System Setup and Software Installation Guide for Cisco NCS 6000 Series Routers, Release 6.1.x

First Published: 2016-08-12

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

Preface

This Preface contains these sections:

Changes to This Document

This table lists the technical changes made to this document since it was first released.

Table 1: Changes to This Document

Date	Summary
November 2016	Republished for R6.1.2.
August 2016	Initial release of this document.

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

CHAPTER 1

New and Changed Feature Information

This topic summarizes the new and changed feature information for the *System Setup and Software Installation Guide for Cisco NCS 6000 Series Routers*.

- New and Changed Information, on page 1

New and Changed Information

Table 2: New and Changed Features

Feature	Description	Changed in Release	Where Documented
Named SDR XR Upgrade	This feature was introduced.	Release 6.1.2	*Perform System Upgrade and Install Feature Packages* chapter Named SDR XR Upgrade, on page 59

CHAPTER 2

Cisco NCS 6008 System Features

The topics covered in this chapter are:

Cisco NCS 6008 Product Overview

Cisco Network Convergence System 6000 Series

The Cisco Network Convergence System (NCS) 6000 Series System delivers outstanding network agility, packet optical convergence, and a system scale measured in petabits per second. It also facilitates the build-out of next-generation core to:

- support elastic capacity at the lowest total ownership cost
- deliver high-bandwidth mobile, video, and cloud services

Running the Cisco IOS XR operating system, Cisco's innovative virtualized operating environment, the Cisco NCS 6000 Series advances the concept of distributed routing and virtualization. With Cisco Virtualized IOS XR, the Cisco NCS 6000 Series brings new levels of programmability and virtualization to:

- enhance application service offerings
- increase provisioning speed
- optimize network economics

The Cisco NCS 6000 Series System is engineered for environmental efficiency, with the use of adaptable power consumption. The Cisco NCS 6000 Series System is powered by the Cisco nPower Network Processor Units (NPU). These technologies aid the Cisco NCS 6000 Series the lowest carbon footprint in service provider routing.

Cisco Network Convergence System 6008 Router

The Cisco NCS 6008 router, part of the Cisco NCS 6000 Series System, is the next-generation core router that provides industry-leading 8 Tbps of full-duplex network bandwidth through eight line cards.

The Cisco NCS 6008 router runs on Cisco IOS XR software, with Linux as the underlying host operating system. A Kernel-based Virtual Machine (KVM) hypervisor provides a virtualized environment to independently run system administration and routing functions on separate virtual machines. This provision makes the new system versatile and robust, providing immense flexibility for future expansion without the need for a complete system overhaul.

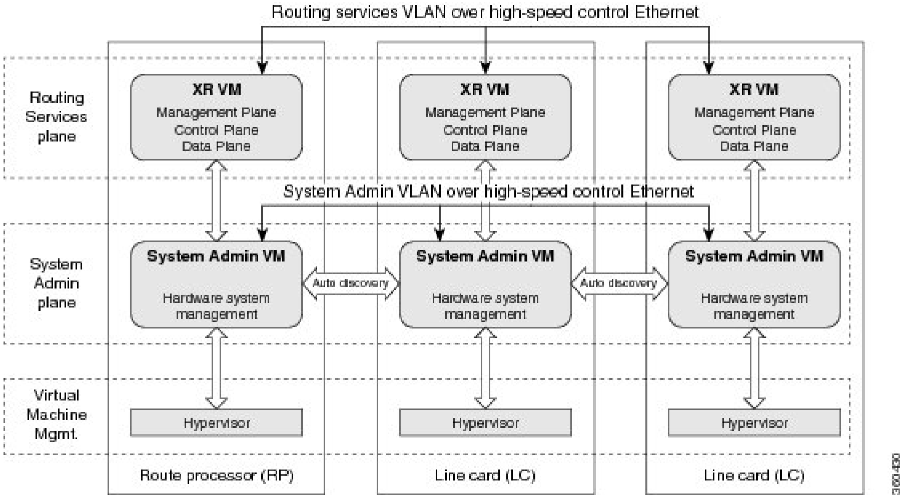
A multi-slice architecture of line cards enables the system to be configured to operate in a mixed operating mode, simultaneously supporting traffic at 10 Gbps and 100 Gbps on slice-level granularity.

Virtual Machine based Routing and System Administration

On the Cisco NCS Series router, the routing functions and the System Administration functions are run on separate virtual machines (VMs) over a Linux host operating system. The VMs simulate individual physical computing environments over a common hardware.. Available hardware resources, like processor, memory, hard disk, and so on, are virtualized and allocated to individual virtual machines by the hypervisor.

The VM topology on the Cisco NCS Series router is shown in this figure.

Figure 1: Virtualized IOS XR on Cisco NCS Series Router



Implementation of Virtualized IOS XR on Cisco NCS Series Router

- The hypervisor creates and manages individual VM environments.
- On every route processor (RP) and line card (LC) there are two VMs; one for system administration (System Admin VM) and one for managing the routing functions (XR VM).
- The two VMs on each node operate on their respective planes. On each plane, the VMs are connected to each other using a dedicated VLAN over a high-speed Control Ethernet connection.
- The System Admin VMs can detect each other's presence by auto discovery and thus maintain complete system awareness.

To access the XR VM, connect to the XR VM console port on the RP. To access the System Admin VM, in the XR VM CLI, execute the **admin** command.

Advantages of Virtualized IOS XR on the Cisco NCS Series Router

- Faster boot time—Because the System Admin functions are on a dedicated VM, the boot time is considerably reduced.
- Independent upgrades—Software packages can be independently installed on the System Admin VM and the XR VM, resulting in minimal system downtime.
- Self-starting VMs—Both the System Admin VM and the XR VM are automatically launched during router boot-up without any user intervention. They have a default set-up that is ready for use.
- System redundancy—In spite of their interconnectivity, there is also a level of isolation between the VMs. Therefore, if a particular VM experiences any issues, it does not affect the functioning of other VMs.

Command Modes

The Cisco NCS 6000 Series router runs on virtualized Cisco IOS XR software. Therefore, the CLI commands must be executed on virtual machines, namely the XR VM and the System Admin VM. This table lists the command modes for the VMs.

Command Mode	Description
XR EXEC mode (XR VM execution mode)	Run commands on the XR VM to display the operational state of the entire secure domain router (SDR). Example: `RP/0/RP0/CPU0:router#`

XR Config mode
(XR VM configuration mode)
	Perform security, routing, and other XR feature configurations on the XR VM.
	Example:
	`RP/0/RP0/CPU0:router#`**`configure`**
	`RP/0/RP0/CPU0:router(config)#`

System Admin EXEC mode
(System Admin VM execution mode)
	Run commands on the System Admin VM to display and monitor the operational state of the router hardware. The chassis or individual hardware modules can be reloaded from this mode.
	Example:
	`RP/0/RP0/CPU0:router#`**`admin`**
	`sysadmin-vm:0_RP0#`

System Admin Config mode
(System Admin VM configuration mode)
	Run configuration commands on the System Admin VM to manage and operate the hardware modules of the entire chassis.
	Example:
	`RP/0/RP0/CPU0:router#`**`admin`**
	`sysadmin-vm:0_RP0#`**`config`**
	`sysadmin-vm:0_RP0(config)#`

System Setup Workflow

The system setup of the Cisco NCS 6008 Series router involves these stages:

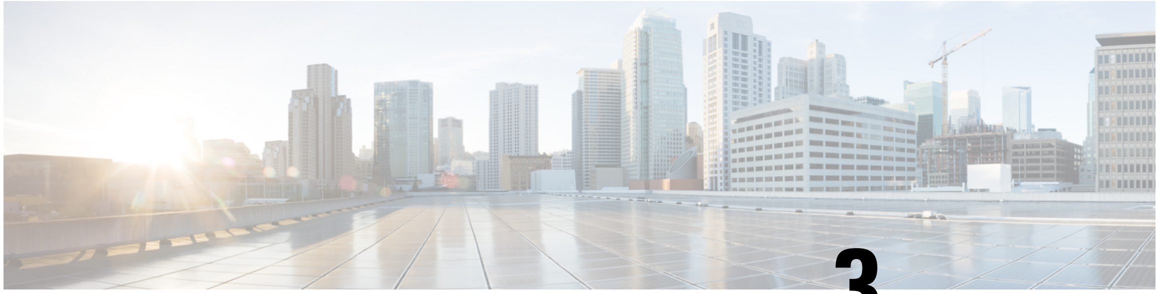
1. Bring-up the Cisco NCS 6008 Router, on page 7—Connect to the router's console and boot-up the router. After booting is complete, specify the root username and password.

2. Perform Preliminary Checks, on page 25—Perform basic verification of the router's default setup. This ensures that, if any setup issue is detected, corrective action is taken at an early stage.

3. Create User Profiles and Assign Privileges, on page 41—Create users and assign privileges, as needed. Privileges are defined by data rules and command rules that are applied to users. Users are either permitted, or denied, the use of certain commands based on assigned privileges.

4. Perform System Upgrade and Install Feature Packages, on page 53—Upgrade the operating system, if the default is not the latest version. Also, install relevant packages to deploy additional features and software patches on the router.

5. Perform Disaster Recovery, on page 77—In the event of a router boot failure due to image corruption, boot the router using an external bootable USB drive.



CHAPTER 3

Bring-up the Cisco NCS 6008 Router

After installing the hardware, boot the Cisco NCS 6008 Series Router . Connect to the XR VM console port and power on the router. The routersystem completes the boot process using the pre-installed operating system (OS) image. If no image is available within the router, the router can be booted using an external bootable USB drive.

After booting is complete, create the root username and password, and then use it to log on to the XR VM console and get the router prompt. From the XR VM console, access the System Admin VM console to configure system administration settings.

For more information about completing the hardware installation, see Cisco Network Convergence System 6000 Series Routers Hardware Installation Guide.

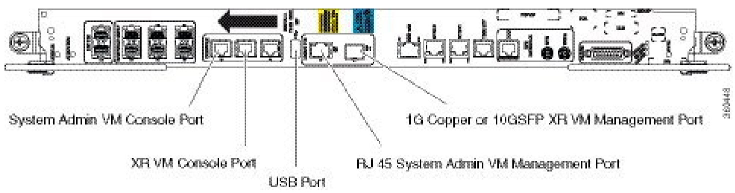
The topics covered in this chapter are:

Connect to the XR VM Console Port and Power the Router

Use the XR VM console port on the Route Processor (RP) to connect to a new router . If required, subsequent connections can be established through the management port, after it is configured.

There are the three console ports on the RP. Console port 2 is for the XR VM.

Figure 2: XR VM console port of the RP


System Admin VM Console Port
1G Copper or 10GSFP XR VM Management Port
XR VM Console Port
RJ 45 System Admin VM Management Port
USB Port
360448

Step 1 Connect a terminal to the XR VM console port of the RP.

Step 2 Start the terminal emulation program on your workstation.

The console settings are 115200 bps, 8 data bits, 1 stop bit and no parity.

Step 3 Power on the router.

Press the power switch up to turn on the power shelves. As the router boots up, you will see boot process details on the console screen of the terminal emulation program.

Step 4 Press **Enter**.

When the system prompts you to enter the root-system username, it indicates that the boot process is complete. If the prompt does not appear, wait for a while to give the router more time to complete the initial boot procedure, then press **Enter**.

Important If the boot process fails, it may be because the pre-installed image on the router is corrupt. In this case, the router can be booted using an external bootable USB drive. For details see, Create Bootable USB Drive Using Shell Script, on page 83 and Boot the Router Using USB, on page 85.

What to do next

Specify the root username and password.

Setup Root User Credentials and Login to XR VM Console

When the router boots for the first time, the system prompts the user to configure root credentials (username and password). These credentials are configured as the root user on the XR VM (root-lr), the System Admin VM (root-system), and as disaster-recovery credentials. In addition to the XR VM console, the System Admin VM console and the XR VM management port can be accessed using these credentials.

Before you begin

The boot process must be complete. For details on how to initiate the boot process, see Connect to the XR VM Console Port and Power the Router, on page 7.

SUMMARY STEPS

1. **Enter root-system username:** *username*
2. **Enter secret:** *password*
3. **Enter secret again:** *password*
4. **Username:** *username*
5. **Password:** *password*
6. (Optional) **show run username**

DETAILED STEPS

Step 1 **Enter root-system username:** *username*

Example:

```
Enter root-system username: root
```

Enter the username of the root user. The character limit is 1023. In this example, the name of the root user is "root".

Important The specified username is mapped to the "root-lr" group on the XR VM. It is also mapped as the "root-system" user on the System Admin VM.

When starting the router for the first time, or after a re-image, the router does not have any user configuration. In such cases, the router prompts you to specify the "root-system username". However, if the router has been configured previously, the router prompts you to enter the "username", as described in Step 4.

Step 2 **Enter secret:** *password*

Example:

```
Enter secret:
```

Enter the password for the root user. The character limit is 253. The password you type is not displayed on the CLI for security reasons.

The root username and password must be safeguarded as it has the superuser privileges. It is used to access the complete router configuration.

Step 3 **Enter secret again:** *password*

Example:

```
Enter secret again:
```

Re-enter the password for the root user. The password is not accepted if it does not match the password entered in the previous step. The password you type is not displayed on the CLI for security reasons.

Step 4 **Username:** *username*

Example:

```
Username: root
```

Enter the root-system username to login to the XR VM console.

Step 5 **Password:** *password*

Example:

```
Password:
```

Enter the password of the root user. The correct password displays the XR VM router prompt.

```
RP/0/RP0/CPU0:router#
```

You are now logged into the XR VM console.

Step 6 (Optional) **show run username**

Example:

RP/0/RP0/CPU0:router#show run username

Displays user details.

```
username root
 group root-lr
 group cisco-support
 secret 5 $1$NBg7$fHs1inKPZVvzqxMv775UE/
!
```

What to do next

- Configure routing functions from the XR VM.
- Configure system administration settings from the System Admin prompt. The System Admin prompt is displayed on accessing the System Admin VM console. For details on how to get the System Admin prompt, see Access the System Admin VM Console, on page 10.

Access the System Admin VM Console

All system administration and hardware management setups are performed from the System Admin VM.

Step 1 Login to the XR VM console as the root user.

Step 2 **admin**

Example:

The following example shows the command output :

```
RP/0/RP0/CPU0:router#admin

Mon May 22 06:57:29.350 UTC

root connected from 127.0.0.1 using console on host
sysadmin-vm:0_RP0# exit
Mon May  22 06:57:32.360 UTC
```

After you enter the System Admin VM console, the router prompt changes to

```
sysadmin-vm:0_RP0#
```

Step 3 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters System Admin Config mode.

Step 4 (Optional) **exit**

Example:

```
sysadmin-vm:0_RP0#exit
```

Return to the XR VM CLI from the System Admin VM CLI.

Alternate Method to Access the System Admin VM

Instead of executing the **admin** command, you can access the System Admin prompt by directly connecting to the System Admin VM console port. Console port 1 on the RP is for System Admin VM. While connecting to the System Admin VM console port, enter the System Admin username and password, when prompted. For more details about System Admin VM username and password, see the chapter Create User Profiles and Assign Privileges, on page 41.

Important It is not possible to access the XR VM through the System Admin VM console port.

Configure the XR VM Management Port

To use the XR VM Management port for system management and remote communication, you must configure an IP address and a subnet mask for the management ethernet interface. To communicate with devices on other networks (such as remote management stations or TFTP servers), you need to configure a default (static) route for the router .

Before you begin

- Consult your network administrator or system planner to procure IP addresses and a subnet mask for the management interface.
- Physical port Ethernet 0 on RP is the management port. Ensure that the port is connected to management network.

SUMMARY STEPS

1. **configure**
2. **interface MgmtEth** *rack/slot/***CPU0***/port*
3. **ipv4 address** *ipv4-address subnet-mask*
4. **ipv4 address** *ipv4 virtual address subnet-mask*
5. **no shutdown**
6. **exit**
7. **router static address-family ipv4 unicast** *0.0.0.0/0 default-gateway*
8. **commit**

DETAILED STEPS

Step 1 **configure**

Step 2 **interface MgmtEth** *rack/slot/***CPU0***/port*

Example:

```
RP/0/RP0/CPU0:router(config)#interface mgmtEth 0/RP0/CPU0/0
```

Enters interface configuration mode for the management interface of the primary RP.

Step 3 **ipv4 address** *ipv4-address subnet-mask*

Example:

```
RP/0/RP0/CPU0:router(config-if)#ipv4 address 10.1.1.1 255.0.0.0
```

Assigns an IP address and a subnet mask to the interface.

Step 4 **ipv4 address** *ipv4 virtual address subnet-mask*

Example:

```
RP/0/RP0/CPU0:router(config-if)#ipv4 address 1.70.31.160 255.255.0.0
```

Assigns a virtual IP address and a subnet mask to the interface.

Step 5 **no shutdown**

Example:

```
RP/0/RP0/CPU0:router(config-if)#no shutdown
```

Places the interface in an "up" state.

Step 6 **exit**

Example:

```
RP/0/RP0/CPU0:router(config-if)#exit
```

Exits the Management interface configuration mode.

Step 7 **router static address-family ipv4 unicast** *0.0.0.0/0 default-gateway*

Example:

```
RP/0/RP0/CPU0:router(config)#router static address-family ipv4 unicast 0.0.0.0/0 12.25.0.1
```

Specifies the IP address of the default-gateway to configure a static route; this is to be used for communications with devices on other networks.

Step 8 **commit**

What to do next

Connect to the management port to the ethernet network. See Connecting to the XR VM Management Port, on page 12.

Connecting to the XR VM Management Port

The XR VM management port supports 10/100G optical small form-factor pluggable (SFP) units to provide high speed network connectivity. The SFPs that can be connected to the XR VM management port are:

SFP module	Datasheet
Cisco SFP-10G-SR	http://www.cisco.com/en/US/prod/collateral/modules/ps5455/data_sheet_c78-455693.html
Cisco SFP-10G-LR	

SFP module	Datasheet
1000BASE-SX SFP	http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6577/product_data_sheet0900aecd8033f885.html
1000BASE-LX/LH SFP	
1000BASE-T SFP	

Before you begin

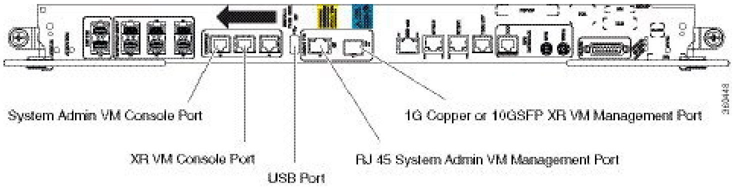
Configure the management port. See Configure the XR VM Management Port, on page 11.

Step 1 Connect the SFP module to the XR VM management port.

The XR VM management port on the RP is shown in this figure.

Note RJ-45 port is disabled by default. Do not use the RJ-45 port. Use only the 1G copper SFP port as shown in the image below.

Figure 3: XR VM console port of the RP


System Admin VM Console Port
1G Copper or 10GSFP XR VM Management Port
260448
XR VM Console Port
RJ 45 System Admin VM Management Port
USB Port

Step 2 Depending on the SFP module type, connect either a optical fiber or an ethernet cable to the SFP.

What to do next

With a terminal emulation program, establish a SSH or telnet connection to the management interface port using its IP address. For details on configuring the IP address of the management port, see Configure the XR VM Management Port, on page 11.

Before establishing a telnet session, use the **telnet ipv4|ipv6 server max-servers** command in the XR Config mode, to set number of allowable telnet sessions to the router.

Note Telnet supports a maximum of 100 (including both IPv4 and IPv6) sessions.

For a SSH connection, the *ncs6k-k9sec* package must be installed on the router. For details about package installation, see Install Packages, on page 55.

Provision Breakout Interfaces

The NCS 6000 line cards have multi-slice architecture. On a 10X100G line card, each slice has two 100 GE ports that can be configured to operate at 100 GE or 10X10 GE. Breakout cables are connected to the 10X10GE interfaces. The 100G ports are mapped to each slice as:

Ports	Slice
0 and 1	0
2 and 3	1
4 and 5	2
6 and 7	3
8 and 9	4

SUMMARY STEPS

1. **configure**
2. **hw-module location** *rack/slot/CPU* **slice** *slice_number* **breakout 10G**
3. **commit**

DETAILED STEPS

Step 1 **configure**

Step 2 **hw-module location** *rack/slot/CPU* **slice** *slice_number* **breakout 10G**

Example:

```
RP/0/RP0/CPU0:router(config)#hw-module location 0/1/CPU0 slice 1 breakout 10G
```

Provisions the interfaces on the specified slice in the 10G breakout mode.

Step 3 **commit**

What to do next

Run the **show ipv4 interface brief** command in the XR EXEC mode to view breakout interfaces. Each 10 GE interface is represented as **TenGigE**<*rack_num*>/<*slot_id*>/<*card_instance*>/<*port_num*>/<*breakout_num*>.

Verify that ten TenGigE interfaces are created for every HundredGigE interface of the slice on which the breakout is configured.

```
RP/0/RP0/CPU0:router(config)#show ipv4 interface brief
Interface                      IP-Address      Status         Protocol Vrf-Name
Bundle-Ether1                  199.1.1.1       Up              Up       default
Loopback0                      100.100.100.100 Up              Up       default
Loopback10                     unassigned      Up              Up       default
Loopback11                     unassigned      Up              Up       default
Loopback12                     unassigned      Up              Up       default
Loopback13                     unassigned      Up              Up       default
....
MgmtEth0/RP1/CPU0/0            4.15.10.145     Up              Up       default
HundredGigE0/0/0/0             unassigned      Up              Up       default
HundredGigE0/0/0/1             unassigned      Up              Up       default
HundredGigE0/0/0/2             unassigned      Up              Up       default
HundredGigE0/0/0/3             unassigned      Up              Up       default
HundredGigE0/0/0/4             10.0.4.1        Up              Up       default
```

```
....
TenGigE0/1/0/0              10.1.0.1       Up             Up       default
TenGigE0/1/0/1              10.1.1.1       Up             Up       default
TenGigE0/1/0/2              10.1.2.1       Up             Up       default
TenGigE0/1/0/3              10.1.3.1       Up             Up       default
TenGigE0/1/0/4              10.1.4.1       Up             Up       default
....
```

Shut Down Unused Linecard Slices

The NCS 6000 linecards, namely, NCS 6000 10x100G Multi-Service CPAK, NCS 6000 10x100G Multi-Service CXP, and NCS 6000 60x10GE PAT, have multi-slice architecture. The 10X100G line cards has 5 slices, whereas the 60X10G line cards has 4 slices. Each slice can be individually shut down:

- To save power- Shutting down a slice will power down the slice. This will reduce the power consumption of that line card. The mode of operating line cards with one or more slices shut is called the green mode.
- For troubleshooting - If a slice is malfunctioning, shutting it down isolates the slice from the system, thus reducing its impact on the router. Also, troubleshooting can be done within the domain of the slice.

SUMMARY STEPS

1. **configure**
2. **hw-module location** *rack/slot/CPU* **slice** *slice_number* **shutdown**
3. **commit**

DETAILED STEPS

Step 1 **configure**

Step 2 **hw-module location** *rack/slot/CPU* **slice** *slice_number* **shutdown**

Example:

```
RP/0/RP0/CPU0:router(config)#hw-module location 0/1/CPU0 slice 3 shutdown
```

Shuts down the specified slice. The interfaces belonging to the slice that is shut down are deleted from the system and are not visible in the output of the **show interfaces brief** command.

Step 3 **commit**

What to do next

To make a shutdown slice operational, use the **no hw-module location** *rack/slot/CPU* **slice** *slice_number* **shutdown** command.

Verify the slice shut down using **show platform** in XR VM or **show platform slices** in System Admin VM.

Perform Clock Synchronization with NTP Server

There are independent system clocks for the XR VM and the System Admin VM. To ensure that these clocks do not deviate from true time, they need to be synchronized with the clock of a NTP server. In this task you will configure a NTP server for the XR VM. After the XR VM clock is synchronized, the System Admin VM clock will automatically synchronize with the XR VM clock.

Before you begin

Configure and connect to the XR VM management port.

SUMMARY STEPS

1. **configure**
2. **ntp server** *server_address*
3. **commit**
4. **exit**
5. **sh run ntp**

DETAILED STEPS

Step 1 **configure**

Step 2 **ntp server** *server_address*

Example:

The XR VM clock is configured to be synchronized with the specified sever.

```
RP/0/RP0/CPU0:router#ntp server 64.90.182.55
```

The System Admin VM clock is configured to be synchronized with the specified sever.

```
sysadmin-vm:0_RP0#ntp server 64.90.182.55
```

Step 3 **commit**

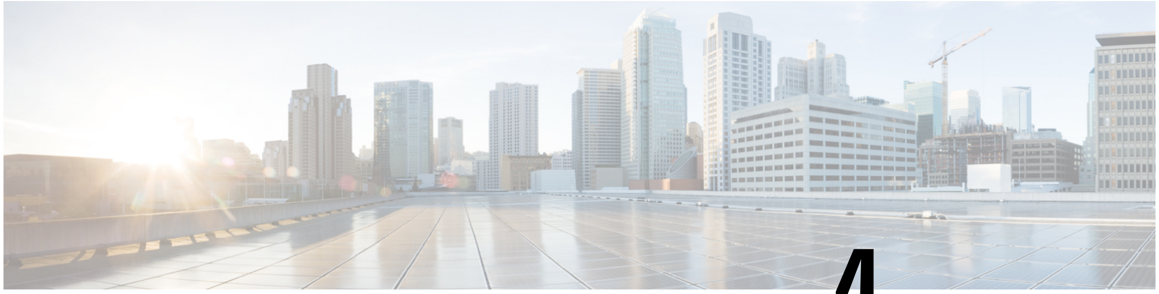
Step 4 **exit**

Step 5 **sh run ntp**

Example:

```
RP/0/RP0/CPU0:router#sh run ntp

ntp
server 202.153.144.25
!
```



CHAPTER 4

Setup Multi-chassis Configuration

Multiple Network Convergence System (NCS) 6008 single chassis can be connected using NCS 6000 fabric card chassis to form a multi-chassis system. This provides high scale of interfaces with single admin and control plane.

The multi-chassis system consists of two types of chassis:

- Line card chassis (LCC)
- Fabric card chassis (FCC)

Multi-chassis system is built with one or more LCC connected to FCCs, with a maximum hardware configuration of 16 LCC and a set of 4 FCC. The LCC has 8 line card slots and 6 fabric card slots, each fabric slot representing a logical fabric plane. The system provides 8 Tbps of full-duplex network bandwidth through eight line cards. The FCC hosts the agnostic fabric cards (FC). Each FCC can have 12 FC slots. The fabric cards used in a single chassis setup is different from the fabric cards used in the multi-chassis system. All the LCCs are connected to the FCC, and traffic flows from one LCC to another LCC through the FCC.

To form a multi-chassis system, two types of connectivity must be established:

- Control ethernet connectivity: The racks are interconnected to form a network. The shelf controller (SC) cards and route processor (RP) cards have two control ethernet ports - port 0 and port 1. These ports are connected to two switches that are in-turn connected using 40G trunk ports.
- Fabric connectivity: The FCC and LCC are connected to form a fabric plane.

After the hardware components are installed, and connectivity is established between the racks, you can setup a multi-chassis system.

The workflow for setting up a multi-chassis system is represented in this flow chart:

Note This workflow image has clickable links that are enabled only in the HTML format (and not in the PDF format) of this document.

Figure 4: Multi-chassis Configuration Interactive Workflow

Assign Rack Number to Chassis

In a multi-chassis system, each chassis must have a unique rack number. This rack number is used to identify a chassis in the system.

Complete this task to identify the chassis and its connections and to establish a multi-chassis network:

Before you begin

- Install the hardware components of the multi-chassis system. In Line card chassis (LCC), line cards, fabric cards, and route processors are installed, and in Fabric card chassis (FCC), fabric cards (FC), shelf-controller switch cards (SC-SW) and shelf controllers (SC) are installed.
- Connect the chassis in the multi-chassis system using control ethernet cables. The control ethernet network provides inter-connectivity between chassis, and a two-way management ethernet path from System Admin and XR VM console. For more information see Cabling the Ethernet Control Plane Network section in the Cisco Network Convergence System 6000 Fabric Card Chassis Hardware Installation Guide.
- The fabric cards on the LCC and FCC are connected using fabric cables. This is used for data traffic. For more information see Cabling the Fabric section in the Cisco Network Convergence System 6000 Fabric Card Chassis Hardware Installation Guide.

SUMMARY STEPS

1. **admin**
2. **show chassis**
3. **config**
4. **chassis serial <chassis serial number>**
5. **rack <rack number>**
6. Repeat step 3 to 5 for all the chassis in the multi-chassis system.
7. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters System Admin EXEC mode.

Step 2	**show chassis**
	Example:
	The following example shows a 2 + 2 (2 LCC and 2 FCC) configuration:
	`sysadmin-vm:0_RP0#show chassis`
	`Wed Jun  4  17:18:22.498 UTC`
		Shows the chassis details including the chassis serial number.
		Identify the serial numbers for which rack numbers are to be assigned.

	Command or Action	Purpose

```
Serial Num    Rack Num    Rack Type   Rack State
 Data Plane  Ctrl Plane

FMP12020050   0           LCC         UP
 CONN        CONN
FMP12260408   F1          FCC         UP
 CONN        CONN
FMP16320213   1           LCC         UP
 CONN        CONN
FMP17260334   F0          FCC         UP
 CONN        CONN
```

The following example shows a 4 + 2 (4 LCC and 2 FCC)configuration:

```
sysadmin-vm:0_RP0#show chassis
Wed Jun  4  17:18:22.498 UTC
Serial Num    Rack Num    Rack Type   Rack State
 Data Plane  Ctrl Plane

FLM17326A2K   0           LCC         OPERATIONAL
  CONN        CONN
FLM17326A2J   1           LCC         OPERATIONAL
  CONN        CONN
FLM17386E28   2           LCC         OPERATIONAL
  CONN        CONN
FLM17075XWM   3           LCC         OPERATIONAL
  CONN        CONN
FMP17210228   F0          FCC         OPERATIONAL
  CONN        CONN
FMP17380420   F1          FCC         OPERATIONAL
  CONN        CONN
```

	Command or Action	Purpose
Step 3	**config** **Example:** `sysadmin-vm:0_RP0#config`	Enters the configuration mode.
Step 4	**chassis serial <chassis serial number>** **Example:** `sysadmin-vm:0_RP0(config)# chassis serial FMP12020050`	Enters the configuration mode for the chassis serial number.
Step 5	**rack <rack number>** **Example:** `sysadmin-vm:0_RP0(config-serial-FMP12020050)# rack 0`	Type a rack number to associate the rack number to the chassis.
Step 6	Repeat step 3 to 5 for all the chassis in the multi-chassis system.	
Step 7	**commit**	

What to do next

Perform preliminary checks to verify that the chassis is configured correctly:

- After configuring the chassis serial number, verify that a unique rack number is assigned for each chassis serial number using the **show running-config chassis serial** command in System Admin EXEC mode.

  The following example shows a 2+2 configuration:

  ```
  sysadmin-vm:0_RP0# show running-config chassis serial
  chassis serial FMP12020050
   rack 0
  !
  chassis serial FMP12260408
   rack F1
  !
  chassis serial FMP16320213
   rack 1
  !
  chassis serial FMP17260334
   rack F0
  ```

  The following example shows a 4+2 configuration:

  ```
  sysadmin-vm:0_RP0# show running-config chassis serial
  chassis serial FLM17326A2K
   rack 0
  !
  chassis serial FLM17326A2J
   rack 1
  !
  chassis serial FLM17386E28
   rack 2
  !
  chassis serial FLM17075XWM
   rack 3
  !
  chassis serial FMP17210228
   rack F0
  !
  chassis serial FMP17380420
   rack F1
  ```

- After the rack numbers are assigned to the chassis serial number, verify that all the cards are operational, and XR VM is running on all the cards. For details, see Verify SDR Information, on page 36.

- If the XR VM is not running, no output is shown for that location in the result. In this case, verify the state of secure domain router (SDR) on the node using the **show sdr** command in System Admin EXEC mode. For details, see Verify SDR Information, on page 36.

- After the system has booted, all available interfaces must be discovered by the system. View the number of discovered interfaces using the **show interfaces summary** command. For details, see Verify Interface Status, on page 34

After verifying that the cards in LCC are operational, configure the fabric cards in FCC.

Associate Fabric Card in Fabric Card Chassis to Fabric Plane

The fabric cards in the fabric card chassis (FCC) must be associated to a fabric plane in the multi-chassis system. The system fabric is divided into six fabric planes that are used to evenly distribute traffic across the fabric. The location of each fabric card in the fabric plane is identified by an instance number. The instance number starts from 0 and are sequential.

For information on multi-chassis configurations and cabling, see Cabling a Multi-Chassis Configuration in the Cisco Network Convergence System 6000 Fabric Card Chassis Hardware Installation Guide.

SUMMARY STEPS

1. **admin**
2. **config**
3. **controller fabric plane <plane number>**
4. **instance <instance-number>**
5. **location <fabric-chassis-number/fabric-card-number>**
6. Repeat step 3 to step 5 to associate all fabric cards to an instance in the fabric plane.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters System Admin EXEC mode.
Step 2	**config** **Example:** `sysadmin-vm:0_RP0#config`	Enter System Admin Config mode.
Step 3	**controller fabric plane <plane number>** **Example:** `sysadmin-vm:0_RP0(config)# controller fabric plane 4`	Enter configuration mode for the specified fabric plane.
Step 4	**instance <instance-number>** **Example:** `sysadmin-vm:0_RP0(config-plane-4)# instance 0`	Specify the instance number to which the fabric card is to be mapped.
Step 5	**location <fabric-chassis-number/fabric-card-number>** **Example:** `sysadmin-vm:0_RP0(config-instance-0)# location F0/FC8`	Associate the location of the fabric card in FCC with an instance in a fabric plane.
Step 6	Repeat step 3 to step 5 to associate all fabric cards to an instance in the fabric plane.	

What to do next

Perform preliminary checks to verify that the fabric card chassis is configured correctly:

- After associating the fabric card in FCC to a fabric plane, verify the mapping of fabric plane to an instance. The following is an example of a topology with two instances:

```
sysadmin-vm:0_RP0# show running-config controller fabric
```

```
controller fabric plane 0
  instance 0
    location F0/FC0
  instance 1
    location F1/FC0
  !
!
controller fabric plane 1
   instance 0
      location F0/FC1
   instance 1
      location F1/FC1
   !
!
controller fabric plane 2
  instance 0
    location F0/FC2
  instance 1
    location F1/FC2
  !
!
controller fabric plane 3
   instance 0
      location F0/FC3
   instance 1
      location F1/FC3
   !
!
controller fabric plane 4
  instance 0
    location F0/FC4
  instance 1
    location F1/FC4
  !
!
controller fabric plane 5
   instance 0
      location F0/FC5
   instance 1
      location F1/FC5
   !
!
```

- After all the fabric cards are mapped to an instance in the plane, verify that all the fabric planes are up. For details, see Verify Fabric Plane, on page 35.
- Verify the switch summary. For details, see Verify Control Ethernet Connections, on page 37

The multi-chassis system is setup.

CHAPTER 5

Perform Preliminary Checks

After successfully logging into the XR VM console, you must perform some preliminary checks to verify the default setup. If any setup issue is detected when these checks are performed, take corrective action before making further configurations. These preliminary checks are:

Verify Active VMs

On the router both the XR VM and the System Admin VM must be operational. Instances of both VMs should be running on every RP and LC . Complete this task to verify the VMs are active.

SUMMARY STEPS

1. **admin**
2. **show vm**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **show vm**

Example:

```
sysadmin-vm:0_RP0#show vm
sysadmin-vm:0_RP1# sh vm

Location: 0/0
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.64.1       NA/NA
default-sdr       running       192.0.64.3       1528/1528

Location: 0/1
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.68.1       NA/NA
default-sdr       running       192.0.68.3       1528/1528

Location: 0/2
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.72.1       NA/NA
default-sdr       running       192.0.72.3       1528/1528

Location: 0/3
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.76.1       NA/NA
default-sdr       running       192.0.76.3       1528/1528

Location: 0/4
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.80.1       NA/NA
default-sdr       running       192.0.80.3       1528/1528

Location: 0/5
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.84.1       NA/NA
default-sdr       running       192.0.84.3       1529/1529

Location: 0/6
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.88.1       NA/NA
default-sdr       running       192.0.88.3       1531/1531

Location: 0/7
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.92.1       NA/NA
default-sdr       running       192.0.92.3       1531/1531

Location: 0/RP0
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.0.1        NA/NA
default-sdr       running       192.0.0.4        29736/29736

Location: 0/RP1
Id                Status        IP Address       HB Sent/Recv
-------------------------------------------------------------
sysadmin          running       192.0.4.1        NA/NA
default-sdr       running       192.0.4.4        30534/30534
```

Displays the status of the VMs running on various nodes.

```
------ VMs found at location 0/3 ------
  Id     : sysadmin
  Status : running
  IP Addr: 192.0.76.1
  HB Interval : 0s 0ns
  Last HB Sent: 2026
  Last HB Rec : 2026
  -------
  Id     : default-sdr
  Status : running
  IP Addr: 192.0.76.3
  HB Interval : 10s 0ns
  Last HB Sent: 2026
  Last HB Rec : 2026
  -------
------ VMs found at location 0/RP0 ------
  Id     : sysadmin
  Status : running
  IP Addr: 192.0.0.1
  HB Interval : 0s 0ns
  Last HB Sent: 40660
  Last HB Rec : 40659
  -------
  Id     : default-sdr
  Status : running
  IP Addr: 192.0.0.4
  HB Interval : 0s 500000000ns
  Last HB Sent: 40708
  Last HB Rec : 40707
  -------
------ VMs found at location 0/RP1 ------
  Id     : sysadmin
  Status : running
  IP Addr: 192.0.4.1
  HB Interval : 0s 0ns
  Last HB Sent: 40708
  Last HB Rec : 40708
  -------
  Id     : default-sdr
  Status : running
  IP Addr: 192.0.4.4
  HB Interval : 0s 500000000ns
  Last HB Sent: 40708
  Last HB Rec : 40708
  -------
```

In the above result:

- Id—Name of the VM. "sysadmin" represents System Admin VM; "default-sdr" represents XR VM
- Status—Status of the VM
- IP Addr—Internal IP address of the VM

If a VM is not running on a node, in the output of the **show vm** command, no output is shown for that node.

What to do next

If the XR VM is not running on a node, try reloading the node. To do so, use the **hw-module location** *node-id* **reload** command in the System Admin EXEC mode. Also, use the **show sdr** command in the System Admin EXEC mode to verify that the SDR is running on the node.

Verify Status of Hardware Modules

Hardware modules include RPs, LCs, fan trays, fabric cards, and so on. On the router, multiple hardware modules are installed. Perform this task to verify that all hardware modules are installed correctly and are operational.

Before you begin

Ensure that all required hardware modules have been installed on the router. For installation details, see Cisco Network Convergence System 6000 Series Routers Hardware Installation Guide.

SUMMARY STEPS

1. **admin**
2. **show hw-module** *fpd location*

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **show hw-module** *fpd location*

Displays the list of hardware modules detected on the router.

```
LOCATION  SHOW
----------------
0/RP0     -
0/RP1     -
0/FC0     -
0/FT0     -
0/FT1     -
0/3       -
0/PT1     -
```

From the result, verify that all the hardware modules installed on the chassis are listed. If a module is not listed, it indicates either that module is malfunctioning, or it is not properly installed. Remove and reinstall the hardware module.

Verify Node Status

Each card on the router represents a node. The operational status of the node is verified using the **show platform** command. This command is to be executed independently from both XR VM and System Admin VM CLIs.

For the multi-chassis system, run the command from one chassis. The verification commands will list information for all chassis.

SUMMARY STEPS

1. **sh platform**
2. **admin**
3. **show platform**

DETAILED STEPS

Step 1 **sh platform**

Example:

```
RP/0/RP0/CPU0:router#sh platform
```

The **show platform** command when executed from the XR EXEC mode displays the status of XR VM running on various RPs and LCs.

This is an example for single-chassis system:

```
RP/0/RP1/CPU0:#sh platform
Mon Feb 13 15:07:03.729 UTC
Node              Type                       State             Config state
--------------------------------------------------------------------------------
0/0/CPU0          NC6-10X100G-M-K            IOS XR RUN        NSHUT
0/0/NPU0          Slice                      UP
0/0/NPU1          Slice                      UP
0/0/NPU2          Slice                      UP
0/0/NPU3          Slice                      UP
0/0/NPU4          Slice                      UP
0/1/CPU0          NC6-60X10GE-L-S            IOS XR RUN        NSHUT
0/1/NPU0          Slice                      UP
0/1/NPU1          Slice                      UP
0/1/NPU2          Slice                      UP
0/1/NPU3          Slice                      UP
0/2/CPU0          NC6-10X100G-M-K            IOS XR RUN        NSHUT
0/2/NPU0          Slice                      UP
0/2/NPU1          Slice                      UP
0/2/NPU2          Slice                      UP
0/2/NPU3          Slice                      UP
0/2/NPU4          Slice                      UP
0/3/CPU0          NC6-10X100G-M-K            IOS XR RUN        NSHUT
0/3/NPU0          Slice                      UP
0/3/NPU1          Slice                      UP
0/3/NPU2          Slice                      UP
0/3/NPU3          Slice                      UP
0/3/NPU4          Slice                      UP
0/4/CPU0          NC6-2/10X100G-L-K          IOS XR RUN        NSHUT
```

```
0/4/NPU0          Slice                      UP
0/4/NPU1          Slice                      UP
0/4/NPU2          Slice                      UP
0/4/NPU3          Slice                      UP
0/4/NPU4          Slice                      UP
0/5/CPU0          NC6-10X100G-M-K            IOS XR RUN        NSHUT
0/5/NPU0          Slice                      UP
0/5/NPU1          Slice                      UP
0/5/NPU2          Slice                      UP
0/5/NPU3          Slice                      UP
```

This is an example for multi-chassis system:

```
Node            Type            PLIM            State           Config State
-----------------------------------------------------------------------------
1/RP1/CPU0      RP(Standby)     N/A             IOS XR RUN      PWR,NSHUT,MON
1/7/CPU0        LC              GE              IOS XR RUN      PWR,NSHUT,MON
0/RP1/CPU0      RP(Standby)     N/A             IOS XR RUN      PWR,NSHUT,MON
0/RP0/CPU0      RP(Active)      N/A             IOS XR RUN      PWR,NSHUT,MON
0/0/CPU0        LC              GE              IOS XR RUN      PWR,NSHUT,MON
1/0/CPU0        LC              GE              IOS XR RUN      PWR,NSHUT,MON
0/7/CPU0        LC              GE              IOS XR RUN      PWR,NSHUT,MON
1/RP0/CPU0      RP(Active)      N/A             IOS XR RUN      PWR,NSHUT,MON
RP/0/RP0/CPU0:MCDT3#
```

Verify that all RPs and LCs are listed and their state is "IOS XR RUN". This indicates that the XR VM is operational on the cards.

If the XR VM is not running, no output is shown for that location in the result. In this case, verify the state of SDR on the node using the **show sdr** command in the System Admin EXEC mode. For details, see Verify SDR Information, on page 36. Also, verify that the node state is "OPERATIONAL" in the result of **show platform** command in the System Admin EXEC mode, as described in Step 3.

Step 2 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 3 **show platform**

Example:

```
sysadmin-vm:0_RP0#show platform
```

The **show platform** command when executed from the System Admin EXEC mode displays the status of all hardware units like cards (RPs, LCs, and FCs), and hardware modules (fan trays) on the router.

This is an example for single-chassis system:

```
Location  Card Type               HW State      SW State      Config State
----------------------------------------------------------------------------
0/RP0     NC6-RP                  OPERATIONAL   OPERATIONAL   NSHUT
0/RP1     NC6-RP                  OPERATIONAL   OPERATIONAL   NSHUT
0/FC0     NC6-FC                  OPERATIONAL   N/A           NSHUT
0/FT0     P-L-FANTRAY             OPERATIONAL   N/A           NSHUT
0/FT1     P-L-FANTRAY             OPERATIONAL   N/A           NSHUT
```

```
0/3       NC6-10X100G-M          OPERATIONAL   OPERATIONAL   NSHUT
0/7       NC6-10X100G-M          FAILED        FAILED        NSHUT
0/PT1     PWR-2KW-DC-V2 1.0      OPERATIONAL   N/A           NSHUT
```

This is an example for multi-chassis system:

```
Wed Jun  4  15:08:09.495 UTC
Location  Card Type              HW State      SW State      Config State
-----------------------------------------------------------------------------
0/3       NC6-10X100G-M-P        OPERATIONAL   OPERATIONAL   NSHUT
0/6       NC6-10X100G-M-P        OPERATIONAL   OPERATIONAL   NSHUT
0/RP0     NC6-RP                 OPERATIONAL   OPERATIONAL   NSHUT
0/RP1     P-L-RP                 OPERATIONAL   OPERATIONAL   NSHUT
0/FC2     NC6-FC-MC              OPERATIONAL   N/A           NSHUT
0/FC3     NC6-FC-MC              OPERATIONAL   N/A           NSHUT
0/FC4     NC6-FC-MC              OPERATIONAL   N/A           NSHUT
0/FC5     NC6-FC-MC              OPERATIONAL   N/A           NSHUT
0/FT0     NC6-FANTRAY            OPERATIONAL   N/A           NSHUT
0/FT1     NC6-FANTRAY            OPERATIONAL   N/A           NSHUT
0/PT1     PROTO-AC-PWRTRAY       OPERATIONAL   N/A           NSHUT
1/FC2     NC6-FC-MC              OPERATIONAL   N/A           NSHUT
1/FC3     NC6-FC-MC              OPERATIONAL   N/A           NSHUT
1/FC4     NC6-FC-MC              OPERATIONAL   N/A           NSHUT
1/FC5     NC6-FC-MC              OPERATIONAL   N/A           NSHUT
1/CI0     NCS-CRFT               OPERATIONAL   N/A           NSHUT
1/FT0     NC6-FANTRAY            OPERATIONAL   N/A           NSHUT
1/FT1     NC6-FANTRAY            OPERATIONAL   N/A           NSHUT
1/PT0     NCS-AC-PWRTRAY         OPERATIONAL   N/A           NSHUT
1/PT1     NCS-AC-PWRTRAY         OPERATIONAL   N/A           NSHUT
F0/SC0    P-F-SCSW               OPERATIONAL   OPERATIONAL   NSHUT
F0/SC1    P-F-SC                 OPERATIONAL   OPERATIONAL   NSHUT
F0/FT0    NCS-FCC-FANTRAY        OPERATIONAL   N/A           NSHUT
F0/FT1    NCS-FCC-FANTRAY        OPERATIONAL   N/A           NSHUT
F1/PT1    P-F-AC-PWRTRAY         OPERATIONAL   N/A           NSHUT
F1/SW0    NCS-F-SCSW (SW)        OPERATIONAL   N/A           NSHUT
```

Verify that all cards installed on the router are displayed in the result. The software state of LCs and RPs and the hardware state of FC and FTs should be "OPERATIONAL". Various hardware and software states are listed here.

Hardware states:

- OPERATIONAL—Card is operating normally and is fully functional
- POWERED_ON—Power is on and the card is booting up
- FAILED—Card is powered on but has experienced some internal failure
- PRESENT—Card is in the shutdown state
- OFFLINE—User has changed the card state to OFFLINE. The card is accessible for diagnostics

Software states:

- DIAG_MODE—User has changed the card state to OFFLINE for diagnosis
- OPERATIONAL—Software is operating normally and is fully functional
- SW_INACTIVE—Software is not completely operational
- FAILED—Software is operational but the card has experienced some internal failure

Note In the result, the RPs are not highlighted as active and standby. This is because, at all times, the System Admin VM is operational on both RPs. If one RP fails, the System Admin VM running on the other RP continues to manage all the System Admin functions of the router.

Verify Software Version

The Cisco NCS 6008 router is shipped with the Cisco IOS XR software pre-installed. Verify that the latest version of the software is installed. If a newer version is available, perform a system upgrade. This will install the newer version of the software and provide the latest feature set on the router.

Perform this task to verify the version of Cisco IOS XR software running on the router.

SUMMARY STEPS

1. **show version**

DETAILED STEPS

show version

Example:

```
RP/0/RP0/CPU0:router# show version
```

Displays the version of the various software components installed on the router. The result includes the version of Cisco IOS XR software, its various components, and BIOS information.

Only that portion of the output where the Cisco IOS XR software version is displayed is shown here:

```
Cisco IOS XR Software, Version 6.2.1
Copyright (c) 2013-2017 by Cisco Systems, Inc.

Build Information:
Built By     :
Built On     : Wed Feb 1 13:38:05 PST 2017
Build Host   : iox-lnx-031
Workspace    : /auto/6.2.1.SIT_IMAGE/ncs6k/workspace
Version      : 6.2.1
Location     : /opt/cisco/XR/packages/

cisco NCS-6000 () processor
System uptime is 7 hours, 3 minutes
```

What to do next

Verify the result to ascertain whether a system upgrade or additional package installation is required. If that is required, refer to the tasks in the chapter Perform System Upgrade and Install Feature Packages, on page 53.

Verify Firmware Version

The firmware on various hardware components of the router must be compatible with the Cisco IOS XR image installed. Incompatibility might cause the router to malfunction. Complete this task to verify the firmware version.

SUMMARY STEPS

1. **admin**
2. **show hw-module fpd**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **show hw-module fpd**

Example:

```
sysadmin-vm:0_RP0#show hw-module fpd
```

Displays the firmware information for various hardware components of the router.

```
RP/0/RP1/CPU0:#show hw-module fpd

                                                               FPD Versions
                                                               =================
Location   Card type        HWver FPD device       ATR Status   Running Programd
------------------------------------------------------------------------------
0/0       NC6-10X100G-M-K   2.0   Backup-BIOS      BSP CURRENT           14.00
0/0       NC6-10X100G-M-K   2.0   Backup-CCC-PwrOn BSP CURRENT            1.36
0/0       NC6-10X100G-M-K   2.0   Backup-EthSwitch BSP CURRENT            1.33
0/0       NC6-10X100G-M-K   2.0   BAO-DB-FPGA          CURRENT    1.06    1.06
0/0       NC6-10X100G-M-K   2.0   BAO-MB-FPGA          CURRENT    1.06    1.06
0/0       NC6-10X100G-M-K   2.0   CCC-Bootloader   BSP CURRENT            2.09
0/0       NC6-10X100G-M-K   2.0   CCC-FPGA          S  CURRENT    2.11    2.11
0/0       NC6-10X100G-M-K   2.0   CCC-Power-On      S  CURRENT    1.41    1.41
0/0       NC6-10X100G-M-K         CPAK-bay-0-FPD       NOT READY
0/0       NC6-10X100G-M-K         CPAK-bay-1-FPD       NOT READY
0/0       NC6-10X100G-M-K         CPAK-bay-2-FPD       NOT READY
0/0       NC6-10X100G-M-K         CPAK-bay-3-FPD       NOT READY
0/0       NC6-10X100G-M-K         CPAK-bay-4-FPD       NOT READY
0/0       NC6-10X100G-M-K         CPAK-bay-5-FPD       NOT READY
0/0       NC6-10X100G-M-K   2.0   CPAK-bay-6-SR10      CURRENT    2.03    2.03
0/0       NC6-10X100G-M-K   2.0   CPAK-bay-7-SR10      CURRENT    2.03    2.03
0/0       NC6-10X100G-M-K   2.0   CPAK-bay-8-LR10      CURRENT    2.03    2.03
0/0       NC6-10X100G-M-K   2.0   CPAK-bay-9-SR10      CURRENT    2.03    2.03
0/0       NC6-10X100G-M-K   2.0   Ethernet-Switch   S  CURRENT    1.33    1.33
0/0       NC6-10X100G-M-K   2.0   PLX-8748             CURRENT
```

In the result, the "RUN" column displays the current version of the firmware running on the FPD.

The "ATR Status" column displays the upgrade status of the firmware. It can display these states:

- READY—The firmware of the FPD is ready for an upgrade.
- NOT READY—The firmware of the FPD is not ready for an upgrade.
- NEED UPGD—A newer firmware version is available in the installed image. It is recommended that an upgrade be performed.
- UPGD DONE—The firmware upgrade is successful.
- UPGD FAIL—The firmware upgrade has failed.
- BACK IMG—The firmware is corrupted. Reinstall the firmware.
- UPGD SKIP—The upgrade has been skipped because the installed firmware version is higher than the one available in the image.

What to do next

- Upgrade the required firmware by using the **upgrade hw-module location all fpd** command in the System Admin EXEC mode. You can selectively update individual FPDs, or update all of them together. For the FPD upgrade to take effect, the router needs a power cycle.
- If required, turn on the auto fpd upgrade function. To do so, use the **fpd auto-upgrade enable** command in the System Admin Config mode. After it is enabled, if there are new FPD binaries present in the image being installed on the router, FPDs are automatically upgraded during the system upgrade operation.

Verify Interface Status

After the router has booted, all available interfaces must be discovered by the system. If interfaces are not discovered, it might indicate a malfunction in the unit. Complete this task to view the number of discovered interfaces.

For the multi-chassis system, run the command from one chassis. The verification commands will list information for all chassis.

SUMMARY STEPS

1. **show ipv4 interface summary**

DETAILED STEPS

show ipv4 interface summary

Example:

```
RP/0/RP0/CPU0:router#show ipv4 interface summary
```

When a router is turned on for the first time, all interfaces are in the 'unassigned' state. Verify that the total number of interfaces displayed in the result matches with the actual number of interfaces present on the router.

```
IP address      State   State           State           State
config          up,up   up,down         down,down       shutdown,down
----------------------------------------------------------------------
Assigned        0       0               0               0
Unnumbered      0       0               0               0
Unassigned      0       0               0               4
```

In the above result:

- Assigned— An IP address is assigned to the interface.
- Unnumbered— Interface which has borrowed an IP address already configured on one of the other interfaces of the router.
- Unassigned—No IP address is assigned to the interface.

You can also use the **show interfaces brief** and **show interfaces summary** commands in the XR EXEC mode to verify the interface status.

Verify Fabric Plane

The packets traverse from the ingress to the egress interfaces over the fabric plane. There can be a maximum of six fabric planes. The Cisco NCS routing system fabric is implemented through multiple redundant fabric cards (FCs) installed in the line card chassis.

For the multi-chassis system, run the command from one chassis. The verification commands will list information for all chassis.

Complete this task to verify the status of the fabric planes.

Before you begin

Install all required fabric cards on the router.

SUMMARY STEPS

1. **admin**
2. **show controller fabric plane all**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **show controller fabric plane all**

Example:

```
sysadmin-vm:0_RP0#show controller fabric plane all
```

Displays the status of the switch fabric plane.

```
sysadmin-vm:0_RP1# show controller fabric plane all
Mon Feb  13 15:01:52.594 UTC

Plane Admin Plane  Plane  up->dn  up->mcast
Id    State State  Mode   counter   counter
--------------------------------------
0     UP    UP       B2B         0         0
1     UP    UP       B2B         0         0
2     UP    UP       B2B         0         0
3     UP    UP       B2B         0         0
4     UP    UP       B2B         0         1
5     UP    UP       B2B         0         0
```

Verify that the Admin State and Plane State for all operational planes is "UP". Each fabric card represents one plane. If the Plane State is "DN", it indicates that traffic is not able to reach any destination using the plane. If the Plane State is "MCAST_DN", it indicates that some destinations are not reachable using the plane. This indicates that one fabric card in the line card chassis (LCC) is not operational. Reinstall the fabric card and verify that its state is "OPERATIONAL" in the result of **show platform** command in the System Admin EXEC mode. For details, see Verify Node Status, on page 29.

Verify SDR Information

Secure domain routers (SDRs) divide a single physical system into multiple logically-separated routers. SDRs are also known as logical routers (LRs). On the Cisco NCS 6008 router, only one SDR is supported. This SDR is termed the default-sdr. Every router is shipped with the default-sdr, which owns all RPs and LCs installed in the routing system. An instance of this SDR runs on all nodes. Complete this task to verify the details of the SDR instances.

For the multi-chassis system, run the command from one chassis. The verification commands will list information for all chassis.

SUMMARY STEPS

1. **admin**
2. **sh sdr**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **sh sdr**

Example:

```
sysadmin-vm:0_RP0# sh sdr
```

Displays the SDR information for every node.

```
SDR: default-sdr
Location     IP Address      Status           Boot Count  Time Started
-----------------------------------------------------------------------------
0/RP0/VM1    192.0.0.4       RUNNING          1           02/13/2017 10:06:01
0/RP1/VM1    192.0.4.4       RUNNING          2           02/13/2017 07:27:25
0/0/VM1      192.0.64.3      RUNNING          1           02/10/2017 12:44:02
0/1/VM1      192.0.68.3      RUNNING          1           02/10/2017 12:44:02
0/2/VM1      192.0.72.3      RUNNING          1           02/10/2017 12:44:01
0/3/VM1      192.0.76.3      RUNNING          1           02/10/2017 12:44:01
0/4/VM1      192.0.80.3      RUNNING          1           02/10/2017 12:55:10
0/5/VM1      192.0.84.3      RUNNING          1           02/10/2017 12:44:02
0/6/VM1      192.0.88.3      RUNNING          1           02/10/2017 12:44:04
0/7/VM1      192.0.92.3      RUNNING          1           02/10/2017 12:44:01
1/RP0/VM1    192.1.0.4       RUNNING          1           02/13/2017 10:06:14
1/RP1/VM1    192.1.4.4       RUNNING          1           02/13/2017 07:28:54
1/0/VM1      192.1.64.3      RUNNING          1           02/13/2017 04:31:21
1/1/VM1      192.1.68.3      RUNNING          1           02/13/2017 04:31:22
1/2/VM1      192.1.72.3      RUNNING          1           02/13/2017 04:31:22
1/3/VM1      192.1.76.3      RUNNING          1           02/13/2017 05:19:19
1/4/VM1      192.1.80.3      RUNNING          1           02/13/2017 04:31:20
1/5/VM1      192.1.84.3      RUNNING          1           02/13/2017 04:31:22
1/6/VM1      192.1.88.3      RUNNING          1           02/13/2017 04:40:26
1/7/VM1      192.1.92.3      RUNNING          1           02/13/2017 04:31:22
```

For a functional SDR, the VM State is "RUNNING". If the SDR is not running on a node, no output is shown in the result, for that location. At times the node performs a core dump. During such times the VM State is "Paused & Core Dump in Progress".

What to do next

If you find SDR is not running on a node, try reloading the node. To do that, use the **hw-module location** *node-id* **reload** command in the System Admin EXEC mode.

Verify Control Ethernet Connections

The control ethernet connections connect the chassis within the multi-chassis system. A control ethernet failure disconnects one or more chassis from rest of the system. If the chassis is disconnected, the connectivity with the fabric cards chassis is impaired. The disconnect can be due to fiber cut, hardware failure or software failure.

For the multi-chassis system, run the command from one chassis. The verification commands will list information for all chassis.

Complete this task to verify the status of the control ethernet connections.

SUMMARY STEPS

1. **admin**

2. **show controller switch summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters System Admin EXEC mode.
Step 2	**show controller switch summary** **Example:** `sysadmin-vm:0_RP0#show controller switch summary`	Displays the summary of the switch.

```
Wed Jun  4  17:23:19.752 UTC
Rack  Card  Switch  Rack Serial Number
--------------------------------------
0     RP0   RP-SW   FMP12020050

      Phys   Admin  Port      Protocol  Forward
Port  State  State  Speed     State     State
  Connects To
-------------------------------------------------
0     Down   Up     10-Gbps   Down      -
  LC7
2     Up     Up     10-Gbps   Standby   Forwarding
  LC6
4     Down   Up     1-Gbps    Down      -
  FC0
5     Down   Up     1-Gbps    Down      -
  FC1
6     Down   Up     10-Gbps   Down      -
  LC5
8     Down   Up     10-Gbps   Down      -
  LC4
10    Up     Up     1-Gbps    Standby   Forwarding
  FC2
16    Down   Up     10-Gbps   Down      -
  LC0
18    Down   Up     10-Gbps   Down      -
  LC1
20    Up     Up     1-Gbps    Standby   Forwarding
  FC5
21    Up     Up     1-Gbps    Standby   Forwarding
  FC4
22    Down   Up     10-Gbps   Down      -
  LC2
24    Up     Up     10-Gbps   Standby   Forwarding
  LC3
26    Up     Up     1-Gbps    Standby   Forwarding
  FC3
32    Up     Up     10-Gbps   Standby   Forwarding
  RP1 Card (RP0 Ctrl)
34    Up     Up     10-Gbps   -         Forwarding
  RP1 Card (RP1 Ctrl)
36    Up     Up     1-Gbps    -         Forwarding
  Mgmt Eth0
37    Up     Up     1-Gbps    -         Forwarding
  CCC (RP1 Ctrl)
38    Up     Up     1-Gbps    Standby   Forwarding
  CCC (RP0 Ctrl)
40    Up     Up     10-Gbps   -         Forwarding
```

	Command or Action	Purpose

		`  RP0 CPU (0)`
		`48     Down    Up      10-Gbps   -         -`
		`  I/F Shelf Eth4`
		`49     Down    Up      10-Gbps   -         -`
		`  I/F Shelf Eth5`
		`50     Down    Up      10-Gbps   -         -`
		`  I/F Shelf Eth2`
		`51     Down    Up      10-Gbps   -         -`
		`  I/F Shelf Eth3`
		`54     Up      Up      1-Gbps    -         Forwarding`
		`  Mgmt Eth1`
		`56     Down    Up      10-Gbps   -         -`
		`  I/F Shelf Eth0`
		`57     Down    Up      10-Gbps   -         -`
		`  I/F Shelf Eth1`
		`58     Up      Up      10-Gbps   Active    Forwarding`
		`  Exp Eth0`
		`59     Up      Up      10-Gbps   Standby   Blocking`
		`  Exp Eth1`
		Verify the state of Exp Eth 0 and Exp Eth 1 ports. One port must be in Active (Forwarding) state, and one port in Standby (Blocking) state. The state of the ethernet port is decided by the system. Verify that the connected ports are up, active and in forwarding state. If the states are not displayed correctly, check the control ethernet cabling.

Monitor Craft Panel Interface

Network Convergence System (NCS) 6000 system has a craft panel interface on the front of fabric card chassis (FCC). The craft panel interface assists the field operator in monitoring and troubleshooting the router. It consists of a touch screen LCD display and three LEDs. The LEDs indicate minor, major and critical alarms.

For more information about completing the hardware installation, see Cisco Network Convergence System 6000 Series Routers Hardware Installation Guide.

On powering up, the main screen is displayed on the craft panel LCD. The craft panel has a settings screen to adjust the brightness, volume of audio alarms and inactivity timer for the LCD. You can turn off the LCD display with the help of the sleep button. There is a help option on every screen. This option displays information (in text) for each button. Refresh and back buttons (available on each screen) enable the user to refresh and go back to the previous screen, respectively.

Craft panel interface is used to fetch the following information from the chassis:

- Chassis power configuration and consumption. This is similar to the output of the **show environment power** command.
- Power Entry Module (PEM) status information of the chassis. This is similar to the output of the **show environment power** command.
- Fan operation speed and current status. This is similar to the output of the **show environment fan** command.
- Alarms in the chassis. This is similar to the output of the **show alarms** command.

- Chassis temperature information for the route processors and shelf controllers.
- Hardware and software state of all cards in the chassis.
- Router name and rack-id of chassis (on each screen).
- Uptime of the route processors.
- Messages for the craft operator from the administrator sent from a remote location.

CHAPTER 6

Create User Profiles and Assign Privileges

To provide controlled access to the System Admin configurations on the Cisco NCS 6008 router, user profiles are created with assigned privileges. The privileges are specified using command rules and data rules. The authentication, authorization, and accounting (aaa) commands are used in the System Admin Config mode for the creation of users, groups, command rules, and data rules. The "aaa" commands are also used for changing the disaster-recovery password.

Note You cannot configure the external AAA server and services from the System Admin VM. It can be configured only from the XR VM.

Note If any user on XR is deleted, the local database checks whether there is a first user on System Admin VM.

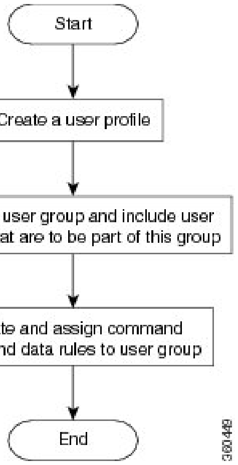
- If there is a first user, no syncing occurs.
- If there is no first user, then the first user on XR (based on the order of creation) is synced to System Admin VM.

For more information on AAA services, see Configuring AAA Services chapter in System Security Configuration Guide for Cisco NCS 6000 Series Routers

Users are authenticated using username and password. Authenticated users are entitled to execute commands and access data elements based on the command rules and data rules that are created and applied to user groups. All users who are part of a user group have such access privileges to the system as defined in the command rules and data rules for that user group.

The workflow for creating user profile is represented in this flow chart:

Figure 5: Workflow for Creating User Profiles


Start
Create a user profile
Create a user group and include user profiles that are to be part of this group
Create and assign command rules and data rules to user group
End
360449

Note The root-lr user, created for the XR VM during initial router start-up, is mapped to the root-system user for the System Admin VM. The root-system user has superuser permissions for the System Admin VM and therefore has no access restrictions.

Use the **show run aaa** command in the System Admin Config mode to view existing aaa configurations.

The topics covered in this chapter are:

- Create a User Profile, on page 42
- Create a User Group, on page 44
- Create Command Rules, on page 46
- Create Data Rules, on page 48
- Change Disaster-recovery Username and Password, on page 50
- Recover Password using PXE Boot, on page 51

Create a User Profile

Create new users for the System Admin VM. Users are included in a user group and assigned certain privileges. The users have restricted access to the commands and configurations in the System Admin VM console, based on assigned privileges.

The router supports a maximum of 1024 user profiles.

Note Users created in the System Admin VM are different from the ones created in XR VM. As a result, the username and password of a System Admin VM user cannot be used to access the XR VM, and vice versa.

The root-lr user of XR VM can access the System Admin VM by entering **Admin** command in the XR EXEC mode. The router does not prompt you to enter any username and password. The XR VM root-lr user is provided full access to the System Admin VM.

If you access the System Admin VM by directly connecting to the System Admin VM console port or System Admin VM management port, you will be prompted to enter the System Admin username and password that is created in this task.

SUMMARY STEPS

1. **admin**
2. **config**
3. **aaa authentication users user** *user_name*
4. **password** *password*
5. **uid** *user_id_value*
6. **gid** *group_id_value*
7. **ssh_keydir** *ssh_keydir*
8. **homedir** *homedir*
9. **commit**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters System Admin Config mode.

Step 3 **aaa authentication users user** *user_name*

Example:

```
sysadmin-vm:0_RP0(config)#aaa authentication users user us1
```

Creates a new user and enters user configuration mode. In the example, the user "us1" is created.

Step 4 **password** *password*

Example:

```
sysadmin-vm:0_RP0(config-user-us1)#password pwd1
```

Enter the password that will be used for user authentication at the time of login into System Admin VM.

Step 5 **uid** *user_id_value*

Example:

```
sysadmin-vm:0_RP0(config-user-us1)#uid 100
```

Specify a numeric value. You can enter any 32 bit integer.

Step 6 **gid** *group_id_value*

Example:

```
sysadmin-vm:0_RP0(config-user-us1)#gid 50
```

Specify a numeric value. You can enter any 32 bit integer.

Step 7 **ssh_keydir** *ssh_keydir*

Example:

```
sysadmin-vm:0_RP0(config-user-us1)#ssh_keydir dir1
```

Specify any alphanumeric value.

Step 8 **homedir** *homedir*

Example:

```
sysadmin-vm:0_RP0(config-user-us1)#homedir dir2
```

Specify any alphanumeric value.

Step 9 **commit**

What to do next

- Create user group that includes the user created in this task. See Create a User Group, on page 44.
- Create command rules that apply to the user group. See Create Command Rules, on page 46.
- Create data rules that apply to the user group. See Create Data Rules, on page 48.

Create a User Group

Create a new user group to associate command rules and data rules with it. The command rules and data rules are enforced on all users that are part of the user group.

The router supports a maximum of 32 user groups.

Before you begin

Create a user profile. See Create a User Profile, on page 42.

SUMMARY STEPS

1. **admin**
2. **config**
3. **aaa authentication groups group** *group_name*
4. **users** *user_name*
5. **gid** *group_id_value*
6. **commit**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters System Admin Config mode.

Step 3 **aaa authentication groups group** *group_name*

Example:

```
sysadmin-vm:0_RP0(config)#aaa authentication groups group gr1
```

Creates a new user group (if it is not already present) and enters the group configuration mode. In this example, the user group "gr1" is created.

Note By default, the user group "root-system" is created by the system at the time of root user creation. The root user is part of this user group. Users added to this group will get root user permissions.

Step 4 **users** *user_name*

Example:

```
sysadmin-vm:0_RP0(config-group-gr1)#users us1
```

Specify the name of the user that should be part of the user group.

You can specify multiple user names enclosed withing double quotes. For example, **users** "*user1 user2 ...*".

Step 5 **gid** *group_id_value*

Example:

```
sysadmin-vm:0_RP0(config-group-gr1)#gid 50
```

Specify a numeric value. You can enter any 32 bit integer.

Step 6 **commit**

What to do next

- Create command rules. See Create Command Rules, on page 46.
- Create data rules. See Create Data Rules, on page 48.

Create Command Rules

Command rules are rules based on which users of a user group are either permitted or denied the use of certain commands. Command rules are associated to a user group and get applied to all users who are part of the user group.

A command rule is created by specifying whether an operation is permitted, or denied, on a command. This table lists possible operation and permission combinations:

Operation	**Accept Permission**	**Reject Permission**
Read (R)	Command is displayed on the CLI when "?" is used.	Command is not displayed on the CLI when "?" is used.
Execute (X)	Command can be executed from the CLI.	Command cannot be executed from the CLI.
Read and execute (RX)	Command is visible on the CLI and can be executed.	Command is neither visible nor executable from the CLI.

By default, all permissions are set to **Reject**.

Each command rule is identified by a number associated with it. When multiple command rules are applied to a user group, the command rule with a lower number takes precedence. For example, cmdrule 5 permits read access, while cmdrule10 rejects read access. When both these command rules are applied to the same user group, the user in this group gets read access because cmdrule 5 takes precedence.

As an example, in this task, the command rule is created to deny read and execute permissions for the "show platform" command.

Before you begin

Create an user group. See Create a User Group, on page 44.

SUMMARY STEPS

1. **admin**
2. **config**
3. **aaa authorization cmdrules cmdrule** *command_rule_number*
4. **command** *command_name*
5. **ops {r | x | rx}**
6. **action {accept | accept_log | reject}**
7. **group** *user_group_name*
8. **context** *connection_type*
9. **commit**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters System Admin Config mode.

Step 3 **aaa authorization cmdrules cmdrule** *command_rule_number*

Example:

```
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 1100
```

Specify a numeric value as the command rule number. You can enter a 32 bit integer.

Important Do no use numbers between 1 to 1000 because they are reserved by Cisco.

This command creates a new command rule (if it is not already present) and enters the command rule configuration mode. In the example, command rule "1100" is created.

Note By default "cmdrule 1" is created by the system when the root-system user is created. This command rule provides "accept" permission to "read" and "execute" operations for all commands. Therefore, the root user has no restrictions imposed on it, unless "cmdrule 1" is modified.

Step 4 **command** *command_name*

Example:

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#command "show platform"
```

Specify the command for which permission is to be controlled.

If you enter an asterisk '*' for **command**, it indicates that the command rule is applicable to all commands.

Step 5 **ops {r | x | rx}**

Example:

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#ops rx
```

Specify the operation for which permission has to be specified:

- **r** — Read
- **x** — Execute
- **rx** — Read and execute

Step 6 **action** {**accept** | **accept_log** | **reject**}

Example:

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#action reject
```

Specify whether users are permitted or denied the use of the operation.

- **accept** — users are permitted to perform the operation
- **accept_log**— users are permitted to perform the operation and every access attempt is logged.

- **reject**— users are restricted from performing the operation.

Step 7 **group** *user_group_name*

Example:

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#group gr1
```

Specify the user group on which the command rule is applied.

Step 8 **context** *connection_type*

Example:

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#context *
```

Specify the type of connection to which this rule applies. The connection type can be *netconf* (Network Configuration Protocol), *cli* (Command Line Interface), or *xml* (Extensible Markup Language). It is recommended that you enter an asterisk '*'; this indicates that the command rule applies to all connection types.

Step 9 **commit**

What to do next

Create data rules. See Create Data Rules, on page 48.

Create Data Rules

Data rules are rules based on which users of the user group are either permitted, or denied, accessing and modifying configuration data elements. The data rules are associated to a user group. The data rules get applied to all users who are part of the user group.

Each data rule is identified by a number associated to it. When multiple data rules are applied to a user group, the data rule with a lower number takes precedence.

Before you begin

Create an user group. See Create a User Group, on page 44.

SUMMARY STEPS

1. **admin**
2. **config**
3. **aaa authorization datarules datarule** *data_rule_number*
4. **keypath** *keypath*
5. **ops** *operation*
6. **action** {**accept** | **accept_log** | **reject**}
7. **group** *user_group_name*
8. **context** *connection type*
9. **namespace** *namespace*
10. **commit**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters System Admin Config mode.

Step 3 **aaa authorization datarules datarule** *data_rule_number*

Example:

```
sysadmin-vm:0_RP0(config)#aaa authorization datarules datarule 1100
```

Specify a numeric value as the data rule number. You can enter a 32 bit integer.

Important Do no use numbers between 1 to 1000 because they are reserved by Cisco.

This command creates a new data rule (if it is not already present) and enters the data rule configuration mode. In the example, data rule "1100" is created.

Note By default "datarule 1" is created by the system when the root-system user is created. This data rule provides "accept" permission to "read", "write", and "execute" operations for all configuration data. Therefore, the root user has no restrictions imposed on it, unless "datarule 1" is modified.

Step 4 **keypath** *keypath*

Example:

```
sysadmin-vm:0_RP0(config-datarule-1100)#keypath  /aaa/disaster-recovery
```

Specify the keypath of the data element. The keypath is an expression defining the location of the data element. If you enter an asterisk '*' for **keypath** , it indicates that the command rule is applicable to all configuration data.

Step 5 **ops** *operation*

Example:

```
sysadmin-vm:0_RP0(config-datarule-1100)#ops rw
```

Specify the operation for which permission has to be specified. Various operations are identified by these letters:

- c—Create
- d—Delete
- u—Update
- w— Write (a combination of create, update, and delete)
- r—Read
- x—Execute

Step 6 **action** {**accept** | **accept_log** | **reject**}

Example:

```
sysadmin-vm:0_RP0(config-datarule-1100)#action reject
```

Specify whether users are permitted or denied the operation.

- **accept** — users are permitted to perform the operation
- **accept_log**— users are permitted to perform the operation and every access attempt is logged
- **reject**— users are restricted from performing the operation

Step 7 **group** *user_group_name*

Example:

```
sysadmin-vm:0_RP0(config-datarule-1100)#group gr1
```

Specify the user group on which the data rule is applied. Multiple group names can also be specified.

Step 8 **context** *connection type*

Example:

```
sysadmin-vm:0_RP0(config-datarule-1100)#context *
```

Specify the type of connection to which this rule applies. The connection type can be *netconf* (Network Configuration Protocol), *cli* (Command Line Interface), or *xml* (Extensible Markup Language). It is recommended that you enter an asterisk '*', which indicates that the command applies to all connection types.

Step 9 **namespace** *namespace*

Example:

```
sysadmin-vm:0_RP0(config-datarule-1100)#namespace *
```

Enter asterisk '*' to indicate that the data rule is applicable for all namespace values.

Step 10 **commit**

Change Disaster-recovery Username and Password

When you define the root-system username and password initially after starting the router, the same username and password gets mapped as the disaster-recovery username and password for the System Admin VM. However, it can be changed.

The disaster-recovery username and password is useful in these scenarios:

- Access the system when the AAA database, which is the default source for authentication in System Admin VM, is corrupted.
- Access the system through the management port, when, for some reason, the System Admin VM console is not working.
- Create new users by accessing the System Admin VM using the disaster-recovery username and password, when the regular username and password is forgotten.

Note On the router, you can configure only one disaster-recovery username and password at a time.

Before you begin

Complete the user creation. For details, see Create a User Profile, on page 42.

SUMMARY STEPS

1. **admin**
2. **config**
3. **aaa disaster-recovery username** *username* **password** *password*
4. **commit**

DETAILED STEPS

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:router# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0#config
```

Enters System Admin Config mode.

Step 3 **aaa disaster-recovery username** *username* **password** *password*

Example:

```
sysadmin-vm:0_RP0(config)#aaa disaster-recovery username us1 password pwd1
```

Specify the disaster-recovery username and the password. You have to select an existing user as the disaster-recovery user. In the example, 'us1' is selected as the disaster-recovery user and assigned the password as 'pwd1'. The password can be entered as a plain text or md5 digest string.

When you need to make use of the disaster recovery username, you need to enter it as *username*@**localhost**.

Step 4 **commit**

Recover Password using PXE Boot

If you are unable to login or lost your XR and System administration passwords, use the following steps to create new password. A lost password cannot be recovered, instead a new username and password must be created with a non-graceful PXE boot.

Step 1 To recover XR password, add or remove the SDR from System admin configuration.

After the SDR is added or removed, verify the configuration. See Verify SDR Information, on page 36.

Step 2 To recover the System admin password, PXE boot the router.

Note PXE boot is fully intrusive. The router state, configuration and image is reset.

Step 3 Reset the password.

CHAPTER 7

Perform System Upgrade and Install Feature Packages

On Cisco NCS 6008 routers, system upgrade and package installation processes are executed using **install** commands. The processes involve adding and activating the iso images (*.iso*), feature packages (*.pkg*), and software maintenance upgrade files (*.smu*) on the router. These files are accessed from a network server and then activated on the router. If the installed package or SMU causes any issue on the router, it can be uninstalled.

The topics covered in this chapter are:

Upgrading the OS and Features

You can upgrade the version of Cisco IOS XR on a router, from the XR VM. However, during system upgrade, the version of IOS XR that runs on both the XR VM and the System Admin VM is upgraded.

System upgrade is done by installing a base package known as the Cisco IOS XR unicast routing core bundle, which is essentially a tar file made up of a core .iso file and multiple .rpm files. The file name for this bundle is `ncs6k-iosxr-r622.tar` which consists of *ncs6k-mini-x.iso* and multiple .rpm files, one of which could be `ncs6k-mpls-1.0.2.0-r622.x86_64.rpm`. You can install this bundle on the XR VM by using **install** commands.

For more information about the install process, see Workflow for Install Process, on page 55.

Upgrading Features

Upgrading features is the process of deploying new features and software patches on the router. Feature upgrade is done by installing package files, termed simply, packages. Software patch installation is done by installing Software Maintenance Upgrade (SMU) files.

Installing a package on the router installs specific features that are part of that package. Cisco IOS XR software is divided into various software packages; this enables you to select the features to run on your router. Each package contains components that perform a specific set of router functions, such as routing, security, and so on. Standard XR VM packages are:

- ncs6k-mcast.pkg

- ncs6k-mpls.pkg
- ncs6k-mgbl.pkg
- ncs6k-k9sec.pkg
- ncs6k-doc.pkg
- ncs6k-li.pkg

Package and SMU installation is performed using **install** commands.

For more information about the install process, see Workflow for Install Process, on page 55.

Caution Do not perform any install operations when the router is reloading.

Do not reload the router during an upgrade operation.

There are separate packages and SMUs for the XR VM and the System Admin VM. They can be identified by their filenames. The XR VM package has *ncs6k* as part of its filename, whereas the System Admin VM package has *ncs6k-sysadmin* as part of its filename. The XR VM packages or SMUs are activated from the XR VM, whereas the System Admin VM packages or SMUs are activated from the System Admin VM.

Note Check the type of SMU before installing it in CTC.

Related Topics

Install Prepared Packages, on page 66
install prepare

Upgrading Features

Upgrading features is the process of deploying new features and software patches on the router. Feature upgrade is done by installing package files, termed simply, packages. Software patch installation is done by installing Software Maintenance Upgrade (SMU) files.

Installing a package on the router installs specific features that are part of that package. Cisco IOS XR software is divided into various software packages; this enables you to select the features to run on your router. Each package contains components that perform a specific set of router functions, such as routing, security, and so on. Standard XR VM packages are:

- ncs6k-mcast.pkg
- ncs6k-mpls.pkg
- ncs6k-mgbl.pkg
- ncs6k-k9sec.pkg
- ncs6k-doc.pkg
- ncs6k-li.pkg

Package and SMU installation is performed using **install** commands.

For more information about the install process, see Workflow for Install Process, on page 55.

There are separate packages and SMUs for the XR VM and the System Admin VM. They can be identified by their filenames. The XR VM package has *ncs6k* as part of its filename, whereas the System Admin VM package has *ncs6k-sysadmin* as part of its filename. The XR VM packages or SMUs are activated from the XR VM, whereas the System Admin VM packages or SMUs are activated from the System Admin VM.

Note Check the type of SMU before installing it in CTC.

Workflow for Install Process

The workflow for installation and uninstallation processes is depicted in this flowchart.

For installing a package, see Install Packages, on page 55. For uninstalling a package, see Uninstall Packages, on page 61.

Install Packages

Complete this task to upgrade the system or install a patch. The system upgrade is done using an ISO image file, while the patch installation is done using packages and SMUs. This task is also used to install *.tar* files. The *.tar* file contains multiple packages and SMUs that are merged into a single file. A single *.tar* file can contain up to 64 individual files.

Note Depending on whether you are installing a System Admin package or a XR package, execute the **install** commands in the System Admin EXEC mode or XR EXEC mode respectively. All **install** commands are applicable in both these modes.

The workflow for installing a package is shown in this flowchart.

SUMMARY STEPS

1. Execute one of these:
   - **install add source** *<tftp transfer protocol>/package_path/ filename1 filename2 ...*
   - **install add source** *<ftp or sftp transfer protocol>//user@server:/package_path/ filename1 filename2 ...*
2. **show install request**
3. **show install repository**
4. **show install inactive**
5. Execute one of these:
   - **install activate** *package_name*
   - **install activate id** *operation_id*
6. **install commit**

7. **show install active**

DETAILED STEPS

Step 1 Execute one of these:

- **install add source** *<tftp transfer protocol>/package_path/ filename1 filename2 ...*
- **install add source** *<ftp or sftp transfer protocol>//user@server:/package_path/ filename1 filename2 ...*

Example:

```
RP/0/RP0/CPU0:router#install add source /harddisk:/ ncs6k-mcast.pkg ncs6k-mpls.pkg
```

or

```
RP/0/RP0/CPU0:router#install add source sftp://root@8.33.5.15:/auto/ncs/package/ ncs6k-mcast.pkg
ncs6k-mpls.pkg
```

or

```
RP/0/RP0/CPU0:router#install add source tftp://223.255.254.254/auto/ncs/package/ncs6k-pkg.tar
```

The software files are unpacked from the package and added to the software repository. This operation might take time depending on the size of the files being added. The operation is performed in asynchronous mode. The **install add** command runs in the background, and the EXEC prompt is returned as soon as possible.

You can use ftp, tftp, or sftp protocols to transfer files from the network server to the router. ftp and sftp protocols are supported from Release 5.0.1. In case of ftp and sftp protocols, you need to enter password within 60 seconds to continue with the **install add** operation. Otherwise, the operation is aborted. To use ftp and sftp protocols on the XR VM, it is mandatory that the *ncs6k-k9sec* package has been installed on the router.

Note The repositories for the XR VM and the System Admin VM are different. The system automatically adds a routing package to the XR VM repository and a system administration package to the System Admin VM repository.

Step 2 **show install request**

Example:

```
RP/0/RP0/CPU0:router#show install request
```

(Optional) Displays the operation ID of the add operation and its status. The percentage of installation in progress is displayed. The operation ID can be later used to execute the **activate** command.

```
Install operation 8 is still in progress
```

For system administration packages, the remaining steps must be performed from the System Admin EXEC mode. Use the **admin** command to enter the System Admin EXEC mode.

Step 3 **show install repository**

Example:

```
RP/0/RP0/CPU0:router#show install repository
```

Displays packages that are added to the repository. Packages are displayed only after the `install add` operation is complete.

```
3 package(s) in XR repository:
    ncs6k-mini-x-<release-version>
    ncs6k-mcast-<release-version>
    ncs6k-mpls-<release-version>
```

Step 4 **show install inactive**

Example:

From the XR VM:

```
RP/0/RP0/CPU0:router#sh install inactive

5 inactive package(s) found:
    ncs6k-mcast-<release-version>
    ncs6k-mpls-<release-version>
    ncs6k-mini-x-<release-version>
    ncs6k-xr-<release-version>
    ncs6k-mgbl-<release-version>
```

From the SystemAdmin VM:

```
sysadmin-vm:0_RP0#sh install inactive

Node 0/RP0 [RP]
    Inactive Packages:
       ncs6k-mini-x-<release-version>
       ncs6k-sysadmin-<release-version>
Node 1/RP0 [RP]
    Inactive Packages:
       ncs6k-mini-x-<release-version>
       ncs6k-sysadmin-<release-version>
```

Displays inactive packages that are present in the repository. Only inactive packages can be activated.

```
Two inactive package(s) found:
    ncs6k-mcast-<release-version>
    ncs6k-mpls-<release-version>
```

Step 5 Execute one of these:

- **install activate** *package_name*
- **install activate id** *operation_id*

Example:

```
RP/0/RP0/CPU0:router#install activate ncs6k-mcast-<release-version> ncs6k-mpls-<release-version>
```

or

```
RP/0/RP0/CPU0:router#install activate id 8
```

The package configurations are made active on the router. As a result, new features and software fixes take effect. This operation is performed in asynchronous mode. The **install activate** command runs in the background, and the EXEC prompt is returned as soon as possible.

If you use the operation ID, all packages that were added in the specified operation are activated together. For example, if 5 packages are added in operation 8, by executing **install activate id 8**, all 5 packages are activated together. You do not have to activate the packages individually.

Activation of some SMUs require a manual reloading of the router. When such SMUs are activated, a warning message is displayed to perform reload. The components of the SMU get activated only after the reload is complete. Perform router reload immediately after executing the **install activate** command. If the SMU has dependency on both XR VM and System Admin VM, perform the reload after activating the SMU in both VMs so that they take effect simultaneously. To reload the router, use the **hw-module location all reload** command from the System Admin EXEC mode.

Step 6 **install commit**

Example:

```
RP/0/RP0/CPU0:router#install commit
```

Commits the newly active software.

Step 7 **show install active**

Example:

```
RP/0/RP0/CPU0:router#show install active
```

Displays packages that are active.

```
Node 0/RP0/CPU0 [RP]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>

Node 0/RP1/CPU0 [RP]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>

Node 0/3/CPU0 [LC]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>
```

From the result, verify that the same image and package versions are active on all RPs and LCs.

Installing Packages: Related Commands

Related Commands	Purpose
show install log	Displays the log information for the install process; this can be used for troubleshooting in case of install failure.
show install package	Displays the details of the packages that have been added to the repository. Use this command to identify individual components of a package.
install prepare	Makes pre-activation checks on an inactive package, to prepare it for activation.
show install prepare	Displays the list of package that have been prepared and are ready for activation.

What to do next

- After performing a system upgrade, upgrade FPD by using the **upgrade hw-module location all fpd all** command from the System Admin EXEC mode. The progress of FPD upgrade process can be monitored using the **show hw-module fpd** command in the System Admin EXEC mode. Reload the router after the FPD upgrade is completed.
- Verify the installation using the **install verify packages** command.
- Uninstall the packages or SMUs if their installation causes any issues on the router. See Uninstall Packages, on page 61.

Note ISO images cannot be uninstalled. However, you can perform a system downgrade by installing an older ISO version.

Named SDR XR Upgrade

Perform sequentially XR VM upgrade or downgrade for named SDRs. Each of these SDRs shall be upgraded or downgraded to run different versions of the software, based on the XR image.

SUMMARY STEPS

1. Execute one of these:
   - **install add source** *<tftp transfer protocol>/package_path/ filename1 filename2 ...*
   - **install add source** *<harddisk:/>package_path/ filename1 filename2 ...*
   - **install add source** *<ftp or sftp transfer protocol>//user@server:/package_path/ filename1 filename2 ...*
2. **show install repository**
3. **install extract** *mini_package*
4. **show install repository**
5. **install prepare** *<xr package> package1 package2 ...*
6. **install activate**
7. **install commit**

DETAILED STEPS

Step 1 Execute one of these:

- **install add source** *<tftp transfer protocol>/package_path/ filename1 filename2 ...*
- **install add source** *<harddisk:/>package_path/ filename1 filename2 ...*
- **install add source** *<ftp or sftp transfer protocol>//user@server:/package_path/ filename1 filename2 ...*

Example:

The software files are unpacked from the package and added to the software repository. This operation might take time depending on the size of the files being added. The operation is performed in asynchronous mode. The **install add** command runs in the background, and the XR EXEC mode is returned as soon as possible.

Step 2 **show install repository**

Example:

```
RP/0/RP0/CPU0:router#show install repository
```

Displays packages that are added to the repository. Packages are displayed only after the **install add source** operation is complete.

```
19 package(s) in XR repository:
    ncs6k-xr-<release-version>
    ncs6k-mpls-<release-version>
    ncs6k-mcast-<release-version>
    ncs6k-doc-<release-version>
    ncs6k-k9sec-<release-version>
    ncs6k-mini-x-<release-version>
    ncs6k-k9sec-<release-version>
    ncs6k-xr-<release-version>
    ncs6k-doc-<release-version>
    ncs6k-mgbl-<release-version>
    ncs6k-mpls-<release-version>
    ncs6k-doc-<release-version>
    ncs6k-mgbl-<release-version>
    ncs6k-mcast-<release-version>
    ncs6k-k9sec-<release-version>
    ncs6k-mgbl-<release-version>
    ncs6k-mpls-<release-version>
    ncs6k-mcast-<release-version>
    ncs6k-mini-x-<release-version>
```

Step 3 **install extract** *mini_package*

Example:

```
RP/0/RP0/CPU0:router#install extract ncs6k-mini-x-<release-version>
```

Extracts the ISO image from ncs6k-mini-x and places it in repository. Running the command from XR VM extracts only the ISO file for XR.

```
Dec 05 16:38:08 Install operation 16 started by root:
  install extract ncs6k-mini-x-<release-version>
Dec 05 16:38:08 Package list:
Dec 05 16:38:08     ncs6k-mini-x-<release-version>
Dec 05 16:38:09 Install operation will continue in the background
RP/0/RP0/CPU0:router#Dec 05 16:39:16 Install operation 16 finished successfully
```

Step 4 **show install repository**

To get the XR package that is extracted in the previous step.

Example:

```
RP/0/RP0/CPU0:router#show install repository
```

Displays XR packages that are added to the repository. Packages are displayed only after the **install extract** of the mini package is complete.

Step 5 **install prepare** *<xr package> package1 package2 ...*

Example:

```
RP/0/RP0/CPU0:router#install prepare ncs6k-xr-<release-version> ncs6k-mcast-<release-version>
ncs6k-mpls-<release-version> ncs6k-mgbl-<release-version> ncs6k-doc-<release-version>
ncs6k-k9sec-<release-version>
```

Prepares the installable files before activation. During the prepare phase, pre-activation checks are made and the components of the installable files are loaded on to the router setup.

```
Dec 05 16:42:38 Install operation 17 started by root:
  install prepare pkg ncs6k-xr-<release-version> ncs6k-mcast-<release-version>
ncs6k-mpls-<release-version> ncs6k-mgbl-<release-version> ncs6k-doc-<release-version>
ncs6k-k9sec-<release-version>
Dec 05 16:42:38 Package list:
Dec 05 16:42:38     ncs6k-xr-<release-version>
Dec 05 16:42:38     ncs6k-mcast-<release-version>
Dec 05 16:42:38     ncs6k-mpls-<release-version>
Dec 05 16:42:38     ncs6k-mgbl-<release-version>
Dec 05 16:42:38     ncs6k-doc-<release-version>
Dec 05 16:42:38     ncs6k-k9sec-<release-version>
Dec 05 16:42:39 Install operation will continue in the background
RP/0/RP0/CPU0:router#Dec 05 16:44:42 Install operation 17 finished successfully
```

Step 6 **install activate**

Example:

```
RP/0/RP0/CPU0:router#install activate
```

All the packages that have been prepared are activated together to make the package configurations active on the router.

Activation of the SMUs requires reboot of the SDR and a warning message is displayed to perform reboot. The components of the SMU get activated only after the reboot is complete. Perform reboot immediately after the execution of the **install activate** command is completed.

```
Dec 05 16:47:35 Install operation 18 started by root:
  install activate
This install operation will reboot the sdr, continue?
 [yes/no]:[yes] yes
Dec 05 16:47:38 Install operation will continue in the background
RP/0/RP0/CPU0:router#Dec 05 16:47:51 Install operation 18 finished successfully
```

Step 7 **install commit**

Example:

```
RP/0/RP0/CPU0:router#install commit
```

Commits the newly activated software.

Note If you want to do the system upgrade of more than one SDR, the **install commit** command has to be executed on the first upgraded SDR before trying to upgrade the remaining SDRs.

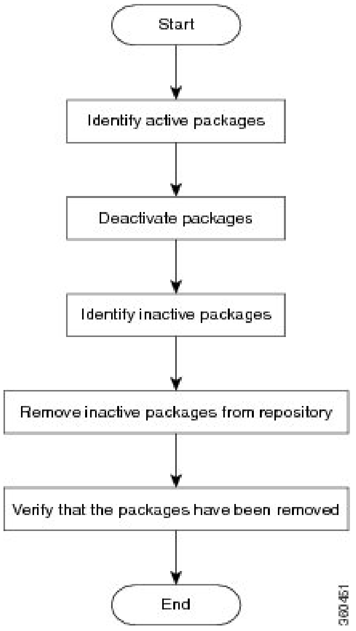
Uninstall Packages

Complete this task to uninstall a package. All router functionalities that are part of the uninstalled package are deactivated. Packages that are added in the XR VM cannot be uninstalled from the System Admin VM, and vice versa.

Note Installed ISO images cannot be uninstalled. Also, kernel SMUs that install third party SMU on host, XR VM and System Admin VM, cannot be uninstalled. However, subsequent installation of ISO image or kernel SMU overwrites the existing installation.

The workflow for uninstalling a package is shown in this flowchart.

Figure 6: Uninstalling Packages Workflow


Start
Identify active packages
Deactivate packages
Identify inactive packages
Remove inactive packages from repository
Verify that the packages have been removed
End
360451

This task uninstalls XR VM packages. If you need to uninstall System Admin packages, run the same commands from the System Admin EXEC mode.

SUMMARY STEPS

1. **show install active**
2. Execute one of these:
   - **install deactivate** *package_name*
   - **install deactivate id** *operation_id*
3. **show install inactive**
4. **install remove** *package_name*
5. **show install repository**

DETAILED STEPS

Step 1 **show install active**

Example:

```
RP/0/RP0/CPU0:router#show install active
```

Displays active packages. Only active packages can be deactivated.

```
Node 0/RP0/CPU0 [RP]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>

Node 0/RP1/CPU0 [RP]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>

Node 0/3/CPU0 [LC]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>
```

Step 2 Execute one of these:

- **install deactivate** *package_name*
- **install deactivate id** *operation_id*

Example:

```
RP/0/RP0/CPU0:router#install deactivate ncs6k-mcast-<release-version> ncs6k-mpls-<release-version>
```

or

```
RP/0/RP0/CPU0:router#install deactivate id 8
```

All features and software patches associated with the package are deactivated. You can specify multiple package names and deactivate them simultaneously.

If you use the operation ID, all packages that were added in the specified operation are deactivated together. You do not have to deactivate the packages individually.

Step 3 **show install inactive**

Example:

```
RP/0/RP0/CPU0:router#show install inactive
```

The deactivated packages are now listed as inactive packages. Only inactive packages can be removed from the repository.

```
Two inactive package(s) found:
    ncs6k-mcast-<release-version>
    ncs6k-mpls-<release-version>
```

Step 4 **install remove** *package_name*

Example:

```
RP/0/RP0/CPU0:router#install remove ncs6k-mcast-<release-version> ncs6k-mpls-<release-version>
```

The inactive packages are removed from the repository.

Use the **install remove** command with the **id** *operation-id* keyword and argument to remove all packages that were added for the specified operation ID.

Step 5 **show install repository**

Example:

```
RP/0/RP0/CPU0:router#show install repository
```

Displays packages available in the repository. The package that are removed are no longer displayed in the result.

```
1 package(s) in XR repository:
    ncs6k-mini-x-<release-version>
```

What to do next

Install required packages. See Install Packages, on page 55

Orchestrated Calvados Upgrade (OCU)

SUMMARY STEPS

1. **install add source/harddisk** *ncs6k-mini-x.iso-<release-version>.DT_IMAGE*
2. **show install repository**
3. **install extract** *mini_package*
4. **show install repository all**
5. **install prepare issu***ncs6k-sysadmin-<release-version>host-<release-version>*
6. **install activate issu**
7. **install commit**

DETAILED STEPS

Step 1 **install add source/harddisk** *ncs6k-mini-x.iso-<release-version>.DT_IMAGE*

Example:

```
RP/0/RP0/CPU0:router## install add source /harddisk: ncs6k-mini-x.iso-<release-version>.DT_IMAGE
```

The software files are unpacked from the package and added to the software repository. This operation might take time depending on the size of the files being added. The operation is performed in asynchronous mode. The **install add** command runs in the background.

```
Tue Apr  19 18:25:37.570 UTC
result Tue Apr 19 18:25:38 2016 Install operation 4 (install add) started by user 'root' will continue
 asynchronously.
sysadmin-vm:0_RP0# show install log 4
Tue Apr  19 18:27:51.667 UTC
log 4
  Apr 19 18:25:37 Admin install operation 4 started by user 'root'
Apr 19 18:25:37 install add source /harddisk: ncs6k-mini-x.iso-<release-version>.DT_IMAGE
```

Step 2 **show install repository**

Example:

```
RP/0/RP0/CPU0:router#show install repository
```

Verifies that the host ISO and sysadmin ISO files are properly added to repository.

```
Tue Apr  19 18:28:17.270 UTC
Admin repository
---------------------
ncs6k-mini-x-<release-version>
ncs6k-mini-x-<release-version>
ncs6k-sysadmin-<release-version>
```

```
sysadmin-vm:0_RP0# install extract ncs6k-mini-x-<release-version>
Tue Apr  19 18:28:34.155 UTC
result Tue Apr 19 18:28:35 2016 Install operation 5 (install extract) started by user 'root' will
continue asynchronously.
sysadmin-vm:0_RP0# Tue Apr 19 18:30:13 2016 Install operation 5 completed successfully.
sysadmin-vm:0_RP0# show install repository all
Tue Apr  19 18:30:33.564 UTC
Admin repository
---------------------
ncs6k-mini-x-<release-version>
ncs6k-mini-x-<release-version>
ncs6k-sysadmin-<release-version>
ncs6k-sysadmin-<release-version>

  XR repository
------------------
ncs6k-mini-x-<release-version>
ncs6k-mini-x-<release-version>
ncs6k-xr-<release-version>

  Host repository
---------------------
host-<release-version>
host-<release-version>
```

Step 3 **install extract** *mini_package*

Example:

```
RP/0/RP0/CPU0:router#install extract ncs6k-mini-x-<release-version>
```

Running the command from System Admin VM extracts the host and ISO file for System Admin installation.

```
Tue Apr  19 18:28:34.155 UTC
result Tue Apr 19 18:28:35 2016 Install operation 5 (install extract) started by user 'root' will
continue asynchronously.
sysadmin-vm:0_RP0# Tue Apr 19 18:30:13 2016 Install operation 5 completed successfully.
```

Step 4 **show install repository all**

Example:

```
RP/0/RP0/CPU0:router#show install repository all
```

Verifies that the host ISO and sysadmin ISO files are properly added to repository.

```
Tue Apr  19 18:30:33.564 UTC
Admin repository
---------------------
ncs6k-mini-x-<release-version>
ncs6k-mini-x-<release-version>
ncs6k-sysadmin-<release-version>
ncs6k-sysadmin-<release-version>

  XR repository
------------------
ncs6k-mini-x-<release-version>
ncs6k-mini-x-<release-version>
ncs6k-xr-<release-version>

  Host repository
---------------------
host-<release-version>
host-<release-version>
```

Step 5 **install prepare issu***ncs6k-sysadmin-<release-version>host-<release-version>*

Example:

```
RP/0/RP0/CPU0:router# install prepare issu ncs6k-sysadmin-<release-version> host-<release-version>
```

Prepares the installable files before activation. During the prepare phase, pre-activation checks are made and the components of the installable files are loaded on to the router setup.

```
Tue Apr  19 18:30:55.754 UTC
result Tue Apr 19 18:30:59 2016 Install operation 6 (install prepare issu) started by user 'root'
will continue asynchronously.
sysadmin-vm:0_RP0# Tue Apr 19 18:33:03 2016 Install operation 6 completed successfully.
```

Step 6 **install activate issu**

Example:

```
RP/0/RP0/CPU0:router#install activate issu
```

Activates the upgrade to new version.

```
Tue Apr  19 18:33:14.470 UTC
This install operation will result in admin VMs reload
Do you want to proceed [yes/no]: yes
Proceeding with operation
result Tue Apr 19 18:33:17 2016 Install operation 6 (install activate issu) started by user 'root'
will continue asynchronously.
sysadmin-vm:0_RP0# Tue Apr 19 18:33:17 2016 Calvados ISSU phase one Initiated
sysadmin-vm:0_RP0# Tue Apr 19 18:33:22 2016 Install operation 7 (install activate issu) started by
user 'root' will continue asynchronously.
sysadmin-vm:0_RP0# Tue Apr 19 18:34:46 2016 Install sub operation 7 completed successfully.
sysadmin-vm:0_RP0# Tue Apr 19 18:34:46 2016 Admin VM of nodes 0/RP1,0/1,0/6,0/0 will now reload as
part of the issu operation
Tue Apr 19 18:36:33 2016 Install sub operation 7 (install activate issu) started by user 'root' will
 continue asynchronously.
sysadmin-vm:0_RP0# sysadmin-vm:0_RP0#
sysadmin-vm:0_RP0# Tue Apr 19 18:37:55 2016 Install operation 7 completed successfully.
sysadmin-vm:0_RP0# Tue Apr 19 18:37:55 2016 Admin VM of node 0/RP0 will now reload as part of the
issu operation
```

Step 7 **install commit**

Example:

```
RP/0/RP0/CPU0:router#install commit
```

Commits the newly activated software.

Note After Orchestrated Calvados Upgrade (OCU), wait for few minutes to run the **admin** command.

Install Prepared Packages

A system upgrade or feature upgrade is performed by activating the ISO image file, packages, and SMUs. It is possible to prepare these installable files before activation. During the prepare phase, pre-activation checks are made and the components of the installable files are loaded on to the router setup. The prepare process runs in the background and the router is fully usable during this time. When the prepare phase is over, all the prepared files can be activated instantaneously. The advantages of preparing before activation are:

- If the installable file is corrupted, the prepare process fails. This provides an early warning of the problem. If the corrupted file was activated directly, it might cause router malfunction.
- Directly activating an ISO image for system upgrade takes considerable time during which the router is not usable. However, if the image is prepared before activation, not only does the prepare process run asynchronously, but when the prepared image is subsequently activated, the activation process too takes very less time. As a result, the router downtime is considerably reduced.

Complete this task to upgrade the system and install packages by making use of the prepare operation.

Note Depending on whether you are installing a System Admin package or a XR package, execute the **install** commands in the System Admin EXEC mode or XR EXEC mode respectively. All **install** commands are applicable in both these modes.

Before you begin

- Configure and connect to the XR VM management port. The installable file is accessed through the management port. For details about configuring the XR VM management port, see Configure the XR VM Management Port, on page 11.
- Copy the package to be installed wither on the router's hard disk or on a network server to which the router has access.

SUMMARY STEPS

1. Add the required ISO image and packages to the repository.
2. **show install repository**
3. Execute one of these:
   - **install prepare** *package_name*
   - **install prepare id** *operation_id*
4. **show install prepare**
5. **install activate**
6. **show install active**

DETAILED STEPS

Step 1 Add the required ISO image and packages to the repository.

For details, see Install Packages, on page 55.

Step 2 **show install repository**

Example:

```
RP/0/RP0/CPU0:router#show install repository
```

Perform this step to verify that the required installable files are available in the repository. Packages are displayed only after the "install add" operation is complete.

```
3 package(s) in XR repository:
 ncs6k-mini-x-<release-version>
 ncs6k-mpls-<release-version>
 ncs6k-mcast-<release-version>
```

Step 3 Execute one of these:

- **install prepare** *package_name*
- **install prepare id** *operation_id*

Example:

```
RP/0/RP0/CPU0:router#install prepare ncs6k-mini-x-<release-version> ncs6k-mcast-<release-version>
ncs6k-mpls-<release-version>
```

or

```
RP/0/RP0/CPU0:router#install prepare id 8
```

The prepare process takes place. This operation is performed in asynchronous mode. The **install prepare** command runs in the background, and the EXEC prompt is returned as soon as possible.

If you use the operation ID, all packages that were added in the specified operation are prepared together. For example, if 5 packages are added in operation 8, by executing **install prepare id 8**, all 5 packages are prepared together. You do not have to prepare the packages individually.

Step 4 **show install prepare**

Example:

```
RP/0/RP0/CPU0:router#show install prepare
```

Displays packages that are prepared.

```
RP/0/RP0/CPU0:router#show install prepare
Thu Nov 21 11:48:33.669 UTC
Prepared Boot Image:  ncs6k-mini-x-<release-version>
Prepared Boot Partition:  /dev/panini_vol_grp/xr_lv6
Restart Type: Reboot
Prepared Packages:
 ncs6k-mini-x-<release-version>
 ncs6k-mpls-<release-version>
 ncs6k-mcast-<release-version>

Use the "install activate" command to activate the prepared packages.
Use the "install prepare clean" command to undo the install prepare operation.
```

From the result, verify that all the required packages have been prepared.

Step 5 **install activate**

Example:

```
RP/0/RP0/CPU0:router#install activate
```

All the packages that have been prepared are activated together to make the package configurations active on the router.

Note You should not specify any package name or operation ID in the CLI.

Activation of some SMUs require manual reload of the router. When such SMUs are activated, a warning message is displayed to perform reload. The components of the SMU get activated only after the reload is complete. Perform router reload immediately after the execution of the **install activate** command is completed.

Step 6 **show install active**

Example:

```
RP/0/RP0/CPU0:router#show install active
```

Displays packages that are active.

```
Node 0/RP0/CPU0 [RP]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>

Node 0/RP1/CPU0 [RP]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>

Node 0/3/CPU0 [LC]
    Boot Partition: xr_lv0
    Active Packages: 3
        ncs6k-mini-x-<release-version> version=<release-version> [Boot image]
        ncs6k-mcast-<release-version>
        ncs6k-mpls-<release-version>
```

From the result, verify that on all RPs and LCs, the same image and package versions are active.

Installing Packages: Related Commands

Related Commands	Purpose
show install log	Displays the log information for the install process; this can be used for troubleshooting in case of install failure.
show install package	Displays the details of the packages that have been added to the repository. Use this command to identify individual components of a package.
install prepare clean	Clears the prepare operation and removes all the packages from the prepared state.

What to do next

- After performing a system upgrade, upgrade FPD by using the **upgrade hw-module location all fpd all** command from the System Admin EXEC mode. The progress of FPD upgrade process can be monitored using the **show hw-module fpd** command in the System Admin EXEC mode. Reload the router after the FPD upgrade is completed.
- Verify the installation using the **install verify packages** command.
- Uninstall the packages or SMUs if their installation causes any issues on the router. See Uninstall Packages, on page 61.

Note ISO images cannot be uninstalled. However, you can perform a system downgrade by installing an older ISO version.

Related Topics

Upgrading the OS and Features, on page 53

install prepare

Installing Packages using ISSU

In-Service Software Upgrade (ISSU) provides the ability to upgrade the router software with no outage on the control plane and forwarding plane. ISSU is a user-initiated and user-controlled process that uses Cisco nonstop forwarding (NSF) and non-stop routing (NSR). ISSU supports upgrading an image from a lower to a higher version and downgrading an image from a higher version to a lower version. ISSU supports zero packet loss (ZPL) and zero topology loss (ZTL).

Note If you are performing an IOS XR image upgrade using ISSU, ensure that node reset is disabled on all the line cards. To disable node reset, use the **hw-module reset auto disable** location `node-id` command in the System Admin mode. After completing the IOS XR image upgrade, reenable node reset using **no hw-module reset auto disable location `node-id`** command in the System Admin mode.

The upgrade or downgrade using ISSU installation involves:

- Prepare phase: The installable files are pre-checked and loaded on the router before activation.
- Activate phase: The new image (V2) is downloaded to all nodes in the router replacing the old image (V1). This phase can be run step-by-step phases like *Load*, *Run* and *Cleanup* or by using a one-shot *Activate* phase.

  Note The *Prepare* phase is optional and can be skipped because the *Load* phase prepares the package if *Prepare* phase was not performed before the *Load* phase.

- Commit phase: The ISSU installation is complete with V2 on all nodes.

ISSU supports installing the System Admin and XR VM using ISSU individually. The System Admin and XR VM can also be upgraded sequentially using System ISSU in a single process. The upgrade sequence is System Admin ISSU followed by XR ISSU. The downgrade sequence is XR ISSU followed by System Admin ISSU. Committing the upgrade from XR commits the System Admin and XR software. But committing from System Admin commits only the System Admin software.

System Admin ISSU:

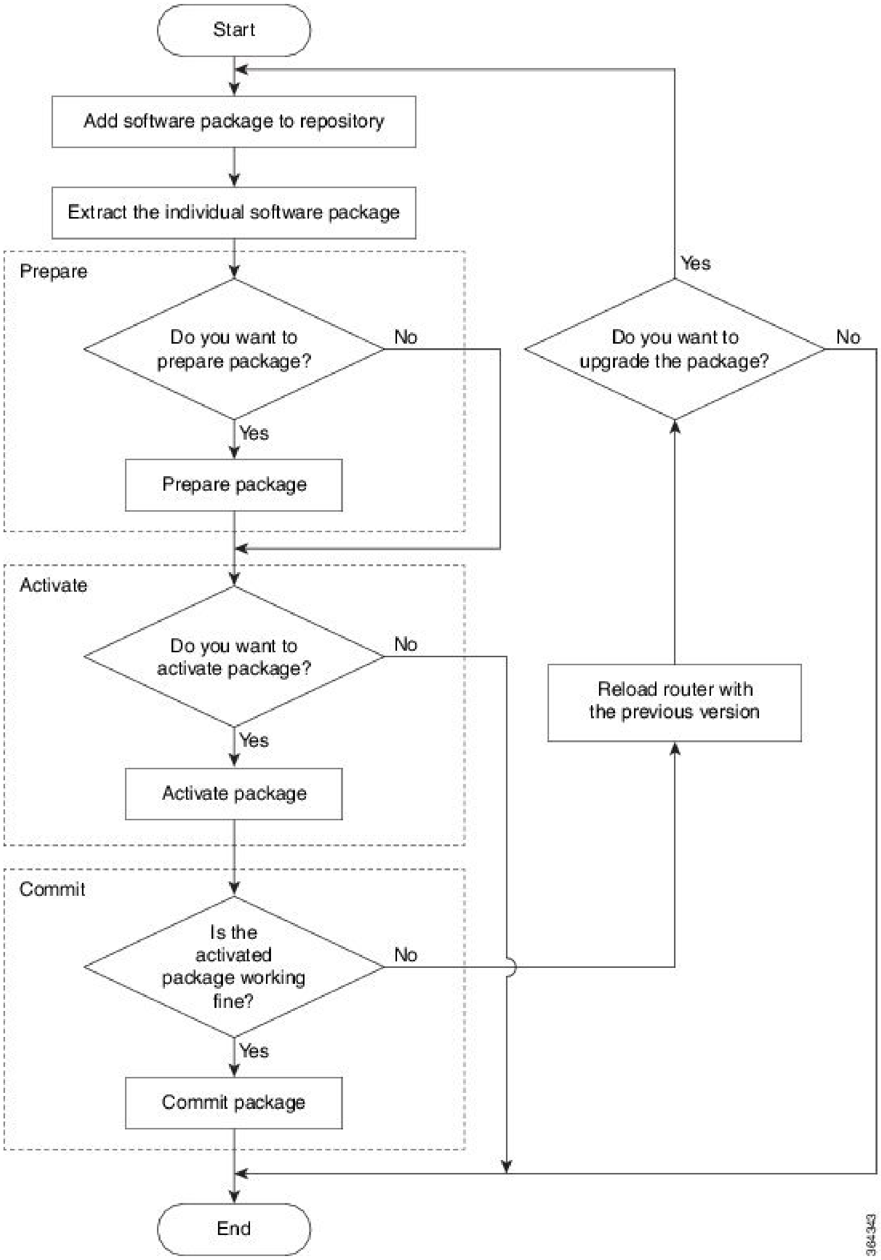
- Packages can be System Admin SMUs, Host SMUs, System Admin ISO and Host ISU
- There is no ISSU SMU for System Admin
- All route processors (RP) must have redundancy
- Upgrade and downgrade are supported
- There is no individual activate load or activate run phases
- Preparing the installable files before activation is optional

- Aborting the process is not supported after the activation starts. Reload the system to restore the old version
- When the image is used to upgrade, the System Admin ISO must be passed along with the host ISO
- Commit command will freeze the new version (V2)
- Host SMUs cannot be deactivated. System Admin SMUs can be deactivated through ISSU

XR ISSU:

- Packages can be SMUs and SMU with ISO.
- If the image is used, the image must be compatible with the current active image.
- All route processors (RP) must have redundancy.
- Upgrade and downgrade are supported.
- Supports step-by-step or one-shot ISSU.
- Aborting the process is not supported after the activation starts. Reload the system to restore the old version.

The workflow for installing a package using ISSU is shown in this flowchart.


Start
Add software package to repository
Extract the individual software package
Prepare
Do you want to prepare package?
No
Yes
Prepare package
Activate
Do you want to activate package?
No
Yes
Activate package
Commit
Is the activated package working fine?
No
Yes
Commit package
End
Yes
Do you want to upgrade the package?
No
Reload router with the previous version
364343

Install Packages using ISSU

Complete this task to upgrade the system or install a patch. The system upgrade is done using an ISO image file, while the patch installation is done using packages and SMUs. Depending on whether you are installing a System Admin package or a XR package, execute these commands in the System Admin EXEC mode or XR EXEC mode respectively.

Note When an upgrade of RSP1 and line cards is performed together using Admin ISSU, all the VMs on those nodes continue to be monitored by the VM manager on RSP0. Hence, RSP1 is always reloaded at the same time as the line cards. Also, as NCS 6000 series does not have active and standby VM pairs; active processes are distributed evenly amongst all VMs.

Before you begin

Copy the package to be installed either on the router's hard disk or on a network server to which the router has access.

Dual route processor (RP) system with standby in "is ready" state.

Step 1 **install add** *package_name*

Example:

For XR VM,

```
RP/0/RP0/CPU0:router#install add ncs6k-x-<release-version>
```

Downloads software package from the location specified by the user to the software repository on route processor (RP) or shelf controller (SC) nodes. The package can be an ISO or a SMU.

Step 2 **install extract** *package_name*

Example:

For XR VM,

```
RP/0/RP0/CPU0:router#install extract ncs6k-x-<release-version>
```

For System Admin VM,

```
sysadmin-vm:0_RP0#install extract ncs6k-x-<release-version>
```

Extracts the ISO image from ncs6k-x.iso and places it in repository. Running the command from XR VM extracts only the ISO file for XR, and running the command from System Admin VM extracts the host and ISO file for System Admin installation. Upgrading the system using ISSU involves upgrading both the System Admin VM and XR VM.

Step 3 **show install repository all**

Verifies that the V2 host ISO and V2 sysadmin ISO for System Admin ISSU, and V2 XR ISO for XR ISSU are properly added to repository.

Step 4 (Optional) **install prepare issu** *V2sysadmin_package_name.iso v2Host_package_Name.iso<V2 SMU's optional>*

Example:

For XR VM,

```
RP/0/RP0/CPU0:router#install prepare issu ncs6k-xr-<release-version>
```

For System Admin VM,

```
sysadmin-vm:0_RP0#install prepare issu ncs6k-sysadmin-<release-version> host-<release-version>
```

Prepares the installable files before activation. During the prepare phase, pre-activation checks are made and the components of the installable files are loaded on to the router setup.

Step 5 Skip to step 6 if you want to install XR ISSU using step-by-step phases. To activate ISSU installation in XR VM and System Admin VM using a single phase, use **install activate issu** command.

Example:

For XR VM,

```
RP/0/RP0/CPU0:router#install activate issu ncs6k-xr-<release-version>
```

For System Admin VM,

```
sysadmin-vm:0_RP0#install activate issu ncs6k-xr-<release-version>
```

Activates the upgrade to new V2 version. If the *Prepare* phase mentioned in step 4 is not performed, the package is implicitly prepared during the *Activate* phase.

Step 6 To activate the XR ISSU in phases, complete these steps:

a) **install activate issu load**

Example:

```
RP/0/RP0/CPU0:router#install activate issu load ncs6k-xr-<release-version>
```

Downloads the new image (V2) to all nodes in the router. The new image is checked for compatibility to ensure that the router can be upgraded. At the start of the *Load* phase, the router configuration mode is locked, and you cannot perform any configuration on the router until ISSU completes the phase. At the end of this stage, all standby nodes run V2 and all active nodes (including all line cards) still run the original software images (V1).

An abort of the upgrade process during the *Load* phase, either manually or due to failures, results in a hitless rollback and each standby or upgraded node is reloaded with V1. The *Load* phase is completed once all standby nodes are successfully loaded with the new image.

b) **install activate issu run**

Example:

```
RP/0/RP0/CPU0:router#install activate issu run
```

Starts version switch from V1 to V2. All the packages that have been prepared are activated to make the package configurations active on the router.

An abort of the upgrade process during the *Run* phase results in a router reload with the original software image.

c) **install activate issu cleanup**

Example:

```
RP/0/RP0/CPU0:router#install activate issu cleanup
```

Initiates shutdown of VMs with previous versions after running the activation. The *Cleanup* phase concludes the ISSU process and the new software runs on all nodes in the system.

Step 7 **install commit**

Commits the newly active software.

Note Committing from XR will commit System Admin and XR software. Whereas, committing from System Admin will only commit the System Admin software.

Installing Packages using ISSU: Related Commands

Related Commands	Purpose
show install log	Displays the log information for the install process; this can be used for troubleshooting in case of install failure.
install activate issu abort	Initiates ISSU abort in XR VM. ISSU aborts if the command is run before ISSU *Run* phase starts. All the changes due to the install activity are reset
install prepare clean	Clears the prepared image.
show install active	Verifies that the versions have changed after installation.

What to do next

- Verify the installation using the **show issu summary** command.
- Uninstall the packages or SMUs if their installation causes any issues on the router.

Note ISO images cannot be uninstalled. However, you can perform a system downgrade by installing an older ISO version.

CHAPTER 8

Perform Disaster Recovery

This chapters covers details on performing disaster recovery using hard disk recovery partition and USB boot process.

Disaster Recovery by Using a Hard Disk Partition

How Disaster Recovery Using a Hard Disk Recovery Partition Works

This new method of disaster recovery introduced from Cisco IOS XR Release 5.2.5 onwards helps overcome operational delays that may occur when a router is in a non-responding state.

Typically, when the router is in a non-responsive state, the administrator has to physically access the router and then take corrective action. Inability to quickly access the router can lead to delays in recovering the router and subsequently cause extended downtime in router operations. To overcome this constraint, this new method of disaster recovery can be performed remotely.

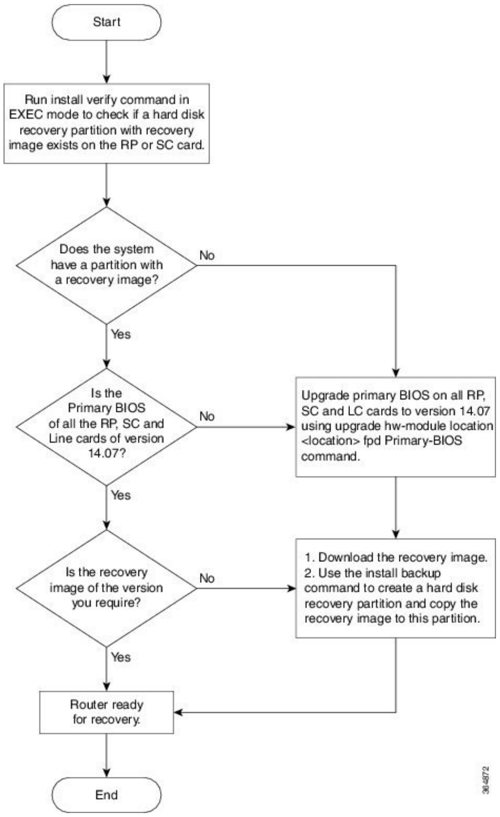
In this method of disaster recovery, while the router is in operational state, a recovery image is copied to a hard disk recovery partition in the RP (route processor) and SC (shelf controller) card. The administrator remotely accesses this recovery image to restore a router.

When the system is in a state of disaster, recovery can be performed only if the following conditions are met:

- The primary BIOS on all RP or SC cards is of version 14.07.
- A hard disk recovery partition already exists on a RP and SC card hard disk with the desired recovery image content.

The following figure illustrates the process of getting a system ready for recovery.

Figure 7: Preparing the System for Disaster Recovery


Start
Run install verify command in EXEC mode to check if a hard disk recovery partition with recovery image exists on the RP or SC card.
Does the system have a partition with a recovery image?
No
Yes
Is the Primary BIOS of all the RP, SC and Line cards of version 14.07?
No
Upgrade primary BIOS on all RP, SC and LC cards to version 14.07 using upgrade hw-module location <location> fpd Primary-BIOS command.
Yes
Is the recovery image of the version you require?
No
1. Download the recovery image.
2. Use the install backup command to create a hard disk recovery partition and copy the recovery image to this partition.
Yes
Router ready for recovery.
End
364872

Note

- To perform disaster recovery in a production environment, it is important that the recovery image be of a release no earlier than Cisco IOS XR Release 5.2.5. The disaster recovery feature is not supported on a release earlier than Cisco IOS XR Release 5.2.5.
- If you upgrade the system to a version higher than R5.2.5, but if the recovery image in the hard disk recovery partition is of Cisco IOS XR Release 5.2.5, the router can still be recovered using this recovery image. After recovery you can upgrade the system to the latest version of software.
- If the system already has a hard disk recovery partition and there is a need to perform disaster recovery using either USB boot or PXE boot, ensure that the image is no earlier than Cisco IOS XR Release 5.2.5 version 37I.

Performing disaster recovery by using a hard disk partition involves the following:

Preparing the Router for Disaster Recovery

Preparing the router for disaster recovery involves copying the recovery image to a hard disk recovery partition when the router is in a fully functional state. To prepare a router for disaster recovery, execute the following steps:

Before you begin

- Download the compressed recovery image from software download page at cisco.com to the hard disk of the router. The filename for the compressed boot file is in this format: ncs6k-dr-boot.tar-*release_number*. For example, ncs6k-dr-boot.tar-5.2.5
- Ensure that the version of primary BIOS on all the RP and SC cards is of version 14.07. If the primary BIOS is of a lower version, use the **upgrade hw-module location location fpd Primary-BIOS** command.
- If you are performing disaster recovery in a multi-chassis environment ensure that there is control ethernet connectivity between the chassis before you boot an RP or SC card from the hard disk recovery partition.

SUMMARY STEPS

1. **install verify packages location** *node-id*
2. **show install log** *install-id*
3. **install backup** *node-id* **location** *destination*

DETAILED STEPS

Step 1 **install verify packages location** *node-id*

Use this command to verify if a partition with a recovery image exists.

Example:

```
sysadmin-vm:0_RP0# install verify packages location 0/RP0

Install operation 30 (install verify) started by user 'root' will continue asynchronously.
replied.check show install log 30 for detailed log.
Install operation completed successfully.
```

Step 2 **show install log** *install-id*

Verify the contents of the log to determine whether creation of hard disk partition is successful.

Example:

```
sysadmin-vm:0_RP0#show install log 30
```

If a hard disk partition already exists, similar output is displayed:

```
sysadmin-vm:0_RP1# show install log 30
Thu Mar  17 01:54:36.776 UTC
log 30
  Mar 17 01:42:00 Admin install operation 30 started by user 'root'
Mar 17 01:42:00 install verify packages location 0/RP1
Mar 17 01:42:26 Disaster Recovery Partition found
./system_image.iso 833636352
MD5: bb73f05528286c87b6b1209754ac9e64 ./system_image.iso
./EFI/Recovery/grub.cfg 516
MD5: 525ce5b5b65701c3942afefd3d4a3249 ./EFI/Recovery/grub.cfg
./EFI/Recovery/grub.efi 887836
MD5: 4abf58ec0fd23255d42e1548aeae2e3e ./EFI/Recovery/grub.efi
Mar 17 01:42:26 Node 0/RP1  completed verification successfully

Mar 17 01:42:26 Install operation 30 completed successfully.
Mar 17 01:42:26 Ending 'install verify' operation 30
```

If a hard disk partition does not exist, similar output is displayed:

```
sysadmin-vm:0_RP1# show install log 30
Thu Mar  17 01:54:36.776 UTC
log 30
  Mar 17 01:42:00 Admin install operation 30 started by user 'root'
Mar 17 01:42:00 install verify packages location 0/RP1
Mar 17 01:42:26 Disaster Recovery Partition Not found
./system_image.iso 833636352
MD5: bb73f05528286c87b6b1209754ac9e64 ./system_image.iso
./EFI/Recovery/grub.cfg 516
MD5: 525ce5b5b65701c3942afefd3d4a3249 ./EFI/Recovery/grub.cfg
./EFI/Recovery/grub.efi 887836
MD5: 4abf58ec0fd23255d42e1548aeae2e3e ./EFI/Recovery/grub.efi
Mar 17 01:42:26 Node 0/RP1  completed verification successfully

Mar 17 01:42:26 Install operation 30 completed successfully.
Mar 17 01:42:26 Ending 'install verify' operation 30.
```

Step 3 **install backup** *node-id* **location** *destination*

Creates a hard disk partition and copies the recovery image to the hard disk of the RP and SC card. If a partition already exists, the recovery image is updated.

Example:

```
sysadmin-vm:0_RP0#install backup /harddisk:/ncs6k-dr-boot.tar-<release-version>.zip location 0/RP1

The harddisk  and /misc/scratch/core on 0/RP1 may need to be erased to perform this operation
Do you want to proceed [yes/no]:

Yes
Install operation 9 (install backup) started by user 'root' will continue asynchronously.
Install operation 9 completed successfully.
```

After the operation is completed, use the **show install log** command to verify the details of the operation.

Example:

The following example shows the contents of the log file after **install backup** command is executed.

```
sysadmin-vm:0_RP1# show install log 9
Thu Mar  17 01:55:24.939 UTC
log 9
  Mar 14 18:10:46 Admin install operation 9 started by user 'root'
Mar 14 18:10:46 install backup  /harddisk:/ncs6k-dr-boot.tar-<release-version>.SIT_IMAGE location
0/RP0
Mar 14 18:13:07 all nodes responded,phase 1 done
Mar 14 18:13:07 Install operation 9 completed successfully.
Mar 14 18:13:07 Ending 'install backup' operation 9
```

What to do next

After the router is prepared for disaster recovery, you can recover the router by the recovery image stored in the hard disk recovery partition. For details on recovering the router when it is in a non-responding state, see Recovering a Router, on page 80

Recovering a Router

If the router is in a non-responding state, it can be restored by using a recovery image that is stored in the hard disk recovery partition of the router. Sometimes, even if the router is in a non-responding state, the command-line interface will respond and can be used to execute commands to recover the router. Determine the state of the command-line interface and execute the steps based on the requirement.

The router can be recovered using the following method:

Recovering a Router Using Boot Manager

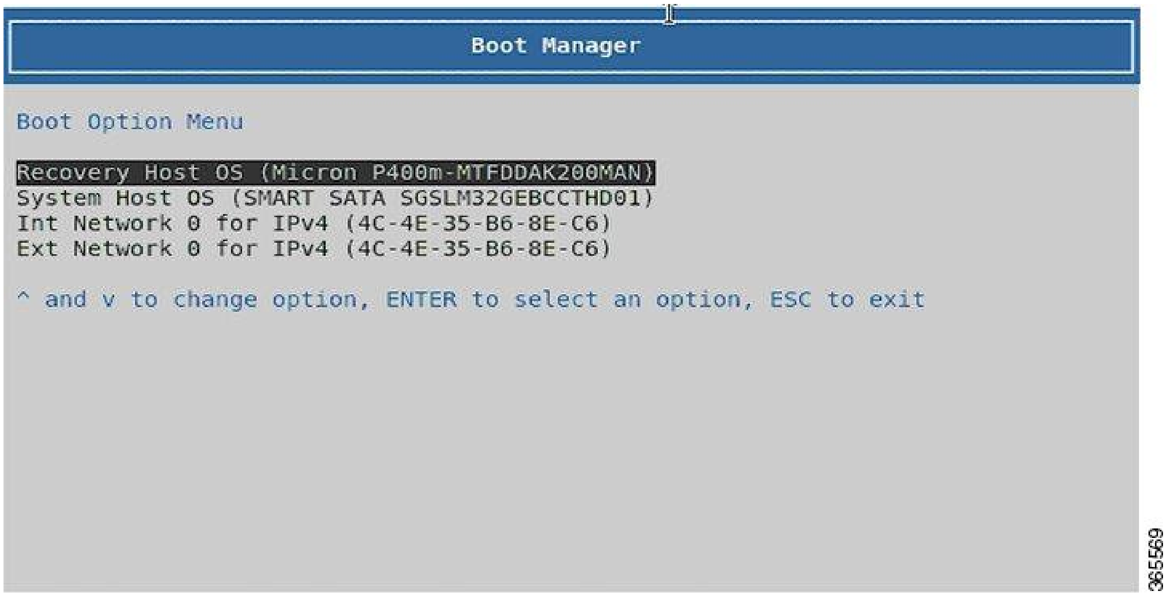
Use this method of recovery if the router is in a non-responding state and the command line interface is not functional.

Before you begin

Ensure that you have prepared the router for disaster recovery by using the information in Preparing the Router for Disaster Recovery, on page 78

Step 1 Power cycle the router.
This results in the entire router rebooting inclusive of all the cards.

Step 2 Press F12 to go to the Boot Manager and select **Recovery Host OS**



```
                              Boot Manager

Boot Option Menu

Recovery Host OS (Micron P400m-MTFDDAK200MAN)
System Host OS (SMART SATA SGSLM32GEBCCTHD01)
Int Network 0 for IPv4 (4C-4E-35-B6-8E-C6)
Ext Network 0 for IPv4 (4C-4E-35-B6-8E-C6)

^ and v to change option, ENTER to select an option, ESC to exit
```

The router is recovered by using the recovery image in the hard disk recovery partition.

Create a Bootable USB Drive

The bootable USB drive is used to re-image the router for the purpose of system upgrade or for booting the router in case of boot failure. The bootable USB drive can be created in two ways:

Create a Bootable USB Drive Using Compressed Boot File

This task is applicable to Cisco IOS XR Software Release 5.0.1.

A bootable USB drive is created by copying a compressed boot file into a USB drive. The USB drive becomes bootable after the contents of the compressed file are extracted.

This task can be completed using Windows, Linux, or MAC operating systems available on your local machine. The exact operation to be performed for each generic step outlined here depends on the operating system in use.

Before you begin

- Have access to a USB drive with a storage capacity that is between 2GB (min) and 32 GB (max). USB 2.0 and USB 3.0 are supported.
- Copy the compressed boot file from the software download page at cisco.com to your local machine. The file name for the compressed boot file is in the format *ncs6k-usb-boot-<release_number>.zip*. For example, *ncs6k-usb-boot-5.0.1.zip*.

SUMMARY STEPS

1. Connect the USB drive to your local machine and format it with FAT32 file system.
2. Copy the compressed boot file to the USB drive.
3. Verify that the copy operation is successful. To verify, compare the file size at source and destination. Additionally, verify the MD5 checksum value.
4. Extract the content of the compressed boot file by unzipping it inside the USB drive. This converts the USB drive to a bootable drive.

DETAILED STEPS

Step 1 Connect the USB drive to your local machine and format it with FAT32 file system.

Step 2 Copy the compressed boot file to the USB drive.

Step 3 Verify that the copy operation is successful. To verify, compare the file size at source and destination. Additionally, verify the MD5 checksum value.

Step 4 Extract the content of the compressed boot file by unzipping it inside the USB drive. This converts the USB drive to a bootable drive.

Note The content of the zipped file ("EFI" and "boot" directories) should be extracted directly into root of the USB drive. If the unzipping application places the extracted files in a new folder, move the "EFI" and "boot" directories to root of the USB drive.

What to do next

Use the bootable USB drive to boot the router or upgrade its image. See:

- Boot the Router Using USB, on page 85
- Perform System Upgrade Using USB, on page 90

Create Bootable USB Drive Using Shell Script

To create the bootable USB drive using shell script, you need an ISO image file and the shell script that creates the boot device. The shell script is already available on the router. Create the bootable USB drive as an preemptive measure when the router is operational. If the router is already unusable, create the bootable USB drive on another active router, or as instructed in the procedure, Create a Bootable USB Drive Using Compressed Boot File, on page 81.

Note The contents of the USB drive is erased during the process of creating the bootable drive.

Before you begin

- Have access to a USB drive with a storage capacity that is between 2GB (min) and 32 GB (max). USB 2.0 and USB 3.0 are supported.
- The ISO image must be present on a network server.

SUMMARY STEPS

1. **copy tftp:***source* **harddisk:***destination*
2. **dir /harddisk:**
3. **dir /usr/bin/usb*.sh**
4. Connect the USB drive.
5. **run**
6. **tail /var/log/messages**
7. **cd** *directory path*
8. *<shell_script_file_name> <location_of_iso_image> <mount_location_of_USB_device>*

DETAILED STEPS

Step 1 **copy tftp:***source* **harddisk:***destination*

Example:

```
RP/0/RP0/CPU0:router# copy tftp://223.255.254.254/image/ncs6k-mini-x.iso harddisk\:/ncs6k-mini-x.iso
```

Copy the ISO image from a network server to the router hard disk.

Step 2 **dir /harddisk:**

Example:

```
RP/0/RP0/CPU0:router#dir /harddisk:
```

Verify that the image is copied. The result of this command displays the ISO file name.

```
Directory of /harddisk:/

    12 -rw-r--r-- 1  7864320 Jun 27 20:30 ncs6k-mini-x.iso
```

Step 3 **dir /usr/bin/usb*.sh**

Example:

```
RP/0/RP0/CPU0:router# dir /usr/bin/usb*.sh
```

Verify that the shell script is available on the router. The *usb-install.sh* script must be present in the command output.

```
Directory of /usr/bin/usb*.sh

430 -rwx------ 1 8456 Jun 20 23:30 /usr/bin/usb-install.sh
```

Step 4 Connect the USB drive.

The USB drive must be connected to the USB port on the RP to which the *iso* image has been copied. The USB port is shown in this figure.

Step 5 **run**

Example:

```
RP/0/RP0/CPU0:router# run
```

Enters the XR VM Linux shell. The router prompt changes to:

```
[xr-vm_node0_RP0_CPU0:/]$
```

Step 6 **tail /var/log/messages**

Example:

```
[xr-vm_node0_RP0_CPU0:/]$ tail /var/log/messages
```

Identifies the device name to which the USB drive is been mapped. The USB drive is auto-discoverable on the XR VM shell.

```
...
...
Aug 16 18:56:07 xr-vm kernel: virtio-pci 0000:c0:08.0: setting latency timer to 64
Aug 16 18:56:07 xr-vm kernel: virtio-pci 0000:c0:08.0: irq 93 for MSI/MSI-X
Aug 16 18:56:07 xr-vm kernel: virtio-pci 0000:c0:08.0: irq 94 for MSI/MSI-X
Aug 16 18:56:07 xr-vm kernel:  vde: vde1
```

In this example, we identify from the last entry that the USB is mapped as "vde".

Step 7 **cd** *directory path*

Example:

```
[xr-vm_node0_RP0_CPU0:/]$ cd /usr/bin
```

Access the directory where the shell script is present.

Step 8 *<shell_script_file_name> <location_of_iso_image> <mount_location_of_USB_device>*

Example:

```
[xr-vm_node0_RP0_CPU0:/usr/bin]$ ./usb-install.sh /harddisk:/ncs6k-mini-x.iso /dev/vde/
```

Runs the script to create the bootable USB drive. After the process is complete, this message is displayed:

```
USB stick set up for EFI boot!
```

What to do next

Use the bootable USB drive to boot the router or upgrade its image. See:

- Boot the Router Using USB, on page 85
- Perform System Upgrade Using USB, on page 90

Boot the Router Using USB

The router can be booted using an external bootable USB drive. This might be required when the router is unable to boot from the installed image. A boot failure may happen when the image gets corrupted. During the USB boot, process the router gets re-imaged with the version available on the USB drive.

The default boot sequence is USB disk, Sata disk, and PXE boot. But from Cisco IOS XR Release 5.2.4 and later, the boot sequence is changed to Sata disk, USB disk and PXE boot.

Note During the USB boot process, the router is completely re-imaged with the ISO image version present in the bootable USB drive. All existing configurations are deleted because the disk 0 content is erased. No optional packages are installed during the upgrade process; they need to be installed after the upgrade is complete.

Before you begin

Create a bootable USB drive. See Create Bootable USB Drive Using Shell Script, on page 83 or Create a Bootable USB Drive Using Compressed Boot File, on page 81 based on the requirement.

Step 1 Connect the USB drive to an RP.

The USB port on the RP is shown in this figure.

Step 2 Connect to the console.

If it is not already connected, connect a terminal to the System Admin console port of the RP. If two RPs are installed on the router, connect to the System Admin console port of both RPs. Start the terminal emulation program on your workstation.

Step 3 Power on the router.

Step 4 Press F12 on the console of the RP to which the USB is not connected. This action displays the boot menu and pauses the boot process. The RP on which the USB is connected should boot normally.

Only the RP having the USB should boot. The booting of other RP is paused.

Step 5 Select the USB drive to boot from USB.

According to the default boot sequence, the Sata disk is the first boot source and the USB drive is the second boot source. During the boot process, the OS image is installed on the router so that in future the router boots without the USB.

Step 6 Press **Enter** to get the host prompt.

Step 7 Login to the host using *root* and *lab* as username and password respectively.

Example:

```
host login: root
Password:
```

If there is no space in the RP, a prompt to either abort installation, or to continue with formatting the disk, is displayed.

The prompt changes to:

```
[Install image, reboot required host:~]$
```

Step 8 Run the **reboot** command.

Example:

```
[Install image, reboot required host:~]$ reboot
```

The RP reboots with the new image. After the booting is completed, specify the root-system username and password. For details, see Setup Root User Credentials and Login to XR VM Console, on page 8.

Step 9 Access the System Admin EXEC mode and reload the RP for which the boot process was paused in Step 4.

Example:

```
sysadmin-vm:0_RP0#hw-module location 0/RP1 reload
```

The shut down RP is reloaded and gets synchronized with the other RP running the new image.

What to do next

- After the booting process is complete, specify the root username and password. For details, see Setup Root User Credentials and Login to XR VM Console, on page 8.
- Install the required optional packages.

Boot the Multi-chassis Router using USB

A multi-chassis router can be booted using an external bootable USB drive when the router is unable to boot from the installed image. A boot failure can happen when the image is corrupt. During the USB boot process, the router is re-imaged with the version available on the USB drive.

The router image can also be upgraded on multi-chassis configuration using an external bootable USB drive. This is required when the router has to be re-imaged, but the ISO image cannot be accessed over the network because of non-availability of network connectivity.

Before you begin

Create a bootable USB drive. See Create Bootable USB Drive Using Shell Script, on page 83.

Step 1 Power off the Line card chassis (LCC) and the Fabric card chassis (FCC).

Step 2 Remove the standby Route processors (RPs) from the LCC.

The initial USB boot recovery procedure must be performed with only the primary RP. The secondary RPs must be removed from both the LCCs.

Step 3 Remove the standby Shelf controllers (SCs) from the FCC.

The initial USB boot recovery procedure must be performed only with the primary SC. The secondary SCs must be removed from the FCCs.

Step 4 Follow the USB boot procedure on LCC0 that is similar to booting a single chassis.

a) Connect the bootable USB drive to an RP.

b) Connect to the console.

If it is not already connected, connect a terminal to the XR VM console port of the RP. If two RPs are installed on the router, connect to the XR VM console port of both RPs. Start the terminal emulation program on your workstation.

c) Power on the router.

d) RP automatically boots from the USB.

According to the default boot sequence, the USB drive is the first source to boot the router. The router automatically boots from the USB device connected to it. During the boot process, the OS image is installed on the router. This helps to boot the router without the USB in future.

```
Cisco BIOS version : <version>
BIOS Build Date : MM/DD/YYYY by
System Memory Speed : 1600 MHz
Processor Type : Intel(R) Xeon(R) CPU E5-2448L @ 1.80GHz

Press F12 to goto Boot Manager..

Booting EFI USB Device (KingstonDataTraveler G3)..

GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from USB..
Loading Kernel..
Loading initrd..
?[    6.660104] i8042.c: No controller found.
Starting udev: [  OK  ]
Setting hostname host:  [  OK  ]
Checking filesystems:[  OK  ]
Remounting root filesystem in read-write mode:  [  OK  ]
Entering non-interactive startup
Bringing up loopback interface:  [  OK  ]
Starting system logger: [  OK  ]
Starting kernel logger: [  OK  ]
Starting kdump:[  OK  ]
Starting system message bus: [  OK  ]
Starting smartd: [  OK  ]
Generating SSH1 RSA host key: [  OK  ]
Generating SSH2 RSA host key: [  OK  ]
Generating SSH2 DSA host key: [  OK  ]
Starting sshd: [  OK  ]
Starting xinetd: [  OK  ]
Fri Aug 22 18:05:29 UTC 2014: Running in  Data LV support model
/etc/rc3.d/S60xrnginstall: line 135: SIMULATION: readonly variable
Fri Aug 22 18:05:29 UTC 2014: Prepping System with calvados.iso
Fri Aug 22 18:05:29 UTC 2014: Installer will install image on sda
Fri Aug 22 18:05:29 UTC 2014: Running in LVM support model
Fri Aug 22 18:05:31 UTC 2014: Partition creation on /dev/sda took 1 seconds
Fri Aug 22 18:05:31 UTC 2014: File system creation on /dev/sda1 took 0 seconds
```

e) Remove the USB drive.

After the initial boot sequences are completed, a message is displayed: `Running install image: Please reboot the system`. Remove the USB drive.

Note The USB drive should not be left connected on the router during regular operation. If the router reloads when the USB drive is connected, all existing configurations are deleted as the router is re-imaged.

f) Press Enter to get the host prompt.

g) Login to the host using *root* and *lab* as username and password respectively.

Example:

```
host login: root Password:
The prompt changes to:
[Install image, reboot required host:~]$
```

h) Run the reboot command.

Example:

```
[Install image, reboot required host:~]$ reboot
```

The RP reboots with the new image. After the booting is completed, specify "**`root`**" and "**`system`**" as username and password respectively.

i) Enter username and password when the router prompts for the same.

Example:

```
!!!!!!!!!!!!!!!!!!!! NO root-system username is configured. Need to configure root-system
username. !!!!!!!!!!!!!!!!!!!!

         --- Administrative User Dialog ---


  Enter root-system username:
  % Entry must not be null.

  Enter root-system username: root
  Enter secret:
Use the 'configure' command to modify this configuration.
User Access Verification

Username: root
Password:
```

j) Confirm that the router has the new image on RP.

Example:

```
sysadmin-vm:0_RP0# show version
Fri Aug  22 18:45:34.794 UTC

Cisco IOS XR Admin Software, Version <release-version>
Copyright (c) 2013-2014 by Cisco Systems, Inc.

Build Information:
 Built By     :
 Built On     : Tue Aug 19 00:50:48 PDT 2014
 Build Host   : iox-lnx-003
 Workspace    : /<path>
 Version      : <release-version>
 Location     : /opt/cisco/calvados/packages/

BIOS Version  : 13.8

System uptime is 28 minutes.
```

Step 5 Configure LCC0 with **chassis serial configuration** and **fabric plane configuration**.

Example:

```
sysadmin-vm:0_RP0(config)# chassis serial FLM17326A2J
sysadmin-vm:0_RP0(config-serial-FLM17326A2J)#  rack 1
sysadmin-vm:0_RP0(config-serial-FLM17326A2J)# !
sysadmin-vm:0_RP0(config-serial-FLM17326A2J)# chassis serial FLM17326A2K
sysadmin-vm:0_RP0(config-serial-FLM17326A2K)#  rack 0
sysadmin-vm:0_RP0(config-serial-FLM17326A2K)# !
sysadmin-vm:0_RP0(config-serial-FLM17326A2K)# chassis serial FMP17210228
sysadmin-vm:0_RP0(config-serial-FMP17210228)#  rack F0
sysadmin-vm:0_RP0(config-serial-FMP17210228)# !
sysadmin-vm:0_RP0(config-serial-FMP17210228)# chassis serial FMP17380420
sysadmin-vm:0_RP0(config-serial-FMP17380420)#  rack F1
sysadmin-vm:0_RP0(config-serial-FMP17380420)# !
sysadmin-vm:0_RP0(config-serial-FMP17380420)#
Mon Aug  25 22:27:49.594 UTC
Uncommitted changes found, commit them? [yes/no/CANCEL] yes

sysadmin-vm:0_RP0# conf t
Mon Aug  25 22:47:38.999 UTC
Entering configuration mode terminal
sysadmin-vm:0_RP0 (config)# controller fabric plane 0
sysadmin-vm:0_RP0 (config-plane-0)# no shutdown
sysadmin-vm:0_RP0(config-plane-0)# instance 0
sysadmin-vm:0_RP0(config-instance-0)#   location F0/FC6
sysadmin-vm:0_RP0(config-instance-0)#  !
sysadmin-vm: 0_RP0 (config-instance-0)# !
sysadmin-vm:0_RP0(config-instance-0)# controller fabric plane 1
sysadmin-vm:0_RP0(config-plane-1)#  no shutdown
Mon Aug  25 22:47:45.944 UTC
sysadmin-vm:0_RP0(config-plane-1)#  instance 0
sysadmin-vm:0_RP0(config-instance-0)#   location F1/FC6
sysadmin-vm:0_RP0(config-instance-0)#  !
sysadmin-vm:0_RP0(config-instance-0)# !
sysadmin-vm:0_RP0(config-instance-0)# controller fabric plane 2
sysadmin-vm:0_RP0(config-plane-2)#  no shutdown
Mon Aug  25 22:47:45.958 UTC
sysadmin-vm:0_RP0(config-plane-2)#  instance 0
sysadmin-vm:0_RP0(config-instance-0)#   location F0/FC7
sysadmin-vm:0_RP0(config-instance-0)#  !
sysadmin-vm:0_RP0(config-instance-0)# !
sysadmin-vm:0_RP0(config-instance-0)# controller fabric plane 3
sysadmin-vm:0_RP0(config-plane-3)#  no shutdown
Mon Aug  25 22:47:45.974 UTC
sysadmin-vm:0_RP0(config-plane-3)#  instance 0
sysadmin-vm:0_RP0(config-instance-0)#   location F1/FC7
sysadmin-vm:0_RP0(config-instance-0)#  !
sysadmin-vm:0_RP0(config-instance-0)# !
sysadmin-vm:0_RP0(config-instance-0)# controller fabric plane 4
sysadmin-vm:0_RP0(config-plane-4)#  no shutdown
Mon Aug  25 22:47:45.983 UTC
sysadmin-vm:0_RP0(config-plane-4)#  instance 0
sysadmin-vm:0_RP0(config-instance-0)#   location F0/FC8
sysadmin-vm:0_RP0(config-instance-0)#  !
sysadmin-vm:0_RP0(config-instance-0)# !
sysadmin-vm:0_RP0(config-instance-0)# controller fabric plane 5
sysadmin-vm:0_RP0(config-plane-5)#  no shutdown
Mon Aug  25 22:47:45.993 UTC
sysadmin-vm:0_RP0(config-plane-5)#  instance 0
sysadmin-vm:0_RP0(config-instance-0)#   location F1/FC8
sysadmin-vm:0_RP0(config-instance-0)#  !
sysadmin-vm:0_RP0(config-instance-0)# !
Mon Aug  25 22:47:55.321 UTC
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
```

Step 6 Power off the LCC0 chassis.

Step 7 Follow Steps 4 to 6 for LCC1, FCC0 and FCC1.

Step 8 Power up all the chassis at the same time. The system boots with the new image.

Note After the router is reboots, all primary RPs have the new image.

```
sysadmin-vm:0_RP0# show install active
Fri Aug  22 21:43:09.700 UTC
 Node 1/RP0 [RP]
    Active Packages: 1
       ncs6k-sysadmin-<release-version> version=<release-version> [Boot image]

 Node 0/RP0 [RP]
    Active Packages: 1
       ncs6k-sysadmin-<release-version> version=<release-version> [Boot image]

 Node F0/SC0 [SC]
    Active Packages: 1
       ncs6k-sysadmin-<release-version> version=<release-version> [Boot image]

 Node F1/SC0 [SC]
    Active Packages: 1
       ncs6k-sysadmin-<release-version> version=<release-version> [Boot image]

 Node 1/1 [LC]
    Active Packages: 1
       ncs6k-sysadmin-<release-version> version=<release-version> [Boot image]

 Node 0/3 [LC]
    Active Packages: 1
       ncs6k-sysadmin-<release-version> version=<release-version> [Boot image]
```

```
sysadmin-vm:1_RP0# show chassis
Thu Aug  21 19:42:41.599 UTC
Serial Num    Rack Num    Rack Type   Rack State  Data Plane  Ctrl Plane
--------------------------------------------------------------------------
FMP12180264   0           LCC         UP          NCONN       CONN
FMP12180281   1           LCC         UP          NCONN       CONN
FMP12240401   F1          FCC         UP          NCONN       CONN
FMP17400526   F0          FCC         UP          NCONN       CONN
```

Step 9 Insert secondary RPs in both LCCs.

Step 10 Insert secondary SC cards in both FCCs.

Note On inserting the secondary SC cards on each FCC, the SC card triggers an internal PXE boot and starts with the new image.

Step 11 Verify that the router has the new image on all RPs, SCs, and LCs.

Perform System Upgrade Using USB

The router image can be upgraded using an external bootable USB drive. This may be required when the router is to be re-imaged, but the ISO image cannot be accessed over the network. It may happen when the network connectivity is unavailable.

Note During an upgrade, all existing configurations are deleted because the disk 0 content is erased.

Before you begin

- Create a bootable USB drive. See Create Bootable USB Drive Using Shell Script, on page 83 or Create a Bootable USB Drive Using Compressed Boot File, on page 81 based on requirement.
- Ensure that the router BIOS version is 9.10, or higher.
  - Verify the BIOS version using the **show fpd package** command in the System Admin EXEC mode.
  - Verify the actual state of all field-programmable gate array (FPGA) of the system and whether it requires an upgrade or not using the **show hw-module fpd** command in System Admin EXEC mode.
  - If required, upgrade the BIOS using the **upgrade hw-module location all fpd BIOS\ FPD** command in the System Admin EXEC mode.

Step 1 **hw-module location** *node-id* **shutdown**

Example:

```
sysadmin-vm:0_RP0#hw-module location 0/RP1 shutdown
```

Shut down one RP. In this example, the RP1 is shut down. During the system upgrade, only one RP should be operational.

Step 2 Connect the USB drive.

The USB drive must be connected to the USB port on the operational RP. The USB port is shown in this figure.

Step 3 *hw-module* **location** *node-id* **reload**

Example:

```
sysadmin-vm:0_RP0#hw-module location 0/RP0 reload
```

Reload the RP on which the USB is connected. As the RP reloads, it boots from the USB drive and gets re-imaged.

Step 4 Remove the USB drive.

After the initial boot sequences are complete, this message is displayed:

```
Running install image: Please reboot the system
```

On receiving this message, remove the USB drive.

Note The USB drive should not be left connected on the router during regular operation. If the router reloads when the USB drive is connected, all existing configurations are deleted as the router gets re-imaged.

Step 5 Press **Enter** to get the host prompt.

Step 6 Login to the host using *root* and *lab* as username and password respectively.

Example:

```
host login: root
Password:
```

The prompt changes to:

```
[Install image, reboot required host:~]$
```

Step 7 Run the **reboot** command.

Example:

```
[Install image, reboot required host:~]$ reboot
```

The RP reboots with the new image. After the booting is completed, specify the root-system username and password. For details, see Setup Root User Credentials and Login to XR VM Console, on page 8.

Step 8 Access the System Admin EXEC mode and reload the RP that was shut down in Step 1.

Example:

```
sysadmin-vm:0_RP0#hw-module location 0/RP1 reload
```

The shut down RP is reloaded and gets synchronized with the other RP running the new image.

What to do next

- Run the **show version** command in the XR EXEC mode to verify that the new image version is successfully installed.
- Install the required optional packages.