically generated from the USB hardware address by using the modified EUI-64 format. The USB hardware address changes when the router reloads.

Configure a cellular IPv6 address

Configuring a cellular IPv6 address is essential to enable IPv6 connectivity and routing over cellular networks. To configure the cellular IPv6 address, perform these steps:

Procedure

Step 1 **ipv6 unicast-routing**

Example:

```
Router(config)# ipv6 unicast-routing
```

In the global configuration mode, enables forwarding of IPv6 unicast data packets.

Step 2 **interface Cellular** {**type** | **number**}

Example:

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

Specifies the cellular interface.

Step 3 ip address negotiated

Example:

```
Router(config-if)# ip address negotiated
```

Obtains the IP address for the specified interface dynamically.

Step 4 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 5 Configure dialer settings.

Example:

```
Router(config-if)# dialer in-band
```

Enables DDR and configures the specified serial interface to use in-band dialing.

Example:

```
Router(config-if)# dialer idle-timeout 0
```

Specifies the dialer idle timeout period.

Example:

```
Router(config-if)# dialer-group 1
```

Specifies the number of the dialer access group to which the specific interface belongs.

Step 6 no peer default ip address

Example:

```
Router(config-if)# no peer default ip address
```

Removes the default address from your configuration.

Step 7 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 8 **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 9 **ipv6 route** *ipv6-prefix/prefix-length 128*

Example:

```
Router(config)#ipv6 route 2001:1234:1234::3/128 Cellular0/1/0
```

Examples

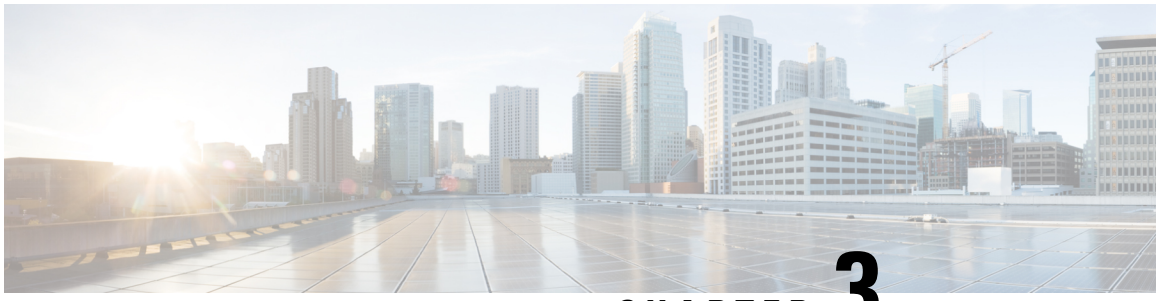
The example shows the Cellular IPv6 configuration for NIM-LTEA-EA and NIM-LTEA-LA modules.

```
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
```

The 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 3

Network Resiliency

High Availability

The Cisco high availability technology is a network resiliency solution that

- enables rapid recovery from disruptions,
- ensures fault transparency to users and network applications, and
- maximizes network uptime through integrated hardware and software design.

These mechanisms that help maintain continuous network operations even during failure events or maintenance.

Interchassis high availability

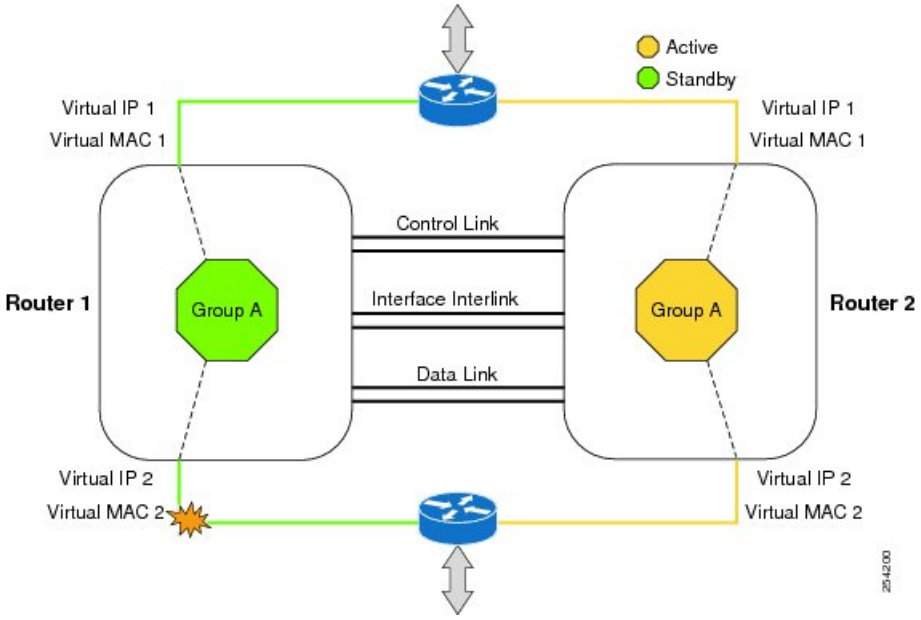
The Interchassis High Availability feature is also known as the box-to-box redundancy feature is a system redundancy solution that

- enables two devices to form a backup pair for high-availability operation,
- automatically monitors device status to detect failures, and
- seamlessly transfers call signaling and media forwarding to a standby device during failover.

Redundancy groups

Groups of redundant interfaces are known as redundancy groups. The 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 2: Redundancy group configuration



The devices are connected 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 transfers stateful information to synchronize the database for the calls and media flows. Each pair of redundant interfaces is configured with the same unique ID number, also known as the RII.

Prerequisites

Before configuring interchassis high availability, ensure that you meet all these requirements:

- 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.

Limitations

- 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 Catalyst 8300 Edge Platform.
- 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.

Configure Interchassis High Availability

For information on configuring Interchassis High Availability on the device, see the IP Addressing: Configuring NAT for IP Address Conservation.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a protocol that

- rapidly detects failures in the forwarding path between two routers,
- provides fast-forwarding path-failure detection times for all media type, routing protocol, or topology, and
- provides consistent and predictable failure detection rates for streamlined network convergence.

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 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, resulting in faster failure detection. By sending rapid failure detection packets to routing protocols, BFD offload helps recalculating the routing table and reduces network convergence time.

Limitation

These are the limitations when configuring tha BFD offload.

- 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.

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.

Configure BFD Offload

BFD offload functionality is enabled by default. You can configure BFD hardware offload on the route processor. For more information, see the IP Routing BFD Configuration Guide.

Verify Interchassis High Availability

You can verify the Interchassis High Availability configuration using these **show** commands. This section provides some examples to verify the configuration.

Use these **show** commands to verify the Interchassis High Availability.

- **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]**

This 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
```

This 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
```

This 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
```

This 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
```

This 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
```

This 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
```

This 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
```

This 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 GigabitEthernet0/0/0
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 GigabitEthernet0/0/0
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
```

This 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 GigabitEthernet0/0/0
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
```

This 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 GigabitEthernet0/0/0
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
```

This 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
```

This 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
```

This 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
```

This 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: GigabitEthernet0/0/0
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: GigabitEthernet0/0/0
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
```

This 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: GigabitEthernet0/0/0
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
```

This 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: GigabitEthernet0/0/0
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
```

This 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
```

This example shows configuration details for redundancy application interface manager group:

```
Router# show redundancy application if-mgr group
 RG ID: 1
 ==========
```

```
 interface      GigabitEthernet0/0/3.152
 ---------------------------------------
 VMAC           0007.b421.4e21
 VIP            203.0.113.1
 Shut           shut
 Decrement      10

 interface      GigabitEthernet0/0/2.152
 ---------------------------------------
 VMAC           0007.b421.5209
 VIP            203.0.113.4
 Shut           shut
 Decrement      10


 RG ID: 2
 ==========

 interface      GigabitEthernet0/0/3.166
 ---------------------------------------
 VMAC           0007.b422.14d6
 VIP            203.0.113.6
 Shut           no shut
 Decrement      10

 interface      GigabitEthernet0/0/2.166
 ---------------------------------------
 VMAC           0007.b422.0d06
 VIP            203.0.113.9
 Shut           no shut
 Decrement      10
```

These examples show configuration details for redundancy application interface manager group 1 and group 2:

```
Router# show redundancy application if-mgr group 1

 RG ID: 1
 ==========

 interface      GigabitEthernet0/0/3.152
 ---------------------------------------
 VMAC           0007.b421.4e21
 VIP            203.0.113.3
 Shut           shut
 Decrement      10

 interface      GigabitEthernet0/0/2.152
 ---------------------------------------
 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      GigabitEthernet0/0/3.166
 ---------------------------------------
 VMAC           0007.b422.14d6
 VIP            203.0.113.5
 Shut           no shut
```

```
Decrement       10

interface       GigabitEthernet0/0/2.166
--------------------------------------
VMAC            0007.b422.0d06
VIP             203.0.113.7
Shut            no shut
Decrement       10
```

This example shows configuration details for redundancy application data-interface group:

```
Router# show redundancy application data-interface group
The data interface for rg[1] is GigabitEthernet0/0/1
The data interface for rg[2] is GigabitEthernet0/0/1
```

These 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 GigabitEthernet0/0/1

Router # show redundancy application data-interface group 2
The data interface for rg[2] is GigabitEthernet0/0/1
```

Verify BFD Offload

Use these commands to verify and monitor BFD offload feature on your device.

- **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.

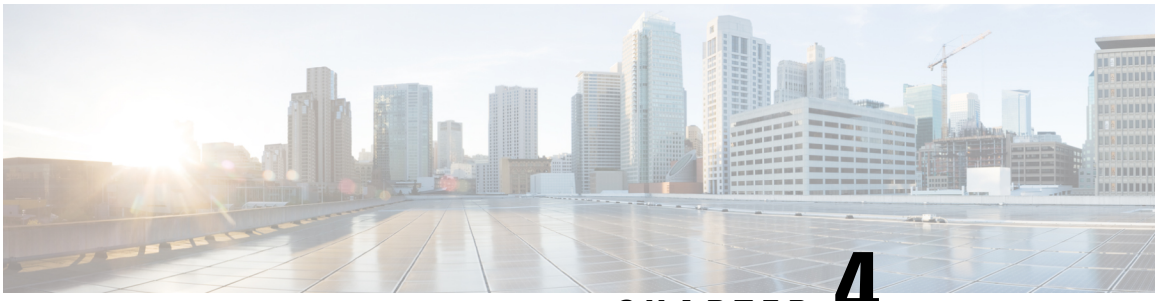
```
Router# debug bfd packet
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Rx IP:192.0.2.1 ld/rd:1941/0 diag:0(No Diagnostic)
 Down C cnt:4 ttl:254 (0)
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Tx IP:192.0.2.1 ld/rd:983/1941 diag:3(Neighbor
Signaled Session Down) Init  C cnt:44 (0)
*Nov 12 23:08:28.007: BFD-DEBUG 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 4

Network Visibility

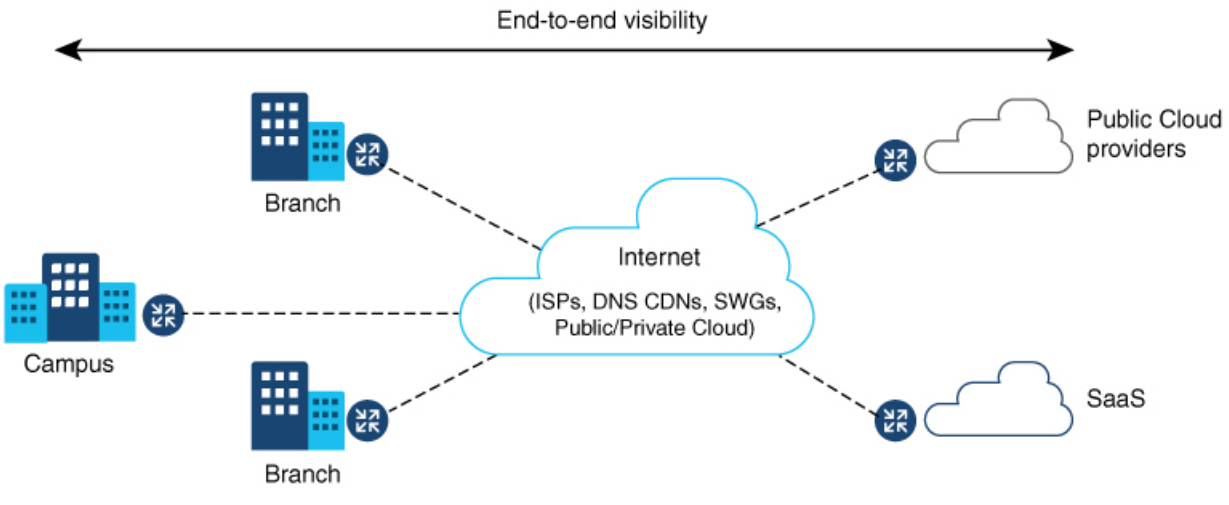
Cisco ThousandEyes Enterprise agent application

Cisco ThousandEyes is a network intelligence platform that

- allows you to use its agents to run a variety of tests to monitor network and application performance,
- enables you to view end-to-end paths across networks and services that impact your business,
- actively monitors network traffic paths across internal, external, and internet networks in real time to analyze network performance, and
- provides application-availability insights enriched with routing and device data for a multidimensional view of digital experience.

From Cisco IOS XE Release 17.6.1, you can use application-hosting capabilities to deploy the Cisco ThousandEyes Enterprise Agent as a container application on Cisco Catalyst 8300 and Catalyst 8200 Series Edge Platforms. This agent application runs as a docker image using Cisco IOx docker-type option. For more information on how to configure Cisco ThousandEyes in controller mode, see Cisco SD-WAN Systems and Interfaces Configuration Guide

Figure 3: Network View through ThousandEyes Application



Supported platforms and system requirements

Supported platforms and system requirements are listed.

Table 12: Supported Platforms and System Requirements

Platforms	Bootflash	FRU Storage	DRAM
Catalyst 8300 Series Edge Platforms			
C8300-1N1S-6T	8 GB	16 GB M.2 USB (Default)	8 GB
C8300-1N1S-4T2X	8 GB	16 GB M.2 USB (Default)	8 GB
C8300-2N2S-6T	8 GB	16 GB M.2 USB (Default)	8 GB
C8300-2N2S-4T2X	8 GB	16 GB M.2 USB (Default)	8 GB
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	8 GB	16 GB M.2 USB (Default)	8 GB
C8200L-1N-4T	8 GB	16 GB M.2 USB (Recommended)	8 GB

Note The minimum DRAM and storage requirement for running Cisco ThousandEyes Enterprise Agent is 8 GB. If the device does not have enough memory or storage, we recommend that you upgrade DRAM or add an external storage such as M.2 USB. When the available resources are not sufficient to run other applications, Cisco IOx generates an error message.

Workflow to install and run the Cisco ThousandEyes application

To install and run the Cisco ThousandEyes image on a device, perform these steps:

Procedure

Step 1 Create a new account on the Cisco ThousandEyes portal.

Step 2 Download the Cisco ThousandEyes application package from the software downloads page and ensure that you use the agent version 4.0.2.

Step 3 Copy the image on the device.

Step 4 Install and launch the image.

Step 5 Connect the agent to the controller.

Note
When you order platforms that support Cisco ThousandEyes application with Cisco IOS XE 17.6.1 software, the Cisco ThousandEyes application package is available in the bootflash of the device.

The Cisco ThousandEyes Enterprise Agent application is successfully installed and running on your device.

Workflow to host the Cisco ThousandEyes application

Use this workflow to install, configure, and launch the Cisco ThousandEyes Enterprise Agent application on your device.

To install and launch the application, perform these steps:

Before you begin

Create a new account on the Cisco ThousandEyes portal and generate the token. The Cisco ThousandEyes agent application uses this token to authenticate and check into the correct Cisco ThousandEyes account. If you receive a message stating that your token is invalid and you want to troubleshoot the issue, see Troubleshooting the Cisco ThousandEyes Application.

Note If you configure the correct token and Domain Name Server (DNS) information, the device is discovered automatically.

Procedure

Step 1 Enable the Cisco IOx application environment on the device.

- Use these commands for non-SD-WAN (autonomous mode) images:

```
config terminal
 iox
end
```

```
write
```

- Use these commands for SD-WAN (controller mode) images:

```
config-transaction
iox
commit
```

Step 2 If the IOx command is accepted, wait for a few seconds and check whether the IOx process is up and running by using the **show iox** command. The output must display that the show IOxman process is running.

```
Device #show iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF) 192.0.2.8     : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Not Supported
Libvirtd 1.3.4                 : Running
```

Step 3 Ensure that the ThousandEyes application LXC tarball is available in the device's *bootflash:*.

Step 4 Create a virtual port group interface to enable the traffic path to the Cisco ThousandEyes application:

```
interface VirtualPortGroup 0
          ip address 192.0.2.22 255.255.255.0
        exit
```

Step 5 Configure the app-hosting application with the generated token:

```
app-hosting appid te
          app-vnic gateway1 virtualportgroup 0 guest-interface 0
          guest-ipaddress 192.0.2.22 netmask 255.255.255.0
          app-default-gateway 192.0.2.22 guest-interface 0
          app-resource docker
             prepend-pkg-opts  Required to get the default run-time options from package.yaml
             run-opts 1 "--hostname thousandeyes"
             run-opts 2 "-e TEAGENT_ACCOUNT_TOKEN=<ThousandEyes token>"
       run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e TEAGENT_PROXY_LOCATION=proxy.something.other:80"
          name-server0 192.0.2.10  ISP's DNS server
        end

app-hosting appid te
 app-resource docker
  prepend-pkg-opts
  run-opts 2 "--hostname
```

Note
You can use the proxy configuration only if the Cisco ThousandEyes agent does not have an internet access without a proxy. Also, the hostname is optional. If you do not provide the hostname during the installation, the device hostname is used as the Cisco ThousandEyes agent hostname. The device hostname is displayed on the Cisco ThousandEyes portal. The DNS name server information is optional. If the Cisco ThousandEyes agent uses a private IP address, ensure that you establish a connection to the device through NAT.

Step 6 Configure the **start** command to run the application automatically when the application is installed on the device using the **install** command:

```
app-hosting appid te
         start
```

Step 7 Install the ThousandEyes application:

```
app-hosting install appid <appid> package [bootflash: | harddisk: | https:]
```

Select a location to install the ThousandEyes application from these options:

```
Device# app-hosting install appid te package ?
           bootflash:  Package path □ ISR4K case if image is locally available in bootflash:
           harddisk:   Package path □ Cat8K case if image is locally available in M.2 USB
           https:      Package path □ Download over the internet if image is not locally present in
 router. URL to ThousandEyes site hosting agent image to be provided here
```

Step 8 Check if the application is up and running:

```
Device#show app-hosting list
 App id                                   State
---------------------------------------------------------
  te                                       RUNNING
```

Note
If any of these steps fail, use the **show logging** command and check the IOx error message. If the error message is about insufficient disk space, clean the storage media (bootflash or hard disk) to free up the space. Use the **show app-hosting resource** command to check the CPU and disk memory.

The Cisco ThousandEyes application is successfully hosted and running on your device.

Download and copy the image to the device

Use this task to ensure the Cisco ThousandEyes application image is correctly placed on your device for installation.

To download and copy the image to bootflash, perform these steps:

Procedure

Step 1 Check if the Cisco ThousandEyes image is precopied to *bootflash:/<directory name>*.

Step 2 If the image is not available in the device directory, perform these steps:

a) If the device has a direct access to internet, use the *https:*. option in the **application install** command. This option downloads the image from the Cisco ThousandEyes software downloads page into *bootflash:/apps* and installs the application.

```
Device# app-hosting install appid <appid string> package [bootflash: | flash | http | https://
| ftp | ] URL to image location hosted on ThousandEyes portal

Device# app-hosting install appid te1000 package
https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar

Installing package
'https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar'
 for 'te1000'.

Use 'show app-hosting list' for progress.
*Jun 29 23:43:29.244: %IOSXE-6-PLATFORM: R0/0: IOx:  App verification successful
```

```
*Jun 29 23:45:00.449: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install succeeded: te1000
installed successfully Current state is DEPLOYED
*Jun 29 23:45:01.801: %IOSXE-6-PLATFORM: R0/0: IOx:  App verification successful
*Jun 29 23:45:51.054: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succeeded: te1000 started
 successfully Current state is RUNNING

Device#show app-hosting detail appid te1000  ( Details of Application)
App id                 : te1000
Owner                  : iox
State                  : RUNNING
Application
  Type                 : docker
  Name                 : ThousandEyes Enterprise Agent
  Version              : 4.0
  Author               : ThousandEyes <support@thousandeyes.com>
  Path                 : bootflash:thousandeyes-enterprise-agent-4.0-22.cisco.tar
Resource reservation
  Memory               : 500 MB
  Disk                 : 1 MB
  CPU                  : 1500 units
  CPU-percent          : 70 %
```

b) If the device has a proxy server, copy the image manually to *bootflash:/apps*.

c) Download the Cisco ThousandEyes application package from the software downloads page and ensure that you use the agent version 4.0.2.

d) Create an application directory in the *bootflash:* to copy the image:

```
Device# mkdir bootflash:apps
Create directory filename [apps]?
Created dir bootflash:/apps
```

e) Copy the Cisco ThousandEyes image to the *bootflash:apps* directory.

f) Validate the image using the **verify** command:

```
verify /md5 bootflash:apps/<file name>
```

The Cisco ThousandEyes image is successfully downloaded and copied to the device's bootflash.

Connect the Cisco ThousandEyes Agent with the controller

This task explains the process of the Cisco ThousandEyes agent connecting to its controller in the cloud environment.

To connect the Cisco ThousandEyes agent with the controller, perform these steps:

Before you begin

Ensure that you have an Internet connection before you connect the agent with the controller.

Procedure

After the Cisco ThousandEyes application is up and running, the agent (ThousandEyes-agent) process connects to the controller that is running on the cloud environment.

Note

If you have issues related to connectivity, the application logs the relevant error messages in the application-specific logs (/var/logs).

The Cisco ThousandEyes agent is successfully connected to the controller.

Modify the agent parameters

Use this task to update the configuration settings of an application agent, which requires stopping and restarting the application.

To modify the agent parameters, perform these actions:

Procedure

Step 1 Stop the application using the **app-hosting stop appid appid** command.
Step 2 Deactivate the application using the **app-hosting deactivate appid appid** command.
Step 3 Make the required changes to the app-hosting configuration.
Step 4 Activate the application using the **app-hosting activate appid appid** command.
Step 5 Start the application using the **app-hosting start appid appid** command.

The agent parameters have been successfully modified and the application is running with the new configuration.

Uninstall the application

Use this task to completely remove a previously installed application from your device.

To uninstall the application, perform these steps:

Procedure

Step 1 Stop the application using the **app-hosting stop appid te** command.
Step 2 Check if the application is in active state using the **show app-hosting list** command.
Step 3 Deactivate the application using the **app-hosting deactivate appid te** command.
Step 4 Ensure that the application is not in active state. Use the **show app-hosting list** command to check status of the application.
Step 5 Uninstall the application using the **app-hosting uninstall appid te** command.
Step 6 After the uninstallation process is complete, use the **show app-hosting list** command to check if the application is uninstalled successfully.

The application has been successfully uninstalled from the device.

Troubleshoot the Cisco ThousandEyes application

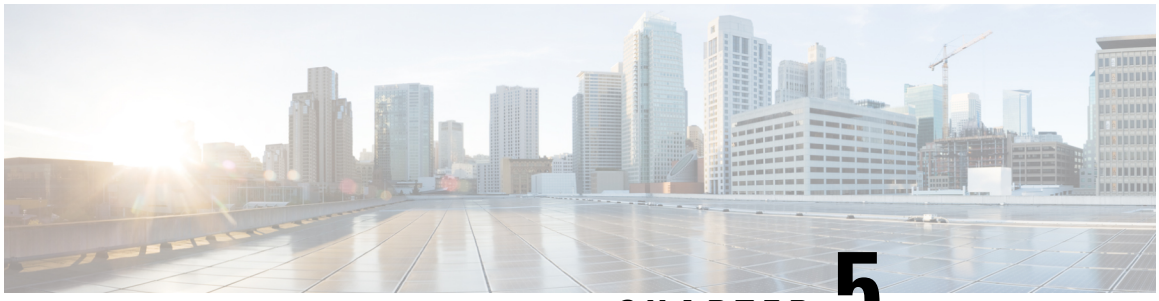
To troubleshoot the Cisco ThousandEyes application, perform these steps.

- Connect to Cisco ThousandEyes agent application using the **app-hosting connect appid appid session /bin/bash** command.
- Verify the configuration applied to the application /etc/te-agent.cfg.
- View the logs in /var/log/agent/te-agent.log. You can use these logs to troubleshoot the configuration.

When the Cisco ThousandEyes application is in running state, it is registered on the ThousandEyes portal. If the application does not show up in a few minutes after the agent is in running state, check using the **app-hosting connect appid thousandeyes_enterprise_agent session** command.

Note Check the DNS server connection. If the Cisco ThousandEyes agent is assigned to a private IP address, check the NAT configuration.

```
Device#app-hosting connect appid thousandeyes_enterprise_agent session
Device#cat /var/log/agent/te-agent.log
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.AptPackageInterface] {} Initialized APT
 package interface
2021-02-04 08:59:29.642 INFO  [e4736a40] [te.agent.main] {} Agent version 1.103.0 starting.
  Max core size is 0 and max open files is 1024
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.db] {} Vacuuming database
2021-02-04 08:59:29.643 INFO  [e4736a40] [te.agent.db] {} Found version 0, expected version
 50
2021-02-04 08:59:29.672 INFO  [e4708700] [te.probe.ServerTaskExecutor] {} ProbeTaskExecutor
 started with 2 threads.
2021-02-04 08:59:29.673 INFO  [e2f05700] [te.probe.ProbeTaskExecutor.bandwidth] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO  [e2704700] [te.probe.ProbeTaskExecutor.realtime] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO  [e1f03700] [te.probe.ProbeTaskExecutor.throughput] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.agent.DnssecTaskProceessor] {} Agent is not
running bind
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
 session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
 session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
 session
2021-02-04 08:59:29.674 INFO  [e4736a40] [te.agent.main] {} Agent starting up
2021-02-04 08:59:29.675 INFO  [e4736a40] [te.agent.main] {} No agent id found, attempting
to obtain one
2021-02-04 08:59:29.675 INFO  [e4736a40] [te.agent.ClusterMasterAdapter] {} Attempting to
get agent id from sc1.thousandeyes.com
2021-02-04 08:59:29.679 ERROR [e4736a40] [te.agent.main] {} Error calling create_agent:
Curl error - Couldn't resolve host name
2021-02-04 08:59:29.680 INFO  [e4736a40] [te.agent.main] {} Sleeping for 30 seconds
```



CHAPTER 5

Wireless Networking

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

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.
- Facilitates routing between line-of-sight and non-line-of-sight paths with ease.
- Provides faster convergence and optimizes route selection to ensure uninterrupted delivery of delay-sensitive traffic, such as voice and video.
- 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 a simple Ethernet connection to radios that are compliant with RFC 5578, R2CP, and DLEP standards.

Restrictions

These restrictions have to be noted before you configure radio aware routing feature:

- The DLEP and R2CP protocols are not supported on Cisco Catalyst 8300 Edge Platform.
- Multicast traffic is not supported in aggregate mode.
- Cisco High Availability (HA) technology is not supported.

License requirements

The radio aware routing feature is made available with the AppX license.

System components

The radio aware routing feature is implemented using the MANET (Mobile ad hoc network) infrastructure comprising of different components:

- PPPoE
- Virtual multipoint interface (VMI)
- QoS
- routing protocol interface and
- RAR protocols

Point-to-Point Protocol over Ethernet (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)

VMI manages and translates events for higher layers, such as routing protocols and 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 Aggregate 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 replicates 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 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
```

Configuration examples for the RAR feature in Bypass Mode

The example shows an end-to-end configuration of RAR in the bypass mode:

Note Before you begin 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 it may not tag *manet_radio* in presentation of a PPPoE Active Discovery Initiate (PADI). By default, bypass mode does not appear in the configuration. It appears only if the mode is configured as bypass.

Configure a service for radio aware routing

```
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 radio aware routing

```
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
```

Configuration examples for the RAR Feature in Aggregate Mode

An example configuration of radio aware routing in aggregate mode is provided.

Note Before you begin 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 radio aware routing

```
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 radio aware routing

```
policy-map type service rar-lab
pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

Configure the 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 radio aware routing session details

Use these show commands to retrieve radio aware routing session details:

```
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
```

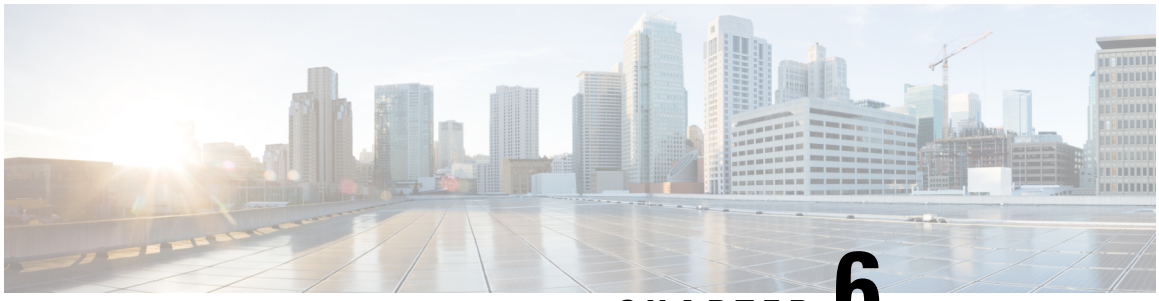
```
         OSPFv3 1 address-family ipv4 (router-id 192.0.2.3)

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

You can troubleshoot the radio aware routing using 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 6

Notification Management

Call Home

The Call home feature is a notification system that

- sends alerts for critical system events via email and web-based notifications,
- supports various message formats for compatibility with pager, email, and automated XML parsing applications, and
- enables direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, or use of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

Prerequisites

Before you configure call home, ensure that these conditions are met.

- Configure the contact e-mail address (required for full registration with smart call home, optional if Call Home is enabled in anonymous mode). Optionally, provide a phone number and street address information. This information enables the receiver to determine the origin of received messages.
- At least one destination profile (predefined or user-defined) must be configured. Select the destination profile based on the type of receiving entity: pager, 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.

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.

Benefits

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.

Obtain 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 these 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.

Configure smart call home (single command)

The smart call home feature is configured to provide proactive diagnostics and real-time email alerts for critical system events on the devices.

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.

Smart call home configuration information

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 (“”).

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
```

Destination profile configuration information

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 these 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.

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.

Use the **show call-home profile** {*name* | **all**} command to display the destination profile configuration for the specified profile or all configured profiles.

```
Router# show call-home profile profile1
```

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. The alert groups available are:

- Crash
- Configuration
- Environment
- Inventory
- Snapshot
- Syslog

The triggering events for each alert group are listed in Alert groups Trigger Events and Commands, and the contents of the alert group messages are listed in Message contents.

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 **call-home**

Example:

```
Router(config)# call-home
```

In the configuration mode, enter Call Home configuration submode.

Step 2 **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 3 **profile** *name*

Example:

```
Router(cfg-call-home)# profile profile1
```

Enters the Call Home destination profile configuration submode for the specified destination profile.

Step 4 **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 5 **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.

Step 6 **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.

Step 7 **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.

Step 8 **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 .

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 9 **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 10 **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.

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. In doing so, the output of the commands added in the Snapshot alert group will be included in the snapshot message.

Step 11 **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:

- 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 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 13: 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

The commands added to the snapshot command list are executed when a snapshot alert is generated.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 the following 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.

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

The following 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

Rate Limit specifies the maximum number of call home messages that a device is allowed to send per minute. This setting helps control the volume of messages sent to avoid overwhelming the network or the receiving system.

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.

Configure HTTP proxy server

An HTTP proxy server acts as an intermediary between a client device and a web server, intercepting requests from the client and forwarding them to the web server on the client's behalf. This task provides details on configuring an HTTP proxy Server for sending Call Home HTTP(S) messages to a destination.

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

AAA authorization is needed to control and limit the services and resources a user can access after they have been authenticated. It enforces policies by determining what activities, resources, or services a user is permitted to use based on their user profile. To specify an HTTP proxy server for sending call home HTTP(S) messages to a destination, use these steps:

Before you begin

-

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

Syslog throttling is used to control and limit the sending of repetitive syslog messages. When syslog throttling is enabled, it prevents the device from sending the same call home syslog messages repeatedly, which helps reduce unnecessary log traffic and avoids overwhelming the management systems with duplicate alerts.

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 a call home test message manually

You can manually send several types of call home communications. To send call home communications, perform the tasks in this section.

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, execute this command:

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 the following 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 the following 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.

To submit a request for analysis and report information from the Cisco Output Interpreter tool, perform the following 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** command includes all inventory alert group commands. The keyword specified after **request** specifies the type of report requested.

- Based on the keyword specifying the type of report requested, the information output is provided:
  - *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.

Example

The following 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 the following 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 this steps:

SUMMARY STEPS

1. **call-home send** {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*]

DETAILED STEPS

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

The following 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
```

The following 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
```

The following 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
```

The following 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
```

The following 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
```

Diagnostic signatures

The diagnostic signatures feature downloads digitally signed signatures to devices. diagnostic signatures 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 diagnostic signatures is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customers networks.

Diagnostic Signature

Diagnostic signatures 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 signatures provide the ability to define more types of events and trigger types than the standard Call Home feature supports. The Diagnostic signatures 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. Diagnostic signatures files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

Diagnostic signatures 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 one of the following 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 following basic information is 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 of Diagnostic Signatures

Before you download and configure diagnostic signatures on a device, you must ensure that these conditions are met:

- You must assign one or more DSs to the device.
- 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 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 diagnostic signature.

Cisco devices 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 diagnostic signature update requests to download these files: regular and forced-download.

- Regular download requests diagnostic signature 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 diagnostic signature is different from the version of the diagnostic signature on the device.

- Periodic download is only started after there is any diagnostic signature assigned to the device from diagnostic signature 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 diagnostic signature download/update. In a diagnostic signature update request message, the status and revision number of the diagnostic signature is included such that only a diagnostic signature with the latest revision number is downloaded.

- Forced-download downloads a specific diagnostic signature or a set of diagnostic signatures. 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 diagnostic signature file is downloaded irrespective of the current DS file version on the device.

The diagnostic signature file is digitally signed, and signature verification is performed on every downloaded diagnostic signature file to make sure it is from a trusted source.

Diagnostic Signature Workflow

Summary

The diagnostic signature feature is enabled by default in Cisco software. These steps outline the workflow for using diagnostic signatures

Workflow

The workflow of Diagnostic Signature involves these stages.

1. Find the diagnostic signature you want to download and assign them to the device. This step is mandatory for regular periodic download, but not required for forced download.
2. The device downloads all assigned diagnostic signature or a specific diagnostic signature by regular periodic download or by on-demand forced download.
3. The device verifies the digital signature of every single diagnostic signature. If verification passes, the device stores the diagnostic signature file into a non-removable disk, such as bootflash or hard disk, so that diagnostic signature files can be read after the device is reloaded. On the router, the diagnostic signature file is stored in the bootflash:/call home directory.
4. The device continues sending periodic regular diagnostic signature download requests to get the latest revision of diagnostic signature and replace the older one in device.
5. The diagnostic signature feature is enabled by default in Cisco software. These steps outline the workflow for using diagnostic signatures:

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 diagnostic signature. The event specification format is one of the following two types:

In single event detection, only one event detector is defined within a diagnostic signature. The event specification format is one of these types:

- diagnostic signature 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 diagnostic signature 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 diagnostic signature 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 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 diagnostic signature that are used to customize the files.

Diagnostic signature actions are categorized into these types:

- call-home
- command
- emailto
- script

Diagnostic signature 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 diagnostic signature ID as the message sub-type.

The commands defined for the diagnostic signature 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 diagnostic signature and are used to customize the diagnostic signature file. All diagnostic signature variable names have the prefix ds_ to separate them from other variables. These are the supported diagnostic signature variable types:

- 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 Diagnostic signatures environment variables. If the Diagnostic signatures file contains unresolved environment variables, this Diagnostic signatures 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 Diagnostic signatures indicates pending.
- Regular expression variable: values assigned from a regular expression pattern match with predefined CLI command outputs. The value is assigned during the Diagnostic signatures run.
- Syslog event variable: values assigned during a syslog event detection in the Diagnostic signatures file. This variable is valid only for syslog event detection.

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 are sent and destination HTTP/secure HTTP (HTTPS) URL to download the diagnostic signatures 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.

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.

Follow these steps to display Call Home configuration information:

Procedure

Step 1 Enter **show call-home** command to display a summary of the call home configuration.

Example:

```
Router# show call-home
```

Step 2 Enter **show call-home detail** command to display detailed call home configuration.

Example:

```
Router# show call-home detail
```

Step 3 Enter **show call-home alert-group** command to view available alert groups and their status.

Example:

```
Router# show call-home alert-group
```

Step 4 Enter **show call-home mail-server status** command to check the availability of the configured email servers.

Example:

```
Router# show call-home mail-server status
```

Step 5 Enter **show call-home profile** { **all** | *name* } command to display configuration for all or specific destination profiles.

Example:

```
Router# show call-home profile all
```

Step 6 Enter the **show call-home statistics** [**detail** | **profile** *profile-name*] command to view statistics of Call Home events.

Example:

```
Router# show call-home statistics
```

The system displays the requested information about call home configuration, profiles, alert groups, email server status, or statistics, enabling you to review or troubleshoot the call home functionality.

Default call home settings

The table lists the default call home settings.

Table 14: Default call home settings

Parameters	Default
Call Home feature status	Disabled

Parameters	Default
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. Each alert group is assigned commands that execute when an event occurs. The output of these commands is included in the transmitted message.

Table 15: Call home alert groups, events, and actions

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Crash	SYSTEM_ CRASH	–	–	These are events related to a software crash. These 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. These 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. These 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. These 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	The 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 was inserted in slot %d, and interfaces were administratively shut down.
Syslog	–	–	–	Event logged to syslog. These 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 significant 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. These 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 16: 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 17: 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 171.	For short text message only
Message type	Specifically “Call Home”.	CallHome/Event/Type
Message subtype	Specific type of message: full, delta, test	CallHome/Event/SubType

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
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 151).	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 The fields may be repeated if multiple commands are executed for this alert group.

Table 18: 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 171).	/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 19: Inserted fields for a reactive or proactive event message

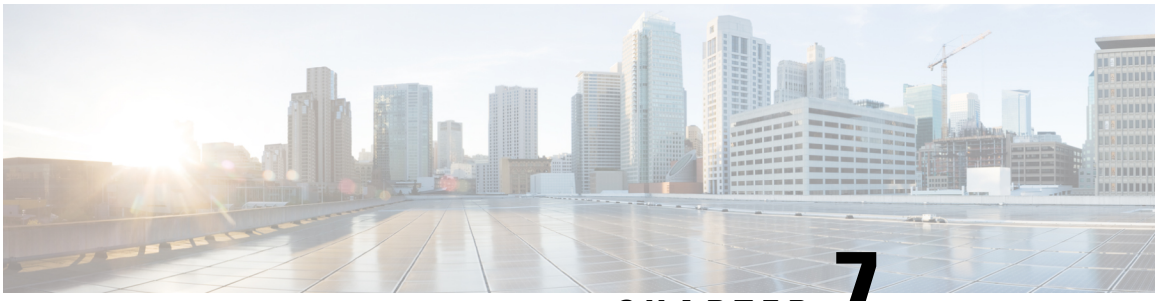
Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/ HardwareVersion
Supervisor module software version	Top-level software version.	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= "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 20: 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 7

Network Policy

Change of Authorization

A Change of Authorization is a network policy mechanism that

- modifies session attributes for active authentication, authorization, and accounting sessions,
- supports actions such as session query, reauthentication, termination, port bounce, and port shutdown, and
- enables dynamic activation or deactivation of service templates.

Change of Authorization is part of Identity-Based Networking Services and enforces policy changes in real time. This feature allows administrators to respond to changes in user roles, device states, or network conditions.

How change of authorization reauthentication works

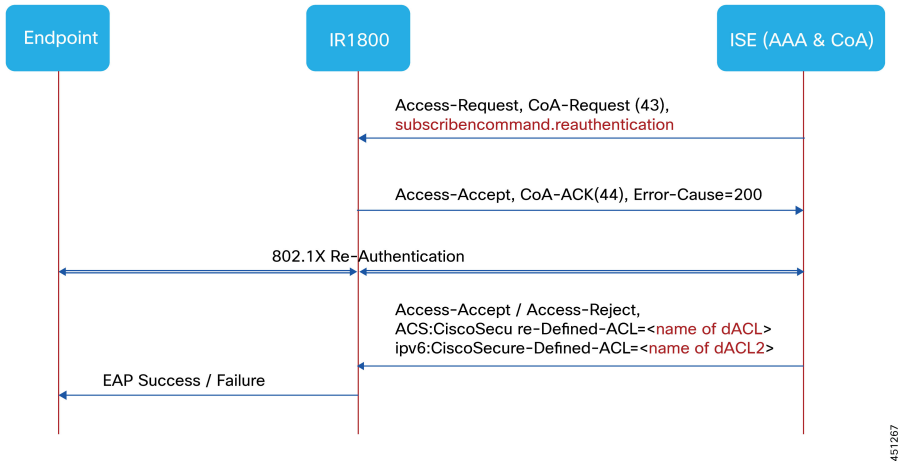
Summary

Change of authorization reauthentication enables dynamic policy changes in AAA sessions after initial authentication.

- When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server.
- The AAA server, such as Cisco Identity Services Engine, uses CoA packets to reinitialize authentication and apply the new policy.
- The RADIUS interface provides various primitives that can be used during a CoA event.
- These primitives and their functions are essential for effectively applying new policies to users or groups during a session.

Workflow

Figure 4: Workflow



1. The administrator changes a user or user group policy in the AAA system.
2. The AAA server sends a RADIUS CoA packet to the network device, specifying policy updates.
3. The device receives the CoA packet and reinitializes authentication, applying the new policy.
4. The RADIUS interface returns either a CoA-ACK (acknowledgement) or CoA-NAK (nonacknowledgement) as a response.

Result

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

- Security and Password
- Accounting
- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

What's next

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

Change of Authorization requests

A Change of Authorization request is a network protocol message that

- enables dynamic modification of attributes for an authenticated AAA session on a network device,
- follows RFC 5176 standard for authorization changes in real time, and
- supports policy enforcement and session control for devices managed by solutions such as Cisco Catalyst SD-WAN Manager.

Topology diagram of Cisco 1000 Series Integrated Services Router as a branch router

The network topology below shows a typical Cisco 1000 Series Integrated Services Router as a branch router in a network for secure access with ISE and other network services deployed in Campus or Data Center. CoA is critical part of the solution to initiate re-authentication or re-authorization to endpoint's network access based on its posture assessment result. Downloadable ACL is the target or purpose of the entire solution.

Figure 5: Network topology of Cisco ISR1000 with ISE and other Network Services

Limitations for Change of Authorization

You must observe these restrictions when configuring change of authorization features:

- Most CoA and posture functions rely on hardware TCAMs, including Downloadable ACL, Redirect ACL, and SISF-based device tracking. Cisco 1000 Series Integrated Services Router 8-Port SKUs are the only platforms that support these features.
- Port ACL is not supported on 1000 Series Integrated Services.
- IPv6 Access Control Entries are not supported.
- IPv4 ACE cannot support IPv4 option header or IP fragment match. TCP or UDP Layer 4 port number matching is supported only with eq (equals sign) or any (asterisk) options. The gt (greater than), lt (less than), and range (A to B) match types are not supported.

  .
- On 1000 Series Integrated Services Routers (except for the C1131 series):
  - Do not exceed 128 dACL ACEs or 64 RACL ACEs for all switchports.
  - Only TCP or UDP port number matching is supported for IPv4 ACE Layer 4 matches.
- On C1131 series routers:
  - Do not exceed 2048 dACL ACEs or 512 RACL ACEs for all switchports.
  - IPv4 ACE Layer 4 match supports TCP or UDP port match, and Layer 4 Flags with match all (not match any).
- SISF device tracking supports IPv4 address glean when security level glean is used, and it supports tracking when tracking enable is configured.
- Multi-authentication per user VLAN assignment is not supported.
- Neither NEAT nor CISP is supported.

Dot1x SANet configuration commands

The following AAA and dot1x configuration commands establish 802.1X authentication using RADIUS on a subscriber network. These commands define authentication and authorization methods, associate RADIUS server groups, enable dot1x operation, and apply necessary policy maps for control.

```
aaa new-model
aaa authentication dot1x default group coa-ise
aaa authorization network default group coa-ise
dot1x system-auth-control
aaa group server radius coa-ise
server name coa
radius server coa
address ipv4 10.10.1.10 auth-port 1812 acct-port 1813
key cisco123
policy-map type control subscriber simple_coa
event session-started match-all
10 class always do-until-failure
10 authenticate using dot1x
```

```
interface gigabitethernet0/0/1\
switchport access vlan 22
switchport mode access
access-session closed
access-session port-control auto
dot1x pae authenticator
service-policy type control subscriber simple_coa
```

Attributes of Change of Authorization

Change of Authorization (CoA) uses specific configuration attributes to enable dynamic authorization with RADIUS servers. The most relevant attributes include:

1. **Client**: Specifies the IP address or host of the device authorized for dynamic changes.
2. **Server-key**: Sets the shared secret between the RADIUS server and client for authorization.
3. **Auth-type**: Determines the authentication type used for requests.
4. **Ignore server-key**: Allows the configuration to skip validating the server key for incoming requests.
5. **ip access-list extended redirect_acl**: Defines network policies permitting or denying certain protocols relevant to CoA operations.
6. **Device-tracking tracking**: Enables device tracking for accurate mapping of endpoints on the network.
7. **Device-tracking policy**: Configures device tracking policies used in conjunction with dynamic authorization.
8. **Tracking enable**: Activates the device-tracking configuration.

The following example allows you to configure Change of Authorization effectively in your network.

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

RADIUS server status example

This example shows how to check if the RADIUS server is active.

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 10.75.28.231, auth-port 1812, acct-port 1813, hostname host
State: current UP
duration 188755s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 188755s, previous duration 0s
```

Device tracking policy verification examples

The following commands help verify device tracking policy configuration and operation:

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

Check enabled device tracking policy parameters

```
Device# show device-tracking policies
Target               Type  Policy               Feature        Target range
Gi0/1/1              PORT  tracking_test        Device-tracking vlan all
Gi0/1/2              PORT  tracking_test        Device-tracking vlan all
Gi0/1/3              PORT  tracking_test        Device-tracking vlan all
Gi0/1/4              PORT  tracking_test        Device-tracking vlan all
```

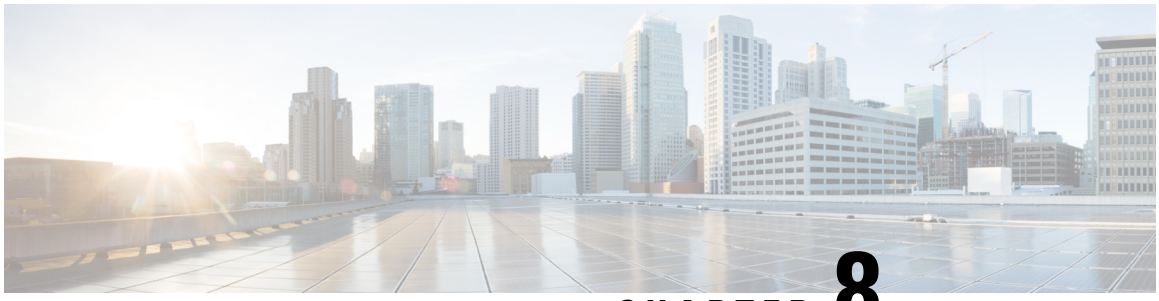
Review SISF table entries

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

Verify access-session authentication and authorization

```
Device# show access-session interface gigabitEthernet 0/1/7 detail
Interface:  GigabitEthernet0/1/7
IIF-ID:  0x0DB9315A
MAC Address:  b496.913d.4f9b
IPv6 Address:  Unknown
IPv4 Address:  10.10.22.27
User-Name:  coa2
Status: Authorized
Domain:  DATA
Oper host mode:  multi-auth
Oper control dir:  both
Session timeout:  N/A
Common Session ID:  611C4B0A00000053F483D7B0
Acct Session ID:  Unknown
Handle:  0x21000049urrent Policy:  POLICY_COA
```

```
Server Policies: Filter-ID: Filter_ID_COA2
Method status list:  Method      State
dot1x          Authc Success
```



CHAPTER 8

Security Management

Security-Enhanced Linux

Security-Enhanced Linux (SELinux) is a solution that incorporates a strong, flexible Mandatory Access Control (MAC) architecture into Cisco IOS-XE platforms through a combination of a Linux kernel security module and system utilities.

SELinux provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements. This approach helps prevent tampering and bypassing of application security mechanisms while limiting damage from malicious or flawed applications.

Security-Enhanced Linux Modes

SELinux can operate either in **Permissive mode** or **Enforcing mode** when enabled on a system.

- **Permissive mode** : SELinux does not enforce the policy and only generates system logs for any denials caused by policy violations. Operations are logged for resource access policy violations but not denied.
- **Enforcing mode** : 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.

Prerequisites

There are no specific prerequisites for this feature.

Restrictions

There are no specific restrictions for this feature.

Configure Security-Enhanced Linux in EXEC Mode

Configuring SELinux in EXEC mode denies resource access based on the access policy rules, and generates system logs. Use this example to configure SELinux in EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	**set platform software selinux** {**default** | **enforcing** | **permissive**}	Configuring SELinux in EXEC mode denies resource access based on the access policy rules, and generates system logs.

Example

```
Device# set platform software selinux ?

default     Set SELinux mode to default
enforcing   Set SELinux mode to enforcing
permissive  Set SELinux mode to permissive
```

Configure Security-Enhanced Linux in CONFIG Mode

Configuring SELinux in CONFIG mode means setting the policy to either **enforcing** or **permissive** state. Use this example to configure SELinux in CONFIG mode:

Use this example to configure SELinux in configuration mode:

Procedure

	Command or Action	Purpose
Step 1	**platform security selinux** {**enforcing** | **permissive**}	Configuring SELinux in CONFIG mode means setting the policy to either **enforcing** or **permissive** state.

Example

```
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)#
```

SYSLOG message reference

This section covers details about syslog messages for SELinux events.

Facility-Severity-Mnemonic	**%SELINUX-1-VIOLATION**
Severity-Meaning	Alert Level Log
Message	N/A
Message Explanation	Resource access was made by the process for which a resource access policy does not exist. The operation was flagged, and resource access was denied. A system log was generated with information that process resource access has been denied.
Component	SELINUX
Recommended Action	Contact Cisco TAC with the following relevant information as attachments: • The exact message as it appears on the console or in the system • Output of the **show tech-support** command (text file) • Archive of Btrace files from the box using the following command: **request platform software trace archive target <URL>** • Output of the **show platform software selinux** command

This example shows 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
```

Verify Security-Enhanced Linux 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
```

Troubleshoot Security-Enhanced Linux

If there is an instance of an SELinux violation on your device or network, please reach out to Cisco TAC with these 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 this command:

  request platform software trace archive target <URL>

- Output of the **show platform software selinux** command

Secure Storage

A secure storage feature is a security mechanism that

- encrypts critical configuration information, such as VPN and IPSec key pairs, pre-shared secrets, and credentials,
- stores an instance-unique encryption key in the hardware trust anchor to prevent compromise, and
- enables protection for type 6 password encryption keys and certain credentials.

By default, this feature is enabled on platforms with a hardware trust anchor. Platforms without a hardware trust anchor do not support secure storage.

Enable secure storage

By default, this feature is enabled on a platform. Use this procedure on a platform where it is disabled.

Procedure

	Command or Action	Purpose
Step 1	Config terminal **Example:** `router#config terminal`	Enters the configuration mode.

	Command or Action	Purpose
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

The following example shows how to enable Secure Storage:

```
router#config terminal
                router(config)# service private-config-encryption
                router(config)# do write memory
```

Disable secure storage

Procedure

	Command or Action	Purpose
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

The following 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. The following 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
```

The following command output indicates that the feature is enabled and the file is encrypted. The file is in 'cipher text' format.

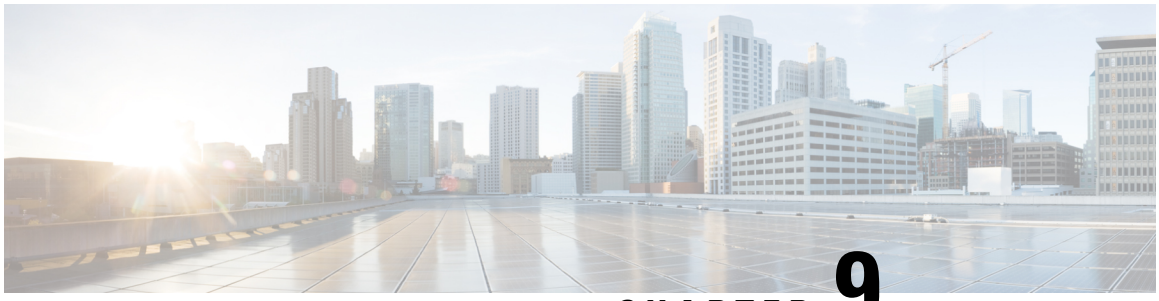
```
router#show parser encrypt file status
Feature: Enabled
File Format: Cipher Text
Encryption Version: Ver1
```

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-----
```



CHAPTER 9

Voice Over IP

Voice Functionality

Call waiting and call transfer

Call Waiting

Call Waiting is a telephone feature that

- allows a user to receive a second incoming call while already engaged in another call,
- plays a call-waiting tone (300 ms duration) when a second call is received,
- displays Caller ID for the waiting call on compatible phones, and.
- enables toggling between active and waiting calls using hookflash.

By using hookflash, you can toggle between the active and a call that is on hold. If the Call Waiting feature is disabled, and you hang up the current call, the second call will hear a busy tone. For more information on Call Waiting, see the https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/sip/configuration/15-mt/sip-config-15-mt-book/voi-sip-hookflash.html

Call Transfer

Call Transfer is a telephone feature that

- allows an active call to be put on hold while a second call is established between two users,
- enables the held party to hear a ringback after the active call is terminated and the second call is connected, and
- supports all three types of call transfers,blind, semi-attended, and attended.

Feature Group D Configuration

To configure the Feature Group D signaling, perform these steps:

Before you begin

Feature Group D service is a trunk side connection that enables telephone customers to choose their long distance network and use the same number of digits irrespective of carrier they use. Routers interface with interexchange carriers using Feature Group D to support voice traffic in the carrier environment.

Before you attempt this configuration, ensure that you meet these prerequisites:

- The platform must be using Digital T1/E1 Packet Voice Trunk Network Modules.
- The Digital T1/E1 Packet Voice Trunk Network Module can have one or two slots for voice/WAN Interface Network Modules (NIMs); NIM supports one to eight ports. Only the dual-mode (voice/WAN) multiple trunk cards are supported in the digital E1 packet voice trunk network module, not older VICs.
- Drop-and-Insert capability is supported only between two ports on the same multiple card.

Procedure

Step 1 **configure terminal** { *ip-address* | *interface-typeinterface-number* [*ip-address*]}

Example:

```
Router(config)# configure terminal
```

Enters global configuration mode.

Step 2 **voice-cardslot/subslot**

Example:

```
Router(config)# voice-card slot/subslot
```

Enters voice card interface configuration mode and specify the slot location by using a value from 0 to 5, depending upon your router.

Step 3 **controller T1/E1slot/subslot/port**

Example:

```
Router(config)# controller T1 slot/subslot/port
```

Enters controller configuration mode for the T1 controller at the specified slot/port location. Valid values for slot and port are 0 and 1.

Step 4 **framing** { *sf* | *esf* }

Example:

```
Router(config)# framing {sf | esf}
```

Sets the framing according to your service provider's instructions. Choose Extended Superframe (ESF) format or Superframe (SF) format.

Step 5 **linecode** { *b8zs* | *ami* }

Sets the line encoding according to your service provider's instructions. Bipolar-8 zero substitution (B8ZS) encodes a sequence of eight zeros in a unique binary sequence to detect line coding violations. Alternate mark inversion (AMI) represents zeros using a 01 during each bit cell, and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independent of the data stream.

Step 6 **ds0-group***ds0-group-no***timeslots** `timeslot-list type` { *e&m-fgd* | *fgd-eana* }

Defines the T1 channels for use by compressed voice calls as well as the signaling method the router uses to connect to the PBX or CO. ds0-group-no is a value from 0 to 23 that identifies the DS0 group. Note The ds0-group command automatically creates a logical voice port that is numbered as follows: slot/port:ds0-group-no. Although only one voice port is created, applicable calls are routed to any channel in the group. timeslot-list is a single number, numbers separated by commas, or a pair of numbers separated by a hyphen to indicate a range of timeslots. For T1, allowable values are from 1 to 24. To map individual DS0 timeslots, define additional groups. The system maps additional voice ports for each defined group. The signaling method selection for type depends on the connection that you are making. The e&m-fgd setting allows E&M interface connections for PBX trunk lines (tie lines) and telephone equipment to use feature group D switched-access service. The fgd-eana setting supports the exchange access North American (EANA) signaling.

Step 7 **no shutdown**

Activates the controller.

Step 8 **exit**

Exits controller configuration mode. Skip the next step if you are not setting up Drop and Insert .

Feature group D is configured.

Media and Signaling Authentication and Encryption

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature implements voice security features that include signaling authentication along with media and signaling encryption on MGCP gateways. For more information on Media and Signaling Authentication and Encryption Feature, see the http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/mgcp/configuration/15-mt/vm-15-mt-book/vm-gw-med-sig.html

Multicast music-on-hold

Multicast Music-on-Hold (MOH) is a Cisco IOS MGCP voice gateway feature that provides music streaming to callers placed on hold via a multicast MOH server.

- Streams music from an MOH server to on-net and off-net callers on hold.
- Utilizes a preconfigured multicast address for gateways to receive RTP packets, and
- Supports multiple MOH servers with unique Class D IP addresses configured in Cisco Communications Manager and MGCP voice gateways.

By means of a preconfigured multicast address on the Cisco Unified Communications Manager or gateway, the gateway can "listen" for Real-Time Transport Protocol (RTP) packets that are broadcast from a default router in the network and can relay the packets to designated voice interfaces in the network. You can initiate the call on hold. However, you cannot initiate music on hold on a MGCP controlled analog phone.

Whenever a called party places a calling party on hold, Cisco Communications Manager requests the MOH server to stream RTP packets to the "on-hold" interface through the preconfigured multicast address. In this way, RTP packets are relayed to appropriately configured voice interfaces that have been placed on hold.

When you configure a multicast address on a gateway, the gateway sends an Internet Gateway Management Protocol (IGMP "join" message to the default router, indicating to the default router that the gateway is ready to receive RTP multicast packets.

Multiple MOH servers can be present in the same network, but each server must have a different Class D IP address, and the address must be configured in Cisco Communications Manager and the MGCP voice gateways. For more information on configuring MOH, see the http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cminterop/configuration/15-0m/vc-15-0m-book/vc-ucm-mgcp-gw.html#GUID-A3461142-2F05-4420-AEE6-032FCA3B7952

TLS 1.2 support on SCCP Gateways

The TLS 1.2 support on SCCP Gateways feature details the configuration of TLS 1.2 on SCCP protocol for digital signal processor (DSP) farm including Unicast conference bridge (CFB), Media Termination Point (MTP), and SCCP telephony control (STC) application (STCAPP).

DSP on gateways can be used as media resources for transrating or transcoding. Each media resource uses Secure Skinny Client Control Protocol (SCCP) to communicate with Cisco Unified Communications Manager. Currently SSL 3.1, which is equivalent to TLS1.0, is used for sending secure signals. This feature enhances the support to TLS 1.2. From Cisco IOS XE Cupertino 17.7.1a, TLS 1.2 is enhanced to support the Next-Generation Encryption (NGE) cipher suites.

Note Cisco Unified Communications Manager (CUCM) Version 14SU2 has been enhanced to support Secured SCCP gateways with the Subject Name field (CN Name) with or without colons, for example, AA:22:BB:44:55 or AA22BB4455.

CUCM checks the CN field of the incoming certificate from the SCCP Gateway and verifies it against the DeviceName configured in CUCM for this gateway. DeviceName contains MAC address of the gateway. CUCM converts the MAC address in the DeviceName to MAC address with colons (for example: AA:22:BB:44:55) and validates with the CN name in the Gateway's certificate. Therefore, CUCM mandates Gateway to use MAC address with colons for the CN field in the certificate, that is, subject name.

Due to new guidelines from Defense Information Systems Agency (DISA), it is a requirement not to use colons for the subject name field CN. For example, AA22BB4455.

SCCP TLS connection

CiscoSSL is based on OpenSSL. SCCP uses CiscoSSL to secure the communication signals.

If a resource is configured in the secure mode, the SCCP application initiates a process to complete Transport Layer Security (TLS) handshaking. During the handshake, the server sends information to CiscoSSL about the TLS version and cipher suites supported. Previously, only SSL3.1 was supported for SCCP secure signalling. SSL3.1 is equivalent to TLS 1.0. The TLS 1.2 Support feature introduces TLS1.2 support to SCCP secure signalling.

After TLS handshaking is complete, SCCP is notified and SCCP kills the process.

If the handshaking is completed successfully, a REGISTER message is sent to Cisco Unified Communications Manager through the secure tunnel. If handshaking fails and a retry is needed, a new process is initiated.

Note For SCCP-based signalling, only TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is supported.

Cipher Suites

For SCCP-based signaling, TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is supported.

From Cisco IOS XE Cupertino 17.7.1a, the following NGE cipher suites are also supported:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

These cipher suites enable secure voice signaling for both the STCAPP analog phone and the SCCP DSPFarm conferencing service. The cipher suite selection is negotiated between gateway and CUCM.

The following prerequisites are applicable for using NGE cipher suites:

- Configure TLS 1.2. For more information, see Configuring TLS Version for STC application, on page 201.
- Use CUCM Release 14.1 SU1 or later, and Voice Gateways or platforms that support TLS 1.2.
- From the CUCM Web UI, navigate to **Cipher Management** and set the **CIPHER switch** as **NGE**. For more information, see Cipher Management.

For more information about verifying cipher suites, see Verifying TLS Version and Cipher Suites, on page 202.

For the SRTP-encrypted media, you can use higher-grade cipher suites - AEAD-AES-128-GCM or AEAD-AES-256-GCM. The selection of these cipher suites is automatically negotiated between GW and CUCM for both secure analog voice and hardware conference bridge voice media. Authenticated Encryption with Associated Data (AEAD) ciphers simultaneously provide confidentiality, integrity, and authenticity, without built-in SHA algorithms to validate message integrity.

Supported Platforms

The TLS 1.2 support on the SCCP Gateways feature is supported on the following platforms:

- Cisco Catalyst 8200 and 8300 Series Edge Platforms

Configuring TLS Version for STC application

Perform the following task to configure a TLS version for the STC application:

```
enable
configure terminal
stcapp security tls-version v1.2
exit
```

Note The stcapp security tls command sets the TLS version to v.1.0, v1.1, or v1.2 only. If not configured explicitly, TLS v1.0 is selected by default.

Configuring TLS Version in Secure Mode for DSP Farm Profile

Perform the following task to configure the TLS version in secure mode for DSP farm profile:

```
enable
configure terminal
dspfarm profile 7 conference security
  tls-version v1.2
  exit
```

Note Note: The **tls** command can be configured only in security mode.

Verifying TLS Version and Cipher Suites

Perform the following task to verify the TLS version and cipher suite:

```
# show dspfarm profile 100
Dspfarm Profile Configuration

 Profile ID = 100, Service = CONFERENCING, Resource ID = 2
 Profile Service Mode : secure
 Trustpoint : Overlord_DSPFarm_GW
 TLS Version  : v1.2
 TLS Cipher   : ECDHE-RSA-AES256-GCM-SHA384
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Total Number of Resources Configured : 10
 Total Number of Resources Available : 10
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Maximum conference participants : 8
 Codec Configuration: num_of_codecs:6
 Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

Verifying STCAPP Application TLS Version

Perform the following tasks to verify TLS version of the STCAPP application:

```
Device# show call application voice stcapp
App Status: Active
CCM Status: UP
CCM Group: 120
Registration Mode: CCM
Total Devices: 0
Total Calls in Progress: 0
Total Call Legs in Use: 0
ROH Timeout: 45
TLS Version: v1.2

# show stcapp dev voice 0/1/0
Port Identifier:  0/1/0
Device Type:      ALG
Device Id:        585
```

```
Device Name:      ANB3176C85F0080
Device Security Mode : Encrypted
  TLS version        : TLS version 1.2
  TLS cipher         : ECDHE-RSA-AES256-GCM-SHA384
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 80010
Dial Peer(s):     100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Line Mode:        CALL_CONF
Hook State:       OFFHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
HG Status:        Unknown
PLAR:             DISABLE
CWT Repetition Interval: 0 second(s) (no repetition)
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6

Call State for Connection 2 (ACTIVE): TsConnected
Connected Call Info:
   Call Reference: 33535871
   Call ID (DSP):  187
   Local IP Addr:  198.51.100.2
   Local IP Port:  8234
   Remote IP Addr: 198.51.100.20
   Remote IP Port: 8154
   Calling Number: 80010
   Called Number:
   Codec:          g711ulaw
   SRTP:           on
   RX Cipher:      AEAD_AES_256_GCM
   TX Cipher:      AEAD_AES_256_GCM
```

Perform the following task to verify the sRTP cipher suite for the DSPfarm connection.

```
# show sccp connection detail

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id    conn_id    call-id    codec   pkt-period dtmf_method    type
bridge-info(bid, cid)   mmbridge-info(bid, cid) srtp_cryptosuite          dscp
                    call_ref   spid       conn_id_tx

16778224   -          125        N/A     N/A        rfc2833_pthru     confmsp   All RTPSPI
 Callegs      All MM-MSP Callegs      N/A                       N/A
                    -          -          -

16778224   16777232   126        g711u   20         rfc2833_pthru  s- rtpspi    (101,125)
               N/A                      AEAD_AES_256_GCM          184
                    30751576   16777219   -

16778224   16777231   124        g711u   20         rfc2833_pthru  s- rtpspi    (100,125)
               N/A                      AEAD_AES_256_GCM          184
                    30751576   16777219   -
```

```
Total number of active session(s) 1, connection(s) 2, and callegs 3
```

Verifying Call Information

To display call information for TDM and IVR calls stored in the Forwarding Plane Interface (FPI), use the **showvoipfpi calls** command. You can select a call ID and verify the cipher suite using the **show voip fpi calls confID** *call_id_number* command. In this example, cipher suite 6 is AES_256_GCM.

```
#show voip fpi calls
Number of Calls : 2
---------- ---------- ---------- ---------- --------------- ---------------
    confID correlator    AcallID     BcallID           state           event
---------- ---------- ---------- ---------- --------------- ---------------
         1          1         87         88       ALLOCATED DETAIL_STAT_RSP
        21         21         89         90       ALLOCATED DETAIL_STAT_RSP

#show voip fpi calls confID 1
--------------------------------------------------------------------------------
VoIP-FPI call entry details:
--------------------------------------------------------------------------------
Call Type        :           TDM_IP     confID          :                1
correlator       :                1     call_state      :        ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :      1796860810
modify_start_time:                0     delete_start_time:               0
Media Type(SideA):             SRTP     cipher suite    :                6
--------------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted             :         1
.........
```

Table 21: Feature Information for TLS 1.2 support on SCCP Gateways

Feature Name	Releases	Feature Information
Support for NGE Cipher Suites	Cisco IOS XE Cupertino 17.7.1a	This feature supports NGE cipher suites for secure voice signaling and secure media. These cipher suites are applicable for both the STCAPP analog phone and the SCCP DSPFarm conferencing service.

Support for Software Media Termination Point

The Software Media Termination Point (MTP) is a feature that enables Cisco Unified Communications Manager (CUCM) to facilitate media stream bridging and call relaying between diverse connection types.

- Bridges media streams between two connections.
- Allows CUCM to relay calls routed through SIP or H.323 endpoints, and
- Utilizes Skinny Client Control Protocol (SCCP) commands to establish an MTP for call signaling.

This feature is crucial for ensuring interoperability and proper media handling when different signaling protocols (like SIP, H.323, and SCCP) are involved in a call path within a Cisco Unified Communications environment.

Information about support for software media termination point

The extension of software MTP support to Cisco Unified Border Element (Enterprise) is a feature that

- Extends software MTP support to the Cisco Unified Border Element (Enterprise).
- Is an essential component for large-scale deployments of Cisco Unified Communications Manager (UCM), and
- Enables new capabilities for Cisco UBE to function as an Enterprise Edge Cisco Session Border Controller for large-scale SIP trunking deployments.

This enhancement is particularly important for organizations migrating to SIP trunking, as it ensures robust media handling and signaling capabilities at the enterprise edge.

How to configure support for software media termination point

Prerequisites

For the software MTP to function properly, codec and packetization must be configured the same way on both incoming call legs and outgoing call legs

Restrictions

- RSVP Agent is not supported in software MTP.
- Hardware MTP for repacketization is not supported.
- Call Threshold is not supported for standalone software MTP.
- Per-call debugging is not supported.

Configure support for software media termination point

To enable and configure the Support for Software Media Termination Point feature, perform these task.

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 these 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.

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.

Support for software media termination point is configured.

Configuration examples for software media termination point

Output examples for software media termination point.

This 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
```

Troubleshoot software termination point

To troubleshoot software termination point

To verify and troubleshoot this feature, use these **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 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
```

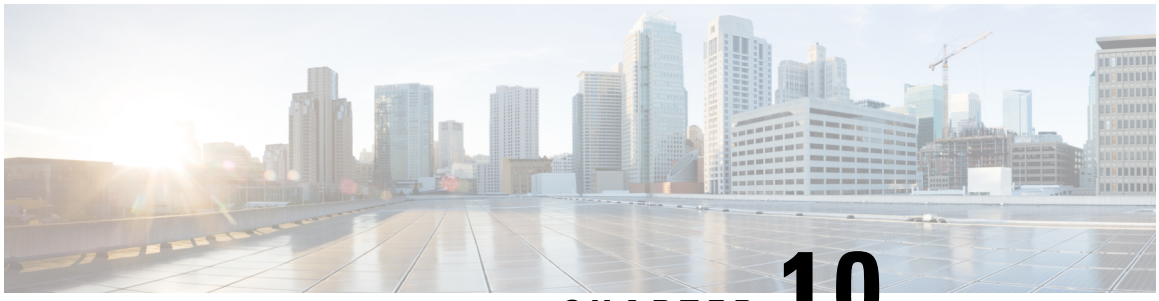
- To display information about RTP connections, use the **show rtpspi call** command:

```
Router#
               show rtpspi call
RTP Service Provider info:
No. CallId dstCallId Mode      LocalRTP RmtRTP LocalIP    RemoteIP   SRTP
    22     19        Snd-Rcv   7242     17510  0x90D080F  0x90D0814    0
    19     22        Snd-Rcv   18050    6900   0x90D080F  0x90D080F    0
```

- 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 are
  - **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**
- To isolate specific problems, use the **debug sccp** command:
  - **debug sccp** [**all** | **config** | **errors** | **events** | **keepalive** | **messages** | **packets** | **parser** | **tls**]



CHAPTER 10

Monitor and Troubleshoot

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.

About process management

You can access system messages by logging in to the console through Telnet protocol. You can monitor your system components remotely from any workstation that supports the Telnet protocol.

Process management refers to starting and monitoring software. 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 details about error messages

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.

INDEX