System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.0.x

First Published: 2015-12-23

Last Modified: 2016-07-13

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

CONTENTS

PREFACE

Preface v

Changes to This Document v

Changes to This Document v

Obtaining Documentation and Submitting a Service Request vi

CHAPTER 1

Cisco NCS 5500 Product Overview 1

Cisco NCS 5500 Product Overview 1

Command Modes 1

CHAPTER 2

Bring-up the Router 3

Boot the Router 3

Setup Root User Credentials 4

Access the System Admin Console 5

Configure the Management Port 6

Perform Clock Synchronization with NTP Server 7

CHAPTER 3

Perform Preliminary Checks 9

Verify Software Version 9

Verify Status of Hardware Modules 10

Verify Firmware Version 11

Verify SDR Information 13

Verify Interface Status 15

CHAPTER 4

Create User Profiles and Assign Privileges 17

Create a User Profile 18

Create a User Group 20

Create Command Rules 22
Create Data Rules 24
Change Disaster-recovery Username and Password 26
Recover Password using PXE Boot 27

CHAPTER 5 **Perform System Upgrade and Install Feature Packages 29**
Upgrading the System 29
Upgrading Features 30
Workflow for Install Process 31
Install Packages 31
Install Prepared Packages 36
Uninstall Packages 39

CHAPTER 6 **Manage Automatic Dependency 43**
Update RPMs and SMUs 44
Upgrade Base Software Version 45

CHAPTER 7 **Disaster Recovery 47**
Boot using USB Drive 47
Create a Bootable USB Drive Using Compressed Boot File 47
Boot the Router Using USB 48
Boot using iPXE 49
Zero Touch Provisioning 49
Setup DHCP Server 50
Invoke ZTP 52
Invoke ZTP Manually 52
Boot the Router Using iPXE 53

Preface

This Preface contains these sections:

- Changes to This Document, on page v
- Changes to This Document, on page v
- Obtaining Documentation and Submitting a Service Request, on page vi

Changes to This Document

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

Date	Summary
July 2016	Republished with documentation updates for Cisco IOS XR Release 6.0.2 features.
April 2016	Removed the following packages from the 'Upgrading Features' section: • Infra - ncs5500-infra-1.0.0.0-r60023I.x86_64.rpm • OS - ncs5500-os-1.0.0.0-r60023I.x86_64.rpm • os-support - ncs5500-os-support-1.0.0.0-r60023I.x86_64.rpm
December 2015	Initial release of this document.

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

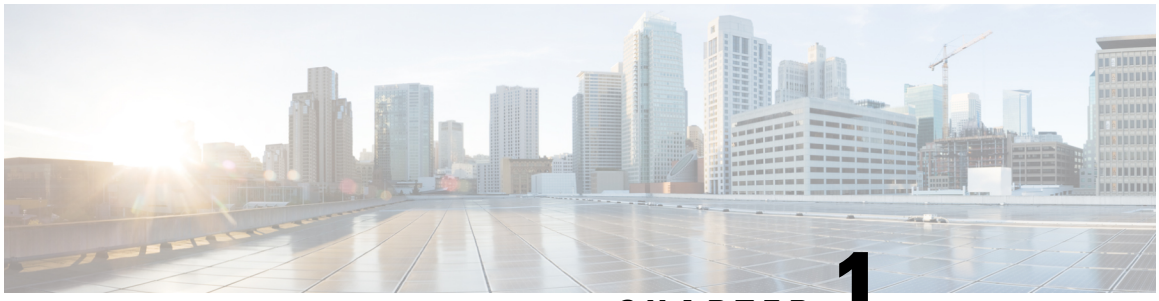
Date	Summary
November 2016	Republished for R6.1.2.

Date	Summary
August 2016	Initial release of this document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 1

Cisco NCS 5500 Product Overview

Cisco NCS 5500 system is a high fault-resilient platform, which provides next generation data-center switching environment with high bandwidth and low latency.

Cisco NCS 5500 system provides:

- A modular router with a centralized route processor with multiple line card per chassis.
- High density, high performance, and merchant silicon-based line cards.
- IP and MPLS switching at a low cost per 100G.
- Label Switched Router (LSR) and possible Light Label switched Edge Router (LER) features and functionality with limited hardware scale and software functionality.

- Cisco NCS 5500 Product Overview, on page 1
- Command Modes, on page 1

Cisco NCS 5500 Product Overview

Cisco NCS 5500 system is a high fault-resilient platform, which provides next generation data-center switching environment with high bandwidth and low latency.

Cisco NCS 5500 system provides:

- A modular router with a centralized route processor with multiple line card per chassis.
- High density, high performance, and merchant silicon-based line cards.
- IP and MPLS switching at a low cost per 100G.
- Label Switched Router (LSR) and possible Light Label switched Edge Router (LER) features and functionality with limited hardware scale and software functionality.

Command Modes

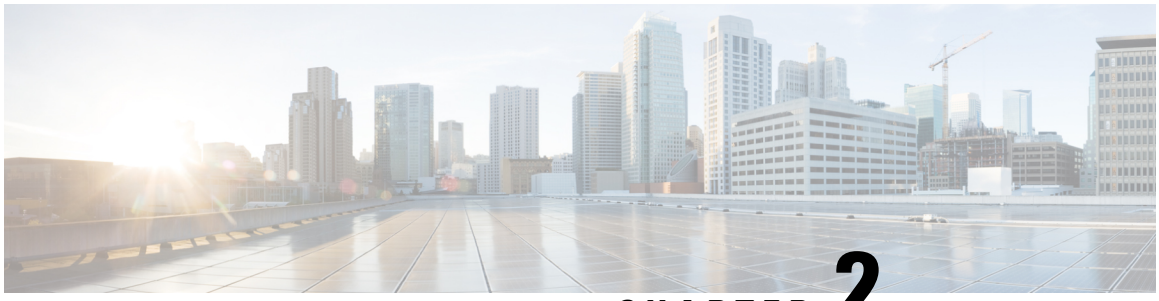
The router runs on virtualized Cisco IOS XR software. Therefore, the CLI commands must be executed on virtual machines, namely the XR LXC and the System Admin LXC. This table lists the command modes for the LXCs.

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

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

System Admin EXEC mode
(System Admin LXC execution mode)
	Run commands on the System Admin LXC 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 LXCconfiguration mode)
	Run configuration commands on the System Admin LXC 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)#`



CHAPTER 2

Bring-up the Router

After installing the hardware, boot the router. Connect to the XR console port and power on the router. The router 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 iPXE boot or 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 console and get the router prompt. The first user created in XR console is synchronized to the System Admin console. From the XR console, access the System Admin console to configure system administration settings.

- Boot the Router, on page 3
- Setup Root User Credentials, on page 4
- Access the System Admin Console, on page 5
- Configure the Management Port, on page 6
- Perform Clock Synchronization with NTP Server, on page 7

Boot the Router

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

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

Step 2 Start the terminal emulation program on your workstation.

For modular chassis RP, the console settings are baud rate 9600 bps, no parity, 2 stop bits and 8 data bits. For fixed chassis, the console settings are baud rate 115200 bps, no parity, 2 stop bits and 8 data bits. The baud rate is set by default and cannot be changed.

Step 3 Power on the router.

Connect the power chord to Power Entry Module (PEM) and the router boots up. The boot process details is displayed on the console screen of the terminal emulation program.

Step 4 Press **Enter**.

The boot process is complete when the system prompts to enter the root-system username. 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.

What to do next

Specify the root username and password.

Setup Root User Credentials

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 (root-lr) console, the System Admin LXC (root-system), and as disaster-recovery credentials.

Before you begin

The boot process must be complete. For details on how to initiate the boot process, see Bring-up the Router, on page 3.

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*

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 console. It is also mapped as the "root-system" user on the System Admin console.

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*

Enter the password for the root user. The character range of the password is between 6 and 253 charcters. 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*

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*

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

Step 5 **Password:** *password*

Enter the password of the root user. The correct password displays the router prompt. You are now logged into the XR LXC console.

Step 6 (Optional) **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 console.
- Configure system administration settings from the System Admin prompt. The System Admin prompt is displayed on accessing the System Admin console. For details on how to get the System Admin prompt, see Access the System Admin Console, on page 5.

Access the System Admin Console

You must login to the System Admin console through the XR console to perform all system administration and hardware management setups.

SUMMARY STEPS

1. Login to the XR console as the root user.
2. **admin**
3. (Optional) **exit**

DETAILED STEPS

Step 1 Login to the XR 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
```

Step 3 (Optional) **exit**

Return to the XR mode from the System Admin mode.

Configure the Management Port

To use the 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 and Ethernet 1 on RP are the management ports. Ensure that the port is connected to management network.

Note The Physical port MgmtEth0/RP0/CPU0/1 on XR must be shut down while configuring manageability applications.

SUMMARY STEPS

1. **configure**
2. **interface MgmtEth** *rack/slot/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/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 10.1.1.1/8
```

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. With a terminal emulation program, establish a SSH or telnet connection to the management interface port using its IP address. 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.

Perform Clock Synchronization with NTP Server

There are independent system clocks for the XR console and the System Admin console. 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 console. After the XR console clock is synchronized, the System Admin console clock will automatically synchronize with the XR console clock.

Before you begin

Configure and connect to the management port.

SUMMARY STEPS

1. **configure**
2. **ntp server** *server_address*

DETAILED STEPS

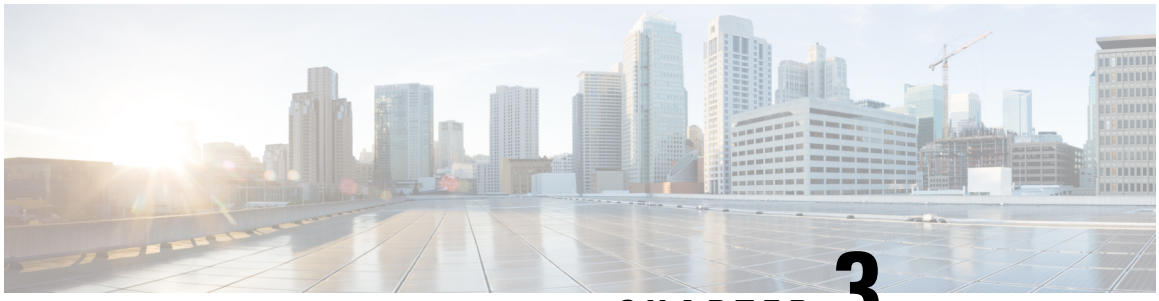
Step 1 **configure**

Step 2 **ntp server** *server_address*

Example:

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

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



CHAPTER 3

Perform Preliminary Checks

After successfully logging into the 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 Software Version, on page 9
- Verify Status of Hardware Modules, on page 10
- Verify Firmware Version, on page 11
- Verify SDR Information, on page 13
- Verify Interface Status, on page 15

Verify Software Version

The 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 and its various components.

Example

```
Cisco IOS XR Software, Version <release-version>
Copyright (c) 2013-2015 by Cisco Systems, Inc.

Build Information:
Built By : <user>
Built On : <date and time stamp>
Build Host :
Version : <release-version>
Location : /opt/cisco/XR/packages/

cisco NCS-5500 () processor
System uptime is 3 hours, 42 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 29.

Verify Status of Hardware Modules

Hardware modules include RPs, LCs, fan trays, 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.

SUMMARY STEPS

1. **admin**
2. **show platform**

DETAILED STEPS

Step 1 **admin**

Example:

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

Enters System Admin EXEC mode.

Step 2 **show platform**

Example:

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

Displays the list of hardware modules detected on the router.

```
Location  Card Type              HW State      SW State      Config State
```

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

0/0       NC55-36X100G            OPERATIONAL   OPERATIONAL   NSHUT
0/1       NC55-36X100G            OPERATIONAL   OPERATIONAL   NSHUT
0/2       NC55-36X100G            OPERATIONAL   OPERATIONAL   NSHUT
0/3       NC55-36X100G            OPERATIONAL   OPERATIONAL   NSHUT
0/4       NC55-36X100G            OPERATIONAL   OPERATIONAL   NSHUT
0/5       NC55-36X100G            OPERATIONAL   OPERATIONAL   NSHUT
0/6       NC55-36X100G            OPERATIONAL   OPERATIONAL   NSHUT
0/7       NC55-36X100G            OPERATIONAL   OPERATIONAL   NSHUT
0/RP0     NC55-RP                 OPERATIONAL   OPERATIONAL   NSHUT
0/RP1     NC55-RP                 OPERATIONAL   OPERATIONAL   NSHUT
0/FC0     NC55-5508-FC            OPERATIONAL   OPERATIONAL   NSHUT
0/FC1     NC55-5508-FC            OPERATIONAL   OPERATIONAL   NSHUT
0/FC2     NC55-5508-FC            OPERATIONAL   OPERATIONAL   NSHUT
0/FC3     NC55-5508-FC            OPERATIONAL   OPERATIONAL   NSHUT
0/FC4     NC55-5508-FC            OPERATIONAL   OPERATIONAL   NSHUT
0/FC5     NC55-5508-FC            OPERATIONAL   OPERATIONAL   NSHUT
0/FT0     NC55-5508-FAN           OPERATIONAL   N/A           NSHUT
0/FT1     NC55-5508-FAN           OPERATIONAL   N/A           NSHUT
0/FT2     NC55-5508-FAN           OPERATIONAL   N/A           NSHUT
0/SC0     NC55-SC                 OPERATIONAL   OPERATIONAL   NSHUT
0/SC1     NC55-SC                 OPERATIONAL   OPERATIONAL   NSHUT
```

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 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. **show hw-module fpd**

DETAILED STEPS

show hw-module fpd

Example:

```
RP/0/RP0/CPU0:router# show hw-module fpd

                                                                  FPD Versions
                                                                 ==============
Location  Card type         HWver FPD device       ATR Status   Run    Programd
--------------------------------------------------------------------------------
0/0       NC55-36X100G      0.108 Bootloader           CURRENT    1.15    1.15
0/0       NC55-36X100G      0.108 IOFPGA               CURRENT    0.08    0.08
0/1       NC55-36X100G      0.203 Bootloader           CURRENT    1.15    1.15
0/1       NC55-36X100G      0.203 IOFPGA               CURRENT    0.08    0.08
0/2       NC55-36X100G      0.203 Bootloader           CURRENT    1.15    1.15
0/2       NC55-36X100G      0.203 IOFPGA               CURRENT    0.08    0.08
0/3       NC55-36X100G      0.203 Bootloader           CURRENT    1.15    1.15
```

```
0/3       NC55-36X100G      0.203 IOFPGA              CURRENT    0.08    0.08
0/4       NC55-36X100G      0.203 Bootloader          CURRENT    1.15    1.15
0/4       NC55-36X100G      0.203 IOFPGA              CURRENT    0.08    0.08
0/5       NC55-36X100G      0.203 Bootloader          CURRENT    1.15    1.15
0/5       NC55-36X100G      0.203 IOFPGA              CURRENT    0.08    0.08
0/6       NC55-36X100G      0.203 Bootloader          CURRENT    1.15    1.15
0/6       NC55-36X100G      0.203 IOFPGA              CURRENT    0.08    0.08
0/7       NC55-36X100G      0.203 Bootloader          CURRENT    1.15    1.15
0/7       NC55-36X100G      0.203 IOFPGA              CURRENT    0.08    0.08
0/RP0     NC55-RP           1.1   Bootloader          CURRENT    9.19    9.19
0/RP0     NC55-RP           1.1   IOFPGA              CURRENT    0.06    0.06
0/RP1     NC55-RP           1.1   Bootloader          CURRENT    9.19    9.19
0/RP1     NC55-RP           1.1   IOFPGA              CURRENT    0.06    0.06
0/FC0     NC55-5508-FC      0.109 Bootloader          CURRENT    1.64    1.64
0/FC0     NC55-5508-FC      0.109 IOFPGA              CURRENT    0.11    0.11
0/FC1     NC55-5508-FC      0.109 Bootloader          CURRENT    1.64    1.64
0/FC1     NC55-5508-FC      0.109 IOFPGA              CURRENT    0.11    0.11
0/FC2     NC55-5508-FC      0.109 Bootloader          CURRENT    1.64    1.64
0/FC2     NC55-5508-FC      0.109 IOFPGA              CURRENT    0.11    0.11
0/FC3     NC55-5508-FC      0.109 Bootloader          CURRENT    1.64    1.64
0/FC3     NC55-5508-FC      0.109 IOFPGA              CURRENT    0.11    0.11
0/FC4     NC55-5508-FC      0.109 Bootloader          CURRENT    1.64    1.64
0/FC4     NC55-5508-FC      0.109 IOFPGA              CURRENT    0.11    0.11
0/FC5     NC55-5508-FC      0.109 Bootloader          CURRENT    1.64    1.64
0/FC5     NC55-5508-FC      0.109 IOFPGA              CURRENT    0.11    0.11
0/SC0     NC55-SC           1.4   Bootloader          CURRENT    1.64    1.64
0/SC0     NC55-SC           1.4   IOFPGA              CURRENT    0.06    0.06
0/SC1     NC55-SC           1.4   Bootloader          CURRENT    1.64    1.64
0/SC1     NC55-SC           1.4   IOFPGA              CURRENT    0.06    0.06
```

Displays the list of hardware modules detected on the router.

Note This command can be run from both XR LXC and System Admin LXC modes.

In the above output, some of the significant fields are:

- FPD Device- Name of the hardware component such as FPD, CFP, and so on.
- ATR-Attribute of the hardware component. Some of the attributes are:
  - B- Backup Image
  - S-Secure Image
  - P-Protected Image
- Status- Upgrade status of the firmware. The different states are:
  - CURRENT-The firmware version is the latest version.
  - 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.
  - RLOAD REQ-The upgrade has been completed, and the ISO image requires a reload.
  - 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.

- Running- Current version of the firmware running on the FPD.

What to do next

If it is required to replace an LC or RP, use one of the two methods:

- Manual FPD upgrade:
  1. Insert the new LC.
  2. If `auto fpd upgrade` option is enabled, use the **show hw-module fpd** command to check the status of the FPDs that are not activated. If the status is `RELOAD_REQ`, reload the LC or RP.
  3. If `auto fpd upgrade` option is not enabled, use the **show hw-module fpd** command to check the FPDs that need to be upgraded. It is recommended to upgrade all the FPDs at once.
  4. Use manual FPD upgrade to upgrade all FPDs for LC. Reload the LC once the FPD upgrade is successful.

- Automatic FPD upgrade:
  1. If automatic FPD upgrade is not configured, use **fpd auto-upgrade** command to configure.
  2. Insert the LC.
  3. After the LC comes up, use the **show hw-module fpd** command to check the status of the FPDs that are not activated. If the status is `RELOAD_REQ`, reload the LC or RP.
  4. Verify that all the other FPDs in the same node are either in `CURRENT` or `RELOAD_REQ` state before starting a manual reload of the router.

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 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 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.

SUMMARY STEPS

1. **admin**
2. **show sdr**

DETAILED STEPS

Step 1 **admin**

Example:

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

Enters mode.

Step 2 **show sdr**

Example:

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

Displays the SDR information for every node.

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

sdr default-sdr
 location 0/0/VM1
  sdr-id             2
  IP Address of VM   192.0.4.3
  MAC address of VM  A4:6C:2A:2B:AA:A6
  VM State           RUNNING
  start-time         2015-12-03T15:38:38.74514+00:00
  Last Reload Reason "SMU:Reboot triggered by install"
  Reboot Count       2
 location 0/1/VM1
  sdr-id             2
  IP Address of VM   192.0.8.3
  MAC address of VM  B0:AA:77:E7:5E:DA
  VM State           RUNNING
  start-time         2015-12-03T15:38:39.730036+00:00
  Last Reload Reason "SMU:Reboot triggered by install"
  Reboot Count       2
 location 0/2/VM1
  sdr-id             2
  IP Address of VM   192.0.12.3
  MAC address of VM  B0:AA:77:E7:67:34
  VM State           RUNNING
  start-time         2015-12-03T15:38:38.886947+00:00
  Last Reload Reason "SMU:Reboot triggered by install"
  Reboot Count       2
 location 0/3/VM1
  sdr-id             2
  IP Address of VM   192.0.16.3
  MAC address of VM  B0:AA:77:E7:58:86
  VM State           RUNNING
  start-time         2015-12-03T15:38:40.391205+00:00
  Last Reload Reason "SMU:Reboot triggered by install"
  Reboot Count       2
 location 0/4/VM1
  sdr-id             2
  IP Address of VM   192.0.20.3
  MAC address of VM  B0:AA:77:E7:46:C2
  VM State           RUNNING
  start-time         2015-12-03T15:38:39.84469+00:00
  Last Reload Reason "SMU:Reboot triggered by install"
  Reboot Count       2
 location 0/5/VM1
  sdr-id             2
```

```
 IP Address of VM   192.0.24.3
 MAC address of VM  B0:AA:77:E7:84:40
 VM State           RUNNING
 start-time         2015-12-04T03:48:24.017443+00:00
 Last Reload Reason "VM_REQUESTED_UNGRACEFUL_RELOAD:Headless SDR"
 Reboot Count       3
location 0/6/VM1
 sdr-id             2
 IP Address of VM   192.0.28.3
 MAC address of VM  B0:AA:77:E7:55:FE
 VM State           RUNNING
 start-time         2015-12-03T15:38:38.74753+00:00
 Last Reload Reason "SMU:Reboot triggered by install"
 Reboot Count       2
location 0/7/VM1
 sdr-id             2
 IP Address of VM   192.0.32.3
 MAC address of VM  B0:AA:77:E7:60:C6
 VM State           RUNNING
 start-time         2015-12-03T15:38:38.691481+00:00
 Last Reload Reason "SMU:Reboot triggered by install"
 Reboot Count       2
location 0/RP0/VM1
 sdr-id             2
 IP Address of VM   192.0.108.4
 MAC address of VM  10:05:CA:D7:FE:6F
 VM State           RUNNING
 start-time         2015-12-04T07:03:04.549294+00:00
 Last Reload Reason CARD_SHUTDOWN
 Reboot Count       1
location 0/RP1/VM1
 sdr-id             2
 IP Address of VM   192.0.112.4
 MAC address of VM  10:05:CA:D8:3F:43
 VM State           RUNNING
 start-time         2015-12-04T09:21:42.083046+00:00
 Last Reload Reason CARD_SHUTDOWN
 Reboot Count       1
```

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 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.

SUMMARY STEPS

1. **show ipv4 interface summary**

DETAILED STEPS

show ipv4 interface summary

Example:

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

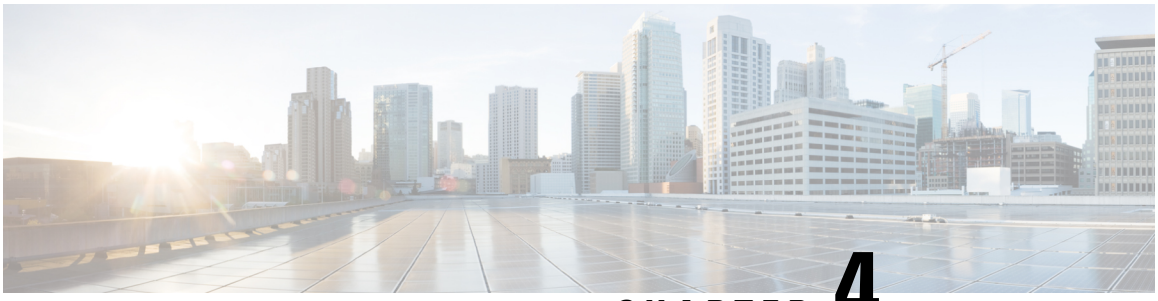
When a router is turned on for the first time, all interfaces are in the 'unassigned' state. Verify that the total number of interfaces displayed in the result matches with the actual number of interfaces present on the router.

```
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.



CHAPTER 4

Create User Profiles and Assign Privileges

To provide controlled access to the System Admin configurations on the 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 LXC. It can be configured only from the XR LXC.

Configure AAA authorization to restrict users from uncontrolled access. If AAA authorization is not configured, the command and data rules associated to the groups that are assigned to the user are bypassed. An IOS-XR user can have full read-write access to the IOS-XR configuration through Network Configuration Protocol (NETCONF), google-defined Remote Procedure Calls (gRPC) or any YANG-based agents. In order to avoid granting uncontrolled access, enable AAA authorization before setting up any configuration.

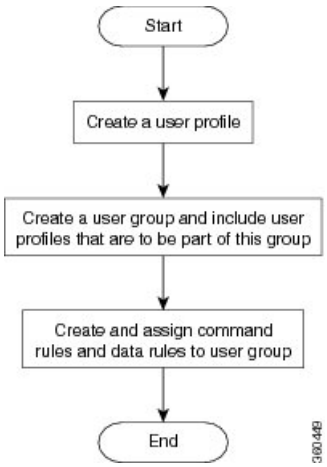
Note If any user on XR is deleted, the local database checks whether there is a first user on System Admin VM.

- 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.

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 1: Workflow for Creating User Profiles



Note The root-lr user, created for the XR LXC during initial router start-up, is mapped to the root-system user for the System Admin LXC. The root-system user has superuser permissions for the System Admin LXC 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 18
- Create a User Group, on page 20
- Create Command Rules, on page 22
- Create Data Rules, on page 24
- Change Disaster-recovery Username and Password, on page 26
- Recover Password using PXE Boot, on page 27

Create a User Profile

Create new users for the System Admin LXC. 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 LXC console, based on assigned privileges.

The router supports a maximum of 1024 user profiles.

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

XR VM and System Admin VM User Profile Synchronization

When the user profile is created for the first time in XR VM, the user name and password are synced to the System Admin VM if no user already exists in System Admin VM.

However, the subsequent password change or user deletion in XR VM for the synced user is not synchronized with the System Admin VM.

Therefore, the passwords in XR VM and System Admin VM may not be the same. Also, the user synced with the System Admin VM will not be deleted if the user is deleted in XR VM.

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

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 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 LXC.

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 20.
- Create command rules that apply to the user group. See Create Command Rules, on page 22.
- Create data rules that apply to the user group. See Create Data Rules, on page 24.

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 User Profiles and Assign Privileges, on page 17.

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 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 22.
- Create data rules. See Create Data Rules, on page 24.

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 20.

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 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 24.

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 20.

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 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 console. 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 console is corrupted.
- Access the system through the management port, when, for some reason, the System Admin console is not working.
- Create new users by accessing the System Admin console 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.

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 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

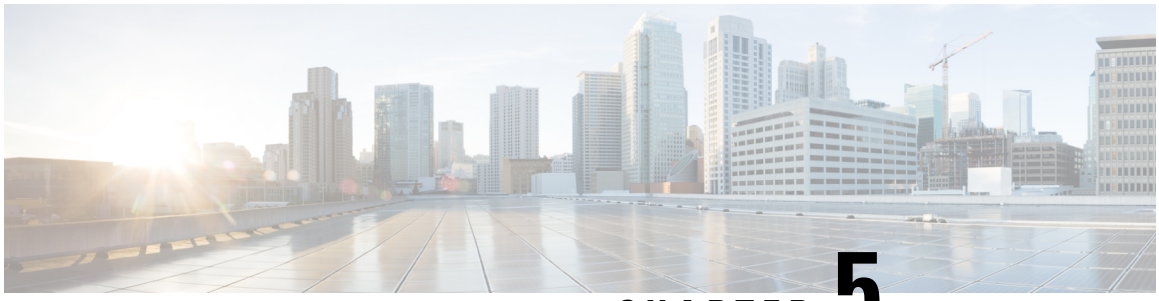
If you are unable to login or lost your XR and System administration passwords, use the following steps to create new password. A lost password cannot be recovered, instead a new username and password must be created with a non-graceful PXE boot.

Step 1 Boot the router using PXE.

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

To PXE boot a router, see Boot the Router Using iPXE, on page 53 .

Step 2 Reset the password.



CHAPTER 5

Perform System Upgrade and Install Feature Packages

The system upgrade and package installation processes are executed using **install** commands on the router. The processes involve adding and activating the iso images (*.iso*), feature packages (*.rpm*), 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 System, on page 29
- Upgrading Features, on page 30
- Workflow for Install Process, on page 31
- Install Packages, on page 31
- Install Prepared Packages, on page 36
- Uninstall Packages, on page 39

Upgrading the System

Upgrading the system is the process of installing a new version of the Cisco IOS XR operating system on the router. The router comes pre-installed with the Cisco IOS XR image. However, you can install the new version in order to keep router features up to date. The system upgrade operation is performed from the XR LXC. However, during system upgrade, the operating systems that run both on the XR LXC and the System Admin LXC get upgraded.

The 1G interface flaps twice instead of once in the Modular Port Adapter (MPA) NC55-MPA-12T-S after you reload any of these NCS 55A2 Fixed Chassis - NCS-55A2-MOD-SL, NCS-55A2-MOD-HD-S, NCS-55A2-MOD-HX-S, or NCS-55A2-MOD-SE-S.

Note If an interface on a router does not have a configuration and is brought up by performing no-shut operation, then upon router reload, the interface state changes to **admin-shutdown** automatically.

System upgrade is done by installing a base package–Cisco IOS XR Unicast Routing Core Bundle. The file name for this bundle is *ncs5500-mini-x.iso*. Install this ISO image using **install** commands. For more information about the install process, see Workflow for Install Process, on page 31.

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

Do not reload the router during an upgrade operation.

For more information on upgrading the system and the RPMs, see *Manage Automatic Dependency* chapter.

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.

For example, the components of the routing package are split into individual RPMs, such as BGP and OSPF. BGP is a mandatory RPM which is a part of the base software version and hence cannot be removed. Optional RPMs such as OSPF can be added and removed as required.

The naming convention of the package is `<platform>-<pkg>-<pkg version>-<release version>.<architecture>.rpm`. Standard packages are:

Feature	Package
Forwarding	ncs5500-fwding-1.0.0.0-<*release-number*>.x86_64.rpm
BGP	ncs5500-bgp-1.0.0.0-<*release-number*>.x86_64.rpm
mpls-te-rsvp	ncs5500-mpls-te-rsvp-1.0.0.0-<*release-number*>.x86_64.rpm
k9sec	ncs5500-k9sec-1.0.0.0-<*release-number*>.x86_64.rpm
mgbl	ncs5500-mgbl-2.0.0.0-<*release-number*>.x86_64.rpm
mpls	ncs5500-mpls-1.0.0.0-<*release-number*>.x86_64.rpm
routing	ncs5500-routing-1.0.0.0-<*release-number*>.x86_64.rpm
security	ncs5500-security-1.0.0.0-<*release-number*>.x86_64.rpm

Package and SMU installation is performed using **install** commands. For more information about the install process, see Install Packages, on page 31.

There are separate packages and SMUs for the XR LXC and the System Admin LXC. They can be identified by their filenames. The XR and System Admin packages and SMUs can be activated from XR and System Admin LXCs.

For more information on upgrading the system and the RPMs, see *Cisco IOS XR Flexible Packaging Configuration Guide*.

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 31. For uninstalling a package, see Uninstall Packages, on page 39.

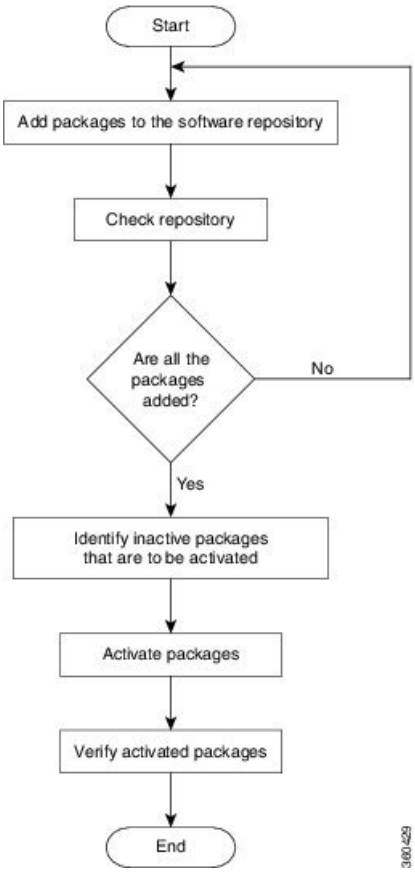
Install Packages

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 *.rpm* files. The *.rpm* file contains multiple packages and SMUs that are merged into a single file. The packaging format defines one RPM per component, without dependency on the card type.

Note The System Admin package and XR package can be executed using **install** commands in the System Admin EXEC mode and XR EXEC mode. All **install** commands are applicable in both these modes.

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

Figure 2: Installing Packages Workflow



Before you begin

- Configure and connect to the management port. The installable file is accessed through the management port. For details about configuring the management port, see Configure the Management Port, on page 6.
- Copy the package to be installed either on the router's hard disk or on a network server to which the router has access.

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. **show install active**
7. **install commit**

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:/ncs5500-mpls-1.0.0.0-r60023I.x86_64.rpm
ncs5500-mgbl-2.0.0.0-r60023I.x86_64.rpm
```

or

```
RP/0/RP0/CPU0:router#install add source /harddisk:/ncs5500-mpls-1.0.0.0-<release-number>.x86_64.rpm
 ncs5500-mgbl-2.0.0.0-<release-number>.x86_64.rpm
```

or

Note A space must be provided between the *package_path* and *filename*.

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.

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

Step 4 **show install inactive**

Example:

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

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

Step 5 Execute one of these:

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

Example:

```
RP/0/RP0/CPU0:router#install activate ncs5500-mpls-1.0.0.0-<release-number>.x86_64.rpm
ncs5500-mgbl-2.0.0.0-<release-number>.x86_64.rpm
```

or

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

The *operation_id* is that of the **install add** operation. This command can also be run from System Admin mode. 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.

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 does not happen instantaneously, but takes some time. 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 LXC and System Admin LXC, perform the reload after activating the SMU in both LXCs 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 **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_lv70
Active Packages: 24
ncs5500-xr-<release-number> version=<release-number> [Boot image]
ncs5500-k9sec-1.0.0.0-<release-number>
ncs5500-m2m-2.0.0.0-<release-number>
ncs5500-mgbl-2.0.0.0-<release-number>
ncs5500-mpls-1.0.0.0-<release-number>
ncs5500-mpls-te-rsvp-1.0.0.0-<release-number>
ncs5500-infra-2.0.0.2-<release-number>.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.2-<release-number>.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.5-<release-number>.CSCxr90016
ncs5500-iosxr-fwding-2.0.0.1-<release-number>.CSCxr55555
ncs5500-iosxr-fwding-2.0.0.6-<release-number>.CSCxr90017
ncs5500-dpa-1.0.0.1-<release-number>.CSCxr90002
ncs5500-dpa-1.0.0.2-<release-number>.CSCxr90004
ncs5500-dpa-fwding-1.0.0.1-<release-number>.CSCxr90005
```

```
ncs5500-k9sec-1.0.0.1-<release-number>.CSCxr80008
ncs5500-os-support-1.0.0.1-<release-number>.CSCxr90013
ncs5500-os-support-1.0.0.2-<release-number>.CSCxr90014
ncs5500-fwding-1.0.0.2-<release-number>.CSCxr90011
ncs5500-fwding-1.0.0.5-<release-number>.CSCxr90019
ncs5500-fwding-1.0.0.1-<release-number>.CSCxr90010
ncs5500-fwding-1.0.0.4-<release-number>.CSCxr90018
ncs5500-mgbl-2.0.0.2-<release-number>.CSCxr80009
ncs5500-mpls-1.0.0.1-<release-number>.CSCxr33333
ncs5500-mpls-te-rsvp-1.0.0.2-<release-number>.CSCxr33335
```

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

Step 7 **install commit**

Example:

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

Commits the XR newly active software. To commit both XR and System Admin software, use **install commit system**.

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 39.

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

Note If you are upgrading power supply modules for NC55-PWR-3KW-DC and NC55-PWR-3KW-2HV, ensure that you first upgrade SC IO FPGA by using **upgrade hw-module location <SC0/SC1> fpd all** command from Sysadmin prompt followed by the **upgrade hw-module location pm-all fpd** command, to upgrade FPD.

Finally use **hw-module location <SC0/SC1> reload**command from Sysadmin prompt to reload the shelf controller.

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. System Admin install operations can be done from XR mode.

Before you begin

- 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.

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**
7. **install commit**

DETAILED STEPS

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

For details, see Install Packages, on page 31.

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.

Step 3 Execute one of these:

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

Example:

```
RP/0/RP0/CPU0:router#install prepare ncs5500-mpls-1.0.0.0-r60023I.x86_64.rpm
```

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. 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_lv70
Active Packages: 24
ncs5500-xr-6.0.0.23I version=6.0.0.23I [Boot image]
ncs5500-k9sec-1.0.0.0-r60023I
ncs5500-m2m-2.0.0.0-r60023I
ncs5500-mgbl-2.0.0.0-r60023I
ncs5500-mpls-1.0.0.0-r60023I
ncs5500-mpls-te-rsvp-1.0.0.0-r60023I
ncs5500-infra-2.0.0.2-r60023I.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.2-r60023I.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.5-r60023I.CSCxr90016
ncs5500-iosxr-fwding-2.0.0.1-r60023I.CSCxr55555
ncs5500-iosxr-fwding-2.0.0.6-r60023I.CSCxr90017
ncs5500-dpa-1.0.0.1-r60023I.CSCxr90002
ncs5500-dpa-1.0.0.2-r60023I.CSCxr90004
ncs5500-dpa-fwding-1.0.0.1-r60023I.CSCxr90005
ncs5500-k9sec-1.0.0.1-r60023I.CSCxr80008
ncs5500-os-support-1.0.0.1-r60023I.CSCxr90013
ncs5500-os-support-1.0.0.2-r60023I.CSCxr90014
ncs5500-fwding-1.0.0.2-r60023I.CSCxr90011
ncs5500-fwding-1.0.0.5-r60023I.CSCxr90019
ncs5500-fwding-1.0.0.1-r60023I.CSCxr90010
ncs5500-fwding-1.0.0.4-r60023I.CSCxr90018
ncs5500-mgbl-2.0.0.2-r60023I.CSCxr80009
ncs5500-mpls-1.0.0.1-r60023I.CSCxr33333
ncs5500-mpls-te-rsvp-1.0.0.2-r60023I.CSCxr33335
```

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

Step 7 **install commit**

Example:

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

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.

Related Commands	Purpose
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.

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

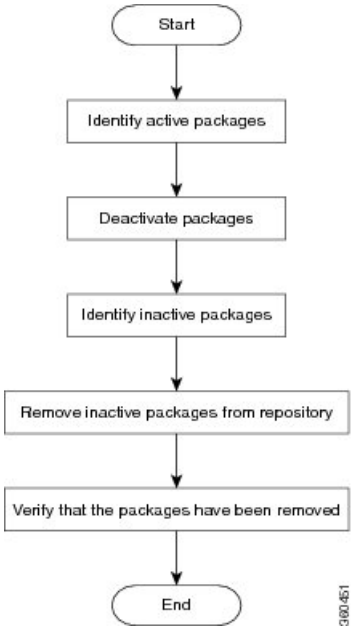
Uninstall Packages

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 LXC cannot be uninstalled from the System Admin LXC, and vice versa.

Note Installed ISO images cannot be uninstalled. Also, kernel SMUs that install third party SMU on host, XR LXC and System Admin LXC, 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 3: Uninstalling Packages Workflow



This task uninstalls XR LXC 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_lv70
Active Packages: 24
ncs5500-xr-6.0.0.23I version=6.0.0.23I [Boot image]
ncs5500-k9sec-1.0.0.0-r60023I
ncs5500-m2m-2.0.0.0-r60023I
ncs5500-mgbl-2.0.0.0-r60023I
```

```
ncs5500-mpls-1.0.0.0-r60023I
ncs5500-mpls-te-rsvp-1.0.0.0-r60023I
ncs5500-infra-2.0.0.2-r60023I.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.2-r60023I.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.5-r60023I.CSCxr90016
ncs5500-iosxr-fwding-2.0.0.1-r60023I.CSCxr55555
ncs5500-iosxr-fwding-2.0.0.6-r60023I.CSCxr90017
ncs5500-dpa-1.0.0.1-r60023I.CSCxr90002
ncs5500-dpa-1.0.0.2-r60023I.CSCxr90004
ncs5500-dpa-fwding-1.0.0.1-r60023I.CSCxr90005
ncs5500-k9sec-1.0.0.1-r60023I.CSCxr80008
ncs5500-os-support-1.0.0.1-r60023I.CSCxr90013
ncs5500-os-support-1.0.0.2-r60023I.CSCxr90014
ncs5500-fwding-1.0.0.2-r60023I.CSCxr90011
ncs5500-fwding-1.0.0.5-r60023I.CSCxr90019
ncs5500-fwding-1.0.0.1-r60023I.CSCxr90010
ncs5500-fwding-1.0.0.4-r60023I.CSCxr90018
ncs5500-mgbl-2.0.0.2-r60023I.CSCxr80009
ncs5500-mpls-1.0.0.1-r60023I.CSCxr33333
ncs5500-mpls-te-rsvp-1.0.0.2-r60023I.CSCxr33335
```

Step 2 Execute one of these:

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

Example:

```
RP/0/RP0/CPU0:router#install deactivate ncs5500-mpls-1.0.0.0-r60023I.x86_64.rpm
ncs5500-mgbl-2.0.0.0-r60023I.x86_64.rpm
```

or

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

The *operation_id* is the ID from **install add** operation. 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. If System admin packages were added as a part of the **install add** operation (of the ID used in deactivate) then those packages will also be deactivated.

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.

Step 4 **install remove** *package_name*

Example:

```
RP/0/RP0/CPU0:router#install remove ncs5500-mpls-1.0.0.0-r60023I.x86_64.rpm
ncs5500-mgbl-2.0.0.0-r60023I.x86_64.rpm
```

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**

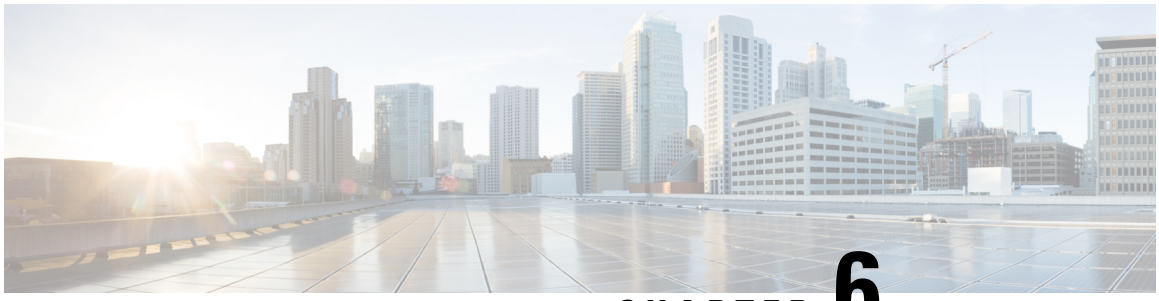
Example:

```
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.

What to do next

Install required packages. See Install Packages, on page 31.

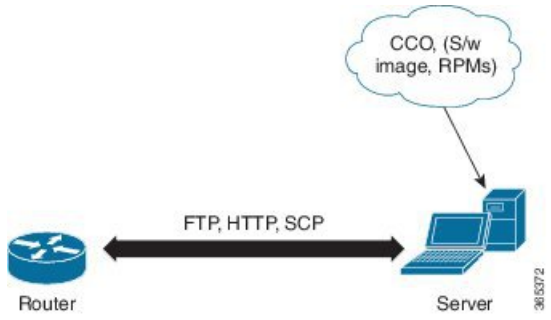


CHAPTER 6

Manage Automatic Dependency

Flexible packaging supports automatic dependency management. While you update an RPM, the system automatically identifies all relevant dependent packages and updates them.

Figure 4: Flow for Installation (base software, RPMs and SMUs)



Until this release, you download the software image and required RPMs from CCO on a network server (the repository),and used the **install add** and the **install activate** commands to add and activate the downloaded files on the . Then, you manually identified relevant dependent RPMs, to add and activate them.

With automatic dependency management, you need not identify dependent RPMs to individually add and activate them. You can execute new install commands to identify and install dependent RPMs automatically.

The new commands are and **install upgrade**. The command identifies and updates dependent packages. The command does not update the base package. The **install upgrade** command upgrades the base package.

Note

1. Cisco IOS XR Version 6.0.2 and later does not provide 3rd-party and host package SMUs as part of automatic dependency management (and **install upgrade** commands). The 3rd party and host package SMUs must be installed separately, and in isolation from other installation procedures (installation of SMUs and RPMs in IOS XR or admin containers).
2. Cisco IOS XR Version 6.0.2 and later does not support asynchronous package upgrades.
3. From Cisco IOS XR Version 6.1.1 onwards, it is possible to update the `mini.iso` file by using the command.

The rest of this chapter contains these sections:

- Update RPMs and SMUs, on page 44

• Upgrade Base Software Version, on page 45

Update RPMs and SMUs

An RPM may contain a fix for a specific defect, and you may need to update the system with that fix. To update RPMs and SMUs to a newer version, use the command. When the command is issued for a particular RPM, the router communicates with the repository, and downloads and activates that RPM. If the repository contains a dependent RPM, the router identifies that dependent RPM and installs that too.

The syntax of the command is:

repository **[rpm]**

Four scenarios in which you can use the command are:

- **When a package name is not specified**

  When no package is specified, the command updates the latest SMUs of all installed packages.

  ```
  [repository]
  ```

  Note From Cisco IOS XR Version 6.1.1 onwards, if the `mini.iso` file is not specified, then it is not added as part of the update. Even if the repository contains the `mini.iso` file, it is not installed.

  ```
  scp://<username>@<server>/my/path/of/packages noprompt
  ```

- **When a package name is specified**

  If the package name is specified, the command installs that package, updates the latest SMUs of that package, along with its dependencies. If the package is already installed, only the SMUs of that package are installed. (SMUs that are already installed are skipped.)

  ```
  [repository] ncs5500-mpls.rpm
  ```

- **When a package name and version number are specified**

  If a particular version of package needs to be installed, the complete package name must be specified; that package is installed along with the latest SMUs of that package present in the repository.

  ```
  [repository] ncs5500-mpls-1.0.2.0-r611.x86_64.rpm
  ```

- **When an SMU is specified**

  If an SMU is specified, that SMU is downloaded and installed, along with its dependent SMUs.

  ```
  [repository] ncs5500-mpls-1.2.0.1-r611.CSCus12345.x86_64.rpm
  ```

- **When a list of packages (containing the mini.iso file) is specified**

  From Cisco IOS XR Version 6.1.1 onwards, if a list of packages (containing the `mini.iso` file) is specified, all the packages in the list and the `mini.iso` file are automatically added as part of the update.

  ```
  scp://<username>@<server>/my/path/of/packages [List of packages] noprompt
  ```

- **When the mini.iso file is specified**

  From Cisco IOS XR Version 6.1.1 onwards, if the `mini.iso` file is specified during the update, then the file is installed with all RPMs and SMUs from the repository.

```
scp://<username>@<server>/my/path/of/packages [mini.iso] noprompt
```

Upgrade Base Software Version

You may choose to upgrade to a newer version of the base software when it becomes available. To upgrade to the latest base software version, use the **install upgrade** command. With the upgrade of the base version, RPMs that are currently available on the router are also upgraded.

Note SMUs are not upgraded as part of this process.

The syntax of the **install upgrade** command is:

install upgrade source *repository* **version** *version***[rpm]**

Note VRF and TPA on dataport is not supported. If the server is reachable only through non-default VRF interface, the file must already be retrieved using ftp, sfp, scp, http or https protocols.

You can use the **install upgrade** command when:

- **The version number is specified**

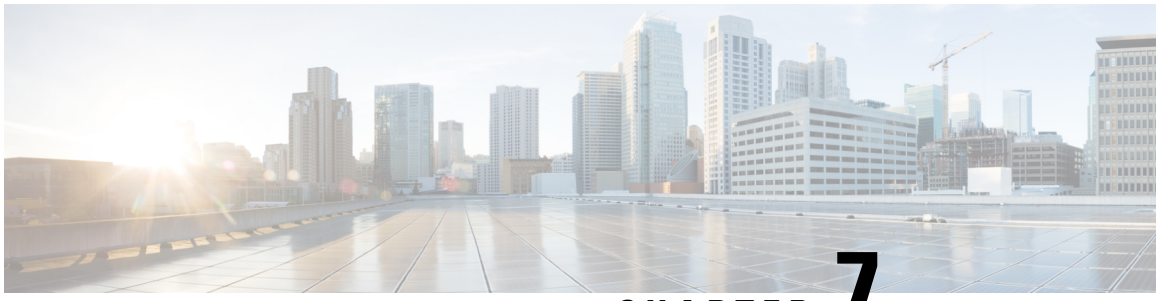
  The base software (.mini) is upgraded to the specified version; all installed RPMs are upgraded to the same release version.

  install upgrade source[repository] version *<release-number>*

- **The version number for an RPM is specified**

  When performing a system upgrade, the user can choose to have an optional RPM to be of a different release (from that of the base software version); that RPM can be specified.

  install upgrade source[repository] version *<release-number>*
  ncs5500-mpls-1.0.2.0-*<release-number>*.x86_64.rpm



CHAPTER 7

Disaster Recovery

The topics covered in this chapter are:

- Boot using USB Drive, on page 47
- Boot using iPXE, on page 49

Boot using USB Drive

The bootable USB drive is used to re-image the router for the purpose of system upgrade or boot the router in case of boot failure. The bootable USB drive can be created using a compressed boot file.

Create a Bootable USB Drive Using Compressed Boot File

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.

Note In case of failure to read or boot from USB drive, ensure that the drive is inserted correctly. If the drive is inserted correctly and still fails to read from USB drive, check the contents of the USB on another system.

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 8GB (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 *ncs5500-usb-boot-<release_number>.zip*.

Step 1 Connect the USB drive to your local machine and format it with FAT32 or MS-DOS file system using the Windows Operating System or Apple MAC Disk Utility.

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.

Step 5 Eject the USB drive from your local machine.

What to do next

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

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.

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 a Bootable USB Drive Using Compressed Boot File, on page 47.

Use one of the two methods to boot the router from USB:

- From Admin EXEC mode - Use this method if Admin LXC is up and Admin Exec prompt is accessible:
  1. Run **show controller card-mgr inventory summary** command and get the RP with mastership.
  2. Insert the USB drive to the active RP.
  3. Run **hw-module location {<loc> | all} bootmedia usb reload**. The RP boots the image from USB and installs the image onto the hard disk. The router boots from the hard disk after installation.
- From RP BIOS boot manager menu - Use this method if Admin LXC is not running:

  Note Use this procedure only on active RP; the standby RP must either be powered OFF or removed from the chassis. After the active RP is installed with images from USB, insert or power ON the standby RP as appropriate.

  1. Insert the USB drive.
  2. Connect to the console.

3. Power the router.
4. Press **Esc** or **Del** to pause the boot process and get the RP to BIOS menu.
5. Select the USB from the boot menu on the RP to which the USB is connected to. The RP boot the image from USB and installs the image onto the hard disk. The router boots from the hard disk after installation.

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

What to do next

- After the booting process is complete, specify the root username and password.
- Install the required optional packages.

Boot using iPXE

iPXE is a pre-boot execution environment that is included in the network card of the management interfaces and works at the system firmware (UEFI) level of the router. iPXE is used to re-image the system, and boot the router in case of boot failure or in the absence of a valid bootable partition. iPXE downloads the ISO image, proceeds with the installation of the image, and finally bootstraps inside the new installation.

iPXE acts as a boot loader and provides the flexibility to choose the image that the system will boot based on the Platform Identifier (PID), the Serial Number, or the management mac-address. iPXE must be defined in the DHCP server configuration file.

Note PID and serial number is supported only if iPXE is invoked using the command `(admin) hw-module location all bootmedia network reload all`. If iPXE is selected manually from BIOS, PID and serial number is not supported.

Zero Touch Provisioning

Zero Touch Provisioning (ZTP) helps in auto provisioning after the software installation of the router using iPXE.

ZTP auto provisioning involves:

- **Configuration:** Downloads and executes the configuration file. The first line of the file must contain `!! IOS XR` for ZTP to process the file as a configuration.
- **Script:** Downloads and executes the script files. The script files include a programmatic approach to complete a task. For example, scripts created using IOS XR commands to perform patch upgrades. The first line of the file must contain `#! /bin/bash` or `#! /bin/sh` for ZTP to process the file as a script.

Setup DHCP Server

A DHCP server must be configured for IPv4, IPv6 or both communication protocols. The following example shows ISC-DHCP server running on Linux system.

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.
- Enable firewall to allow the server to process DHCP packets.
- For DHCPv6, a Routing advertisement (RA) message must be sent to all nodes in the network that indicates which method to use to obtain the IPv6 address. Configure Router-advertise-daemon (radvd, install using yum install radvd) to allow the client to send DHCP request. For example:

```
interface eth3
{
        AdvSendAdvert on;
        MinRtrAdvInterval 60;
        MaxRtrAdvInterval 180;
        AdvManagedFlag on;
        AdvOtherConfigFlag on;
        prefix 2001:1851:c622:1::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr off;
        };
};
```

- The HTTP server can be in the same server as that of the DHCP server, or can be on a different server. After the IP address is assigned from DHCP server, the router must connect to the HTTP server to download the image.

Step 1 Create the `dhcpd.conf` file (for IPv4, IPv6 or both communication protocols), `dhcpv6.conf` file (for IPv6) or both in the `/etc/` or `/etc/dhcp` directory. This configuration file stores the network information such as the path to the script, location of the ISO install file, location of the provisioning configuration file, serial number, MAC address of the router.

Step 2 Test the server once the DHCP server is running. For example, for IPv4:

- Use MAC address of the router:

  Note Using the `host` statement provides a fixed address that is used for DNS, however, verify that option `77` is set to iPXE in the request. This option is used to provide the bootfile to the system when required.

```
host ncs5500
{
hardware ethernet <router-mac-address>;
if exists user-class and option user-class = "iPXE" {
 filename = "http://<httpserver-address>/<path-to-image>/ncs5500-mini-x.iso";
}
```

  Ensure that the above configuration is successful.
- Use serial number of the router:

```
host ncs5500
{
option dhcp-client-identifier "<router-serial-number>";
  filename "http://<IP-address>/<path-to-image>/ncs5500-mini-x.iso";
  fixed-address <IP-address>;
}
```

The serial number of the router is derived from the BIOS and is used as an identifier.

Step 3 Restart DHCP.

```
killall dhcpd
/usr/sbin/dhcpd -f -q -4 -pf /run/dhcp-server/dhcpd.pid
-cf /etc/dhcp/dhcpd.conf ztp-mgmt &
```

Example

The example shows a sample `dhcpd.conf` file:

```
allow bootp;
allow booting;
ddns-update-style interim;
option domain-name "cisco.com";
option time-offset -8;
ignore client-updates;
default-lease-time 21600;
max-lease-time 43200;
option domain-name-servers <ip-address-server1>, <ip-address-server2>;
log-facility local0;
 :
subnet <subnet> netmask <netmask> {
  option routers <ip-address>;
  option subnet-mask <subnet-mask>;
  next-server <server-addr>;
}
  :
host <hostname> {
  hardware ethernet e4:c7:22:be:10:ba;
  fixed-address <address>;
  filename "http://<address>/<path>/<image.bin>";
}
```

The example shows a sample `dhcpd6.conf` file:

```
option dhcp6.name-servers <ip-address-server>;
option dhcp6.domain-search "cisco.com";
dhcpv6-lease-file-name "/var/db/dhcpd6.leases";
option dhcp6.info-refresh-time 21600;
option dhcp6.bootfile-url code 59 = string;
subnet6 <subnet> netmask <netmask> {
       range6 2001:1851:c622:1::2 2001:1851:c622:1::9;
        option dhcp6.bootfile-url "http://<address>/<path>/<image.bin>";
```

What to do next

Invoke ZTP.

Invoke ZTP

ZTP runs within the XR namespace, and within the global VPN routing/forwarding (VRF) namespace for management interfaces and line card interfaces.

Before you begin

Ensure that a DHCP server is setup. For more information, see Setup DHCP Server, on page 50.

Edit the dhcpd.conf file to utilize the capabilities of ZTP.

The following example shows a sample DHCP server configuration including iPXE and ZTP:

```
host <host-name>
{
hardware ethernet <router-serial-number or mac-id>;
fixed-address <ip-address>;
  if exists user-class and option user-class = "iPXE" {
  # Image request, so provide ISO image
  filename "http://<ip-address>/<directory>/ncs5500-mini-x.iso";
  } else
{
  # Auto-provision request, so provide ZTP script or configuration
  filename "http://<ip-address>/<script-directory-path>/ncs5500-ztp.script";
  #filename "http://<ip-address>/<script-directory-path>/ncs5500-ztp.cfg
  }
}
```

Note Either the ZTP .script file or the .cfg file can be provided at a time for auto-provisioning.

With this configuration, the system boots using ncs5500-mini-x.iso during installation, and then download and execute ncs5500-ztp.script when XR LXC is up.

Invoke ZTP Manually

ZTP can also be invoked manually with the modified one touch provisioning approach. The process involves:

Before you begin

A configuration file can be used to specify a list of interfaces that will be brought up in XR and DHCP will be invoked on. /pkg/etc/ztp.config is a platform specific file that allows the platform to specify which if any additional interfaces will be used.

```
#
# List all the interfaces that ZTP will consider running on. ZTP will attempt
# to bring these interfaces. At which point dhclient will be able to use them.
#
# Platforms may add dynamically to this list.
#
#ZTP_DHCLIENT_INTERFACES=" \
#    Gi0_0_0_0 \
#"
...
```

Step 1 Boot the router.

Step 2 Login manually.

Step 3 Enable interfaces.

Step 4 Invoke a new ZTP DHCP session manually using the **ztp initiate** command.

```
Router#ztp initiate
```

For example, to send DHCP requests on the GigabitEthernet interface 0/0/0/0, run the command:

```
Router#ztp initiate debug verbose interface GigabitEthernet0/0/0/0
```

ZTP will run on the management port by default unless the platform has configured otherwise. The logs will be logged in `/disk0:/ztp/ztp/log` location.

Note To configure a 40G interface into 4 separate 10G interfaces, use the **ztp breakout nosignal-stay-in-breakout-mode** command.

Note To enable dataport breakouts and invoke DHCP sessions on all dataport and line card interfaces that are detected, use the **ztp breakout** command.

```
Router#ztp breakout debug verbose
Router#ztp initiate dataport debug verbose
Invoke ZTP?(this may change your configuration) [confirm] [y/n]:
```

To override the prompt:

```
Router#ztp initiate noprompt
Invoke ZTP?(this may change your configuration) [confirm] [y/n]:

ZTP will now run in the background.
Please use "show logging" or look at /disk0:/ztp/ztp/log to check progress.
```

ZTP runs on the management interfaces that are `UP` by default.

Step 5 To terminate the ZTP session, use the **ztp terminate** command.

What to do next

Boot the router using iPXE.

Boot the Router Using iPXE

Before you use the iPXE boot, ensure that:

- DHCP server is set and is running.
- You have logged in to the System Admin console using the **admin** command.

Run the following command to invoke the iPXE boot process to reimage the router:

```
hw-module location all bootmedia network reload
```

Example:

```
sysadmin-vm:0_RP0# hw-module location all bootmedia network reload
Wed Dec 23 15:29:57.376 UTC
Reload hardware module ? [no,yes]
```

The following example shows the output of the command:

```
iPXE 1.0.0+ (3e573) -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP TFTP VLAN EFI ISO9660 NBI Menu
Trying net0...
net0: c4:72:95:a6:14:e1 using dh8900cc on PCI01:00.1 (open)
[Link:up, TX:0 TXE:0 RX:0 RXE:0]
Configuring (net0 c4:72:95:a6:14:e1)................... Ok << Talking to DHCP/PXE server to
 obtain network information
net0: 10.37.1.101/255.255.0.0 gw 10.37.1.0
net0: fe80::c672:95ff:fea6:14e1/64
net0: 2001:1800:5000:1:c672:95ff:fea6:14e1/64 gw fe80::20c:29ff:fefb:b9fe
net1: fe80::c672:95ff:fea6:14e3/64 (inaccessible)
Next server: 10.37.1.235
Filename: http://10.37.1.235/ncs5500/ncs5500-mini-x.iso


http://10.37.1.235/ ncs5500/ncs5500-mini-x.iso... 58% << Downloading file as indicated by
DHCP/PXE server to boot install image
```