System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers, IOS XR Release 7.1.x

First Published: 2020-01-29

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

Note This release has reached end-of-life status. For more information, see the End-of-Life and End-of-Sale Notices.

This preface contains these sections:

Obtaining Documentation and Submitting a Service Request

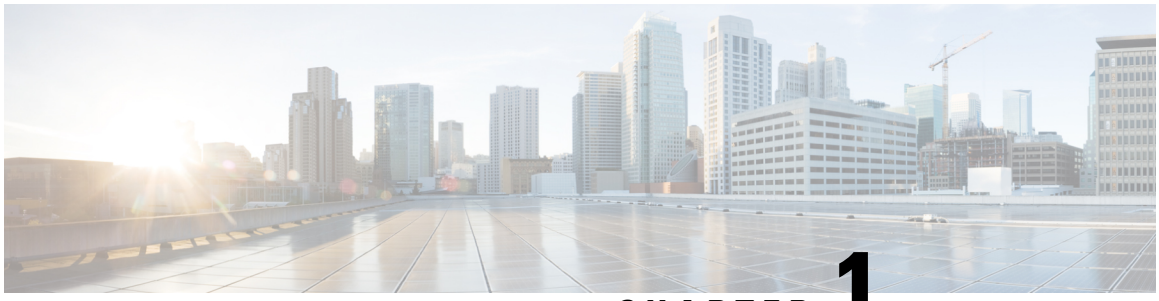
For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

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.

Changes to This Document

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

Date	Summary
January 2020	Initial release of this document



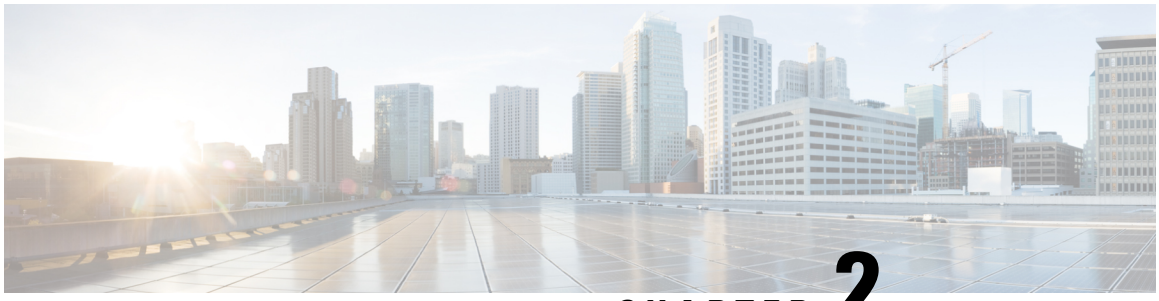
CHAPTER 1

New and Changed Feature Information

This table summarizes the new and changed feature information for the *System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers*.

New and Changed System Setup Features

Feature	Description	Changed in Release	Where Documented
None	No new features introduced	Not applicable	Not applicable



CHAPTER 2

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

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.

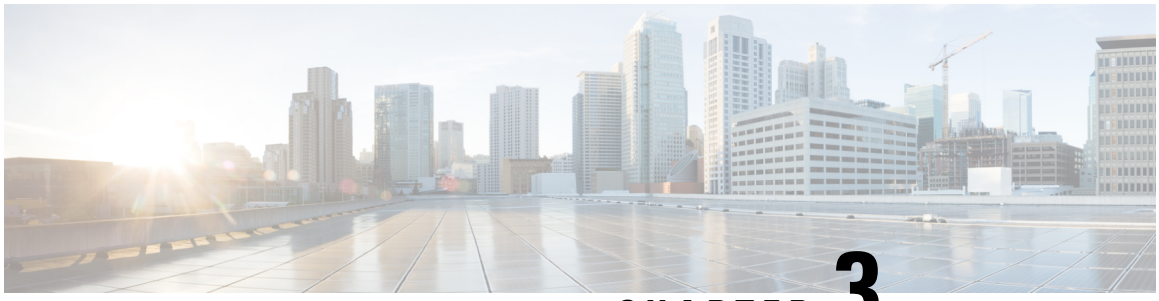
The command modes are applicable for the Cisco NCS 5500 Series Routers. This table lists the command modes for the LXCs.

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)
Note Only the following NCS 540 variants support this mode:
• N540-ACC-SYS
• N540X-ACC-SYS
• N540-24Z8Q2C-SYS
	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#`

Admin Configuration modeSystem Admin Config mode
(System Admin LXCconfiguration mode)
Note Only the following NCS 540 variants support this mode:
• N540-ACC-SYS
• N540X-ACC-SYS
• N540-24Z8Q2C-SYS
	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 3

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 PXE 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

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 necessary, 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.

In the **COM1 Properties** window, select the **Port Settings** tab, and enter the following settings:

The console settings are:

- For modular chassis RP, the console settings are baud rate 9600 bps, no parity, 1 stop bits and 8 data bits
- For fixed chassis, the console settings are baud rate 115200 bps, no parity, 1 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 cord to Power Module. Turn on the router by switching the power switch to the "ON" position. The power switch is usually located near the power module. The router boots up. The boot process details are 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 preinstalled image on the router is corrupt. In this case, the router can be booted using an external bootable USB drive.

Note We recommended that you check the `md5sum` of the image after copying from source location to the server from where router boots up with new version. This ensures that if `md5sum` mismatch is observed, you can remove the corrupted file and ensure that a working copy of the image file is available for setup to begin.

What to do next

Specify the root username and password. For more information, see Setup Root User Credentials, on page 10.

Boot the Router Using USB

The bootable USB drive is used to re-image the router for the purpose of system upgrade, password recovery or boot the router in case of boot failure. The USB on router is mounted as disk 2.

Before you begin

Ensure you have completed the following prerequisites:

- You 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 Center to your local machine. The file name for the compressed boot file is in the format ncs5500-usb_boot-<release_number>.zip.

Step 1 Create a bootable USB 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.

a) 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.
b) Copy the `ncs5500-usb_boot-<release_number>.zip` compressed boot file to the USB drive.
c) Verify that the copy operation is successful. To verify, compare the file size at source and destination. Additionally, verify the MD5 checksum value.
d) Extract the content of the compressed boot file by unzipping it inside the USB drive. This converts the USB drive to a bootable drive.

e) Eject the USB drive from your local machine.

Step 2 Insert the USB on the active RP, and reload or reset the power of the router.

Note Use this procedure only on active RP; the standby RP must either be removed from the chassis, or stopped at the boot menu. After the active RP is installed with images from USB, boot the standby RP.

Step 3 On active XR console, press `CTRL-C` to view BIOS menu. From the menu, select `IOS-XR 64 bit Local boot using front panel USB media`.

```
Got EMT Mode as Disk Boot
Set OS type None, Received OS type=0
Got Boot Mode as Disk Boot

Booting IOS-XR 64 bit Boot previously installed image - Press Ctrl-c to stop
 .
Please select the operating system and the boot device:
     1) Boot to ROMMON
     2) IOS-XR 64 bit Boot previously installed image
     3) IOS-XR 64 bit Mgmt Network boot using DHCP server
     4) IOS-XR 64 bit Mgmt Network boot using local settings (iPXE)
     (Press 'p' for more option)
Selection [1/2/3/4]: p
Please select the operating system and the boot device:
     1) Boot to ROMMON
     2) IOS-XR 64 bit Boot previously installed image
     3) IOS-XR 64 bit Mgmt Network boot using DHCP server
     4) IOS-XR 64 bit Mgmt Network boot using local settings (iPXE)
     5) IOS-XR 64 bit Internal network boot from RSP/RP
     6) IOS-XR 64 bit Local boot using embedded USB media
     7) IOS-XR 64 bit Local boot using front panel USB media
     8) Change baud rate and continue booting
Selection [1/2/3/4/5/6/7/8]: 7
Selected IOS-XR 64 bit Local boot using front panel USB media, Continue ? Y/N: y

Set CBC OS type IOS-XR 64 bit, EMT USB Boot to CBC
Sending boot success notification

Selected boot option - EFI USB Device 1 (SanDisk Cruzer)
Verifying image signature...
Image signature verified successfully
Image Verification Passed
```

522185

If active and standby RPs are not stopped at the boot menu, the previously used boot option is used. If the system is inactive in the boot menu for 30 minutes, the system resets automatically.

Step 4 If standby RP is present and it was stopped in step 2, boot the standby RP after the active RP starts to boot. From the boot options select `IOS-XR 64 bit Internal network boot from RSP/RP`.

Example:

```
Please select the operating system and the boot device:
     1) IOS-XR (32 bit Classic XR)
     2) IOS-XR 64 bit Boot previously installed image
     3) IOS-XR 64 bit Mgmt Network boot using DHCP server
     4) IOS-XR 64 bit Mgmt Network boot using local settings (iPXE)
     5) IOS-XR 64 bit Internal network boot from RSP/RP
     6) IOS-XR 64 bit Local boot using embedded USB media
     7) IOS-XR 64 bit Local boot using front panel USB media
Selection [1/2/3/4/5/6/7]:
```

Select option 5 and proceed with the boot up. After the router boots up, specify the root username and password.

Boot the Router 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 bootstraps within 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.

iPXE boot can be performed during the following scenarios:

- migration from 32-bit to 64-bit using migration script
- recover password
- boot-up failure with 64-bit image

Before you begin

Take a backup of configuration to a TFP or FTP path to load the configuration back after the iPXE boot.

Step 1 Login to the system admin console.

Example:

```
sysadmin-vm:0_RSP0# hw-module location all reload
Tue Mar  6  08:12:47.605 UTC
Reload hardware module ? [no,yes] yes
result Card graceful reload request on all acknowledged.
sysadmin-vm:0_RSP0#
```

Step 2 If the router is unable to boot, press Ctrl +C to stop the boot process when the following information is displayed.

Note Use this procedure only on active RP; the standby RP must either be removed from the chassis, or stopped at the boot menu. After the active RP is installed with images from iPXE boot, boot the standby RP.

Example:

```
IOFPGA Information:
Booted from : Primary FPGA
Revison : 0x1001B
ID : 0x20171FD3
Date : 0x20191205
Fab Revision : 0x5
```

```
Base Board Presence : 0x80000015

Board is : Turin CPU Board
Booting from Primary BIOS
Booting IOS-XR (32 bit Classic XR) - Press Ctrl-c to stop
```

Step 3 Choose option 4 for iPXE boot.

Example:

```
Please select the operating system and the boot device:
     1) IOS-XR (32 bit Classic XR)
     2) IOS-XR 64 bit Boot previously installed image
     3) IOS-XR 64 bit Mgmt Network boot using DHCP server
     4) IOS-XR 64 bit Mgmt Network boot using local settings (iPXE)
     5) IOS-XR 64 bit Internal network boot from RSP/RP
     6) IOS-XR 64 bit Local boot using embedded USB media
     7) IOS-XR 64 bit Local boot using front panel USB media
Selection [1/2/3/4/5/6/7]:
```

Step 4 Manually update iPXE ROMMON details before booting using FTP or TFTP.

Example:

```
iPXE>set cisco/cisco-server-url:string tftp://<path>/asr9k-mini-x64.iso
iPXE>set cisco/cisco-ipv4-address:string 1.3.24.202
iPXE>set cisco/cisco-netmask-address:str 255.255.0.0
iPXE>set cisco/cisco-gateway-address:str 1.3.0.1
```

Step 5 Open the connected management port (0/1).

Example:

```
iPXE>ifclose net0
iPXE>ifclose net1
iPXE>ifopen net1
```

where net0 and net1 represents management port0 and port1 respectively.

Step 6 Boot the required image from FTP or TFTP location.

Example:

```
iPXE> set net0/ip 5.26.8.50
iPXE> set net0/netmask 255.255.0.0
iPXE> set net0/gateway 5.26.0.1
iPXE> ifopen net0
iPXE> boot t ftp://<path>/ncs5500-mini-x-<release-number>.iso
t ftp://<path>/ncs5500-mini-x-<release-number>.iso... Operation canceled ( http://ipxe.org/0b072095)
iPXE>
iPXE> ping 5.0.0.183
64 bytes from 5.0.0.183: seq=1
64 bytes from 5.0.0.183: seq=2
64 bytes from 5.0.0.183: seq=3
Finished: Operation canceled ( http://ipxe.org/0b072095)
iPXE> boot
http://<path>/ncs5500-goldenk9-x-<release-number>-PROD_BUILD_<release-number>_DT_IMAGE__OPTIMISED.iso
http://<path>/ncs5500-goldenk9-x-<release-number>-PROD_BUILD_<release-number>_DT_IMAGE__OPTIMISED.iso...
 ok
Memory required for
image[ncs5500-goldenk9-x-<release-number>-PROD_BUILD_<release-number>_DT_IMAGE__OPTIMISED.iso]:
2345863168, available: 29061079040
Certificate parsing success
```

Step 7 After the active RP is up and running, boot the standby RP. From the boot options select `IOS-XR 64 bit Internal network boot from RSP/RP`.

Example:

```
Please select the operating system and the boot device:
     1) IOS-XR (32 bit Classic XR)
     2) IOS-XR 64 bit Boot previously installed image
     3) IOS-XR 64 bit Mgmt Network boot using DHCP server
     4) IOS-XR 64 bit Mgmt Network boot using local settings (iPXE)
     5) IOS-XR 64 bit Internal network boot from RSP/RP
     6) IOS-XR 64 bit Local boot using embedded USB media
     7) IOS-XR 64 bit Local boot using front panel USB media
Selection [1/2/3/4/5/6/7]:
```

Setup Root User Credentials

When you boot the router for the first time, the system prompts you to configure root credentials (username and password). These credentials have been set up for the root user on the XR console (root-lr), the System Admin VM (root-system), and for disaster recovery purposes.

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 resetting the router's operating system to its default state, 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 from 6 through 253 characters. The password that you type is not displayed on the CLI for security reasons.

The root-system username and password must be safeguarded as they have superuser privileges. They are used to access the complete router configuration.

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

Reenter the password for the root-system user. The password that 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 VM console.

Step 5 **Password:** *password*

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

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

Displays user details.

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

Example

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

Username: admin
Password:

RP/0/RP0/CPU0:ios# show run username
Sun May 30 14:20:42.311 UTC
username admin
 group root-lr
 group cisco-support
 secret 10
$6$RS5knlr/ww.DDn1.$eDFxhqTEYa6hqTs3MODQt11mBp4cMgdQqt.syC/J83lQIl1yJT9vd2W8zEHfBKz4.z4FyImRdzwvKTqAMuyBA0

!
```

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 11.

Access the System Admin Console

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

You must log in to the System Admin console through the XR console to perform all system administration and hardware management setup.

Step 1 Log in to the XR console as the root user.

Step 2 (Optional) Disable the login banner on console port when accessing the System Admin mode from XR mode.

a) **configure**

b) **service sysadmin-login-banner disable**

Example:

```
RP/0/RP0/CPU0:router(config)#service sysadmin-login-banner disable
```

Disable the login banner on console port in System Admin mode.

c) **commit**

d) **end**

Step 3 **admin**

Example:

The login banner is enabled by default. The following example shows the command output with the login banner enabled:

```
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
```

The following example shows the command output with the login banner disabled:

```
RP/0/RP0/CPU0:router#admin
Thu Mar 01:07:14.509 UTC
sysadmin-vm:0_RP0# exit
```

Step 4 (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.

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. Use the **commit** or **end** command.

DETAILED STEPS

Step 1 **configure**

Example:

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

Enters global configuration mode.

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 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

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.

Step 1 **configure**

Example:

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

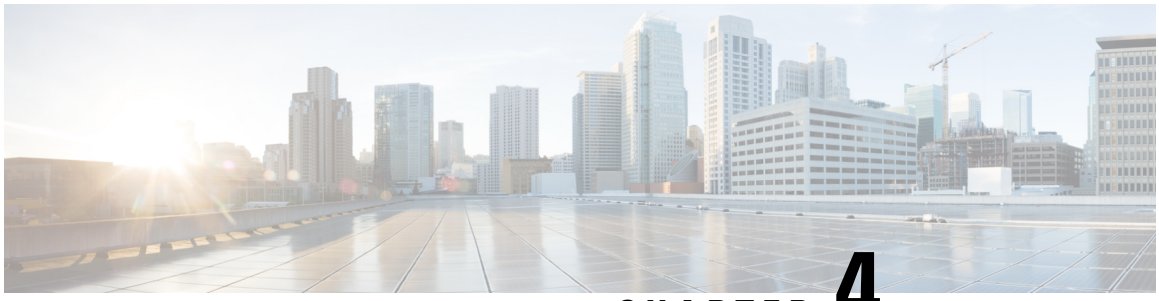
Enters global configuration mode.

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 4

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

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.

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**
3. **show platform**

DETAILED STEPS

Step 1 **admin**

Example:

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

Enters System Admin EXEC mode.

Note Only the following Cisco NCS 540 router variants support this mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

Step 2 **show platform**

Example:

Step 3 **show platform**

Example:

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

Note Only the following Cisco NCS 540 router variants support this mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

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
```

Location	Card type	HWver	FPD device	ATR Status	FPD Versions Run	FPD Versions 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 VM and System Admin VM modes.

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

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 a line card or route processor, use one of the two methods:

- Manual FPD upgrade:
  1. Insert the new line card or route processor.
  2. If `auto fpd upgrade` option is enabled in running configuration, 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 line card or route processor.
  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 line cards and route processors. Reload the line cards or route processors once the FPD upgrade is successful.
- Automatic FPD upgrade:
  1. If automatic FPD upgrade is not configured, use **fpd auto-upgrade enable** command to configure.
  2. Insert the line card or route processor.

3. After the line card or route processor 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 line card or route processor.
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 line cards and route processors. Complete this task to verify the details of the SDR instances.

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

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.

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
```

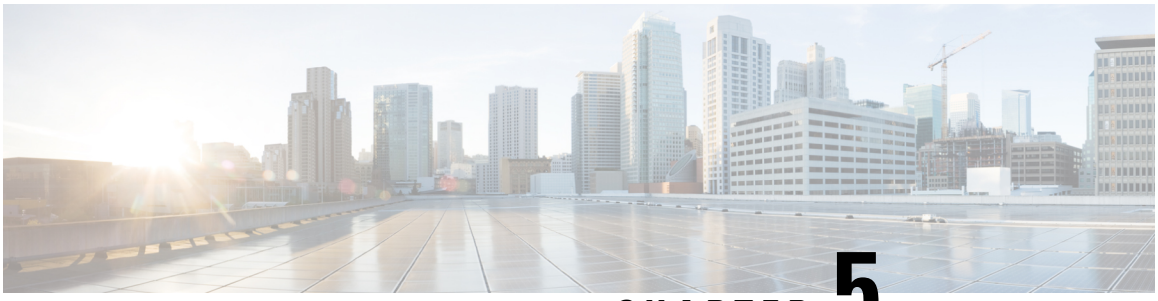
When a router is turned on for the first time, all interfaces are in the 'unassigned' state. Verify that the total number of interfaces displayed in the result matches with the actual number of interfaces present on the router.

```
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 5

Create User Profiles and Assign Privileges

To provide controlled access to the XR and System Admin configurations on the router, user profiles are created with assigned privileges. The privileges are specified using command rules and data rules.

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on how to create user profiles and assign privileges on other Cisco NCS 540 router variants, see the *Create Users and Assign Privileges on Cisco NCS 540 Series Router* section in the *Setup Cisco NCS 540 Series Routers with XR7 OS* chapter.

The authentication, authorization, and accounting (aaa) commands are used for the creation of users, groups, command rules, and data rules. The `aaa` commands are also used for changing the disaster-recovery password.

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

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.

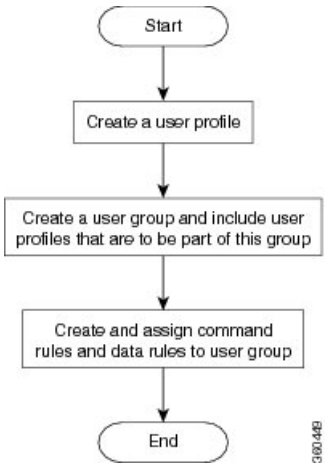
Note If any user on XR is deleted, the local database checks whether there is a first user on System Admin VM.

- 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.
- When a user is added in XR, if there is no user on System Admin mode, then the user is synced to sysadmin-vm. After the synchronization, any changes to the user on XR VM does not synchronize on the System Admin VM.
- A user added on the System Admin VM does not synchronize with XR VM.
- Only the first user or disaster-recovery user created on System Admin VM synchronizes with the host VM.
- Changes to credentials of first user or disaster-recovery user on System Admin VM synchronizes with the host VM.
- The first user or disaster-recovery user deleted on System Admin VM does not synchronize with the host VM. The host VM retains the user.

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

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

The topics covered in this chapter are:

Create User Groups

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.

For extensive information about creating user groups, task groups, RADIUS and TACACS configurations, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*. For detailed information about commands, syntax and their description, see the *Authentication, Authorization, and Accounting Commands* chapter in the *System Security Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 and NCS 560 Series Routers*.

Configure User Groups in XR VM

User groups are configured with the command parameters for a set of users, such as task groups. Entering the **usergroup** command accesses the user group configuration submode. Users can remove specific user groups by using the **no** form of the **usergroup** command. Deleting a usergroup that is still referenced in the system results in a warning.

Before you begin

Note Only users associated with the WRITE:AAA task ID can configure user groups. User groups cannot inherit properties from predefined groups, such as owner-sdr.

Step 1 **configure**

Example:

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

Enters global configuration mode.

Step 2 **usergroup** *usergroup-name*

Example:

```
RP/0/RP0/CPU0:router(config)# usergroup beta
```

Creates a name for a particular user group and enters user group configuration submode.

- Specific user groups can be removed from the system by specifying the **no** form of the **usergroup** command.

Step 3 **description** *string*

Example:

```
 RP/0/RP0/CPU0:router(config-ug)#
description this is a sample user group description
```

(Optional) Creates a description of the user group named in Step 2.

Step 4 **inherit usergroup** *usergroup-name*

Example:

```
 RP/0/RP0/CPU0:router(config-ug)#
inherit usergroup sales
```

- Explicitly defines permissions for the user group.

Step 5 **taskgroup** *taskgroup-name*

Example:

```
 RP/0/RP0/CPU0:router(config-ug)# taskgroup beta
```

Associates the user group named in Step 2 with the task group named in this step.

- The user group takes on the configuration attributes (task ID list and permissions) already defined for the entered task group.

Step 6 Repeat Step for each task group to be associated with the user group named in Step 2.

Step 7 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

Create a User Group in System Admin VM

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on how to create user profiles and assign privileges on other Cisco NCS 540 router variants, see the *Create a User Group* section in the *Setup Cisco NCS 540 Series Routers with XR7 OS* chapter.

Create a user group for the System Admin VM.

The router supports a maximum of 32 user groups.

Before you begin

Create a user profile. See the *Create User* section.

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 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

What to do next

- Create command rules.
- Create data rules.

Create Users

You can create new users and include the user in a user group with certain privileges. The router supports a maximum of 1024 user profiles.

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

XR VM and System Admin VM User Profile Synchronization

Initial User Profile Synchronization: When a user profile is created for the first time within the XR VM, the username and password are synchronized with the System Admin VM, but only if the user does not already exist in the System Admin VM. This initial synchronization ensures consistent user information between the two VMs.

Limitations on Subsequent Changes: However, it is important to note that the System Admin VM does not synchronize subsequent password changes or user deletions made within the XR VM. Consequently, the passwords in the XR VM and the System Admin VM may differ, and user profiles may not be updated in real time to reflect deletions within the XR VM.

User Deleting Handling: Additionally, when a user is deleted within the XR VM, the corresponding user profile in the System Admin VM remains unaffected. In other words, user deletion in the XR VM does not automatically remove the user's profile in the System Admin VM.

For extensive information about creating user groups, task groups, RADIUS and TACACS configurations, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500*

Series Routers. For detailed information about commands, syntax and their description, see the *Authentication, Authorization, and Accounting Commands* chapter in the *System Security Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 and NCS 560 Series Routers*.

Create a User Profile in XR VM

Each user is identified by a username that is unique across the administrative domain. Each user must be a member of at least one user group. Deleting a user group may orphan the users associated with that group. The AAA server authenticates orphaned users but most commands are not authorized.

For more information about AAA, and creating users, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*. For detailed information about related commands, syntax and their description, see the *Authentication, Authorization, and Accounting Commands* chapter in the *System Security Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 and NCS 560 Series Routers*.

Step 1 **configure**

Example:

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

Enters global configuration mode.

Step 2 **username** *user-name*

Example:

```
RP/0/RP0/CPU0:router(config)# username user1
```

Creates a name for a new user (or identifies a current user) and enters username configuration submode.

- The *user-name* argument can be only one word. Spaces and quotation marks are not allowed.

Step 3 Do one of the following:

- **password** {**0** | **7**} *password*
- **secret** {**0** | **5** | **8** | **9** | **10**} *secret*

Example:

```
Router(config-un)# password 0 pwd1
```

or

```
Router(config-un)# secret 0 sec1
```

Specifies a password for the user named in Step 2.

- Use the **secret** command to create a secure login password for the user names specified in Step 2.
- Entering **0** following the **password** command specifies that an unencrypted (clear-text) password follows. Entering **7** following the **password** command specifies that an encrypted password follows.
- For the **secret** command, the following values can be entered:
  - **0** : specifies that a secure unencrypted (clear-text) password follows
  - **5** : specifies that a secure encrypted password follows that uses MD5 hashing algorithm

- **8** : specifies that Type 8 secret that uses SHA256 hashing algorithm follows
- **9** : specifies that Type 9 secret that uses SCrypt hashing algorithm follows

  Note The Type 8 and Type 9 secrets are supported on the IOS XR 64-bit operating system starting from Cisco IOS XR Software Release 7.0.1. Prior to this release, it was supported only on the IOS XR 32-bit operating system.

- **10** : specifies Type 10 secret that uses SHA512 hashing algorithm

  Note
  - Type 10 secret is supported only for Cisco IOS XR 64 bit platform.
  - Backward compatibility issues such as configuration loss, authentication failure, and so on, are expected when you downgrade to lower versions that still use **MD5** or **SHA256** encryption algorithms. If there are any type 10 secrets, convert the **secrets** to type 5 if you are downgrading the system from versions 7.0.1 and above to versions 6.5.3 and above. If you are downgrading the system from versions 7.0.1 and above to versions below 6.5.3, then un-configure all users from the XR-vm and sysadmin-vm before executing install activate.
  - In a first user configuration scenario or when you reconfigure a user, the system synchronises only the Type 5 and Type 10 secrets from XR VM to System Admin VM and Host VM. It does not synchronize the Type 8 and Type 9 secrets in such scenarios.

- Type **0** is the default for the **password** and **secret** commands.
- From Cisco IOS XR Software Release 7.0.1 and later, the default hashing type is 10 (SHA512) when clear text secret is configured without choosing the type in the configuration.

Step 4 **group** *group-name*

Example:

```
RP/0/RP0/CPU0:router(config-un)# group sysadmin
```

Assigns the user named in Step 2 to a user group that has already been defined through the **usergroup** command.

- The user takes on all attributes of the user group, as defined by that user group's association to various task groups.
- Each user must be assigned to at least one user group. A user may belong to multiple user groups.

Step 5 Repeat step 4 for each user group to be associated with the user specified in step 2.

Step 6 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

Create a User Profile in System Admin VM

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on how to create user profiles and assign privileges on other Cisco NCS 540 router variants, see the *Create Users and Assign Privileges on Cisco NCS 540 Series Router* section in the *Setup Cisco NCS 540 Series Routers with XR7 OS* chapter.

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

The router supports a maximum of 1024 user profiles.

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

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 VM.

Step 5 **uid** *user_id_value*

Example:

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

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

Step 6 **gid** *group_id_value*

Example:

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

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

Step 7 **ssh_keydir** *ssh_keydir*

Example:

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

Specify any alphanumeric value.

Step 8 **homedir** *homedir*

Example:

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

Specify any alphanumeric value.

Step 9 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

Create Command Rules

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on how to create user profiles and assign privileges on other Cisco NCS 540 router variants, see the *Setup Cisco NCS 540 Series Routers with XR7 OS* chapter.

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 in System Admin VM, on page 31.

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. Use the **commit** or **end** command.

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 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

What to do next

Create data rules. See Create Data Rules, on page 39.

Create Data Rules

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on user profiles and user groups on other Cisco NCS 540 router variants, see the *Setup Cisco NCS 540 Series Routers with XR7 OS* chapter.

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 in System Admin VM, on page 31.

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. Use the **commit** or **end** command.

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 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.

- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

Change Disaster-recovery Username and Password

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on user profiles and user groups on other Cisco NCS 540 router variants, see the *Setup Cisco NCS 540 Series Routers with XR7 OS* chapter.

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. Use the **commit** or **end** command.

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 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** —Exits the configuration session without committing the configuration changes.
- **Cancel** —Remains in the configuration session, without committing the configuration changes.

Recover Password using PXE Boot

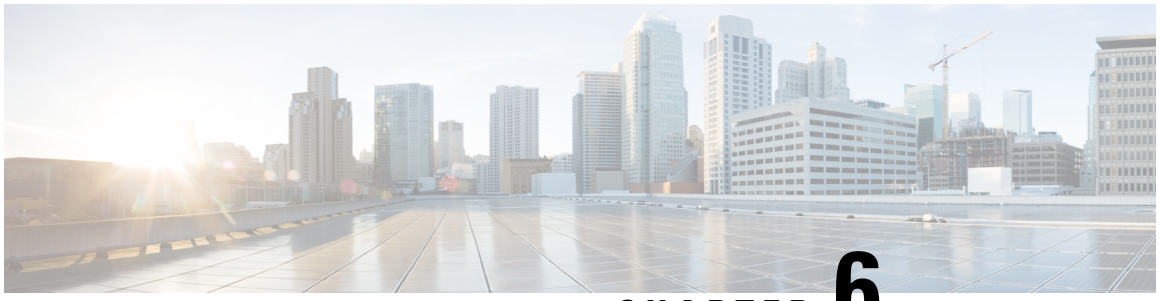
If you are unable to login or lost your XR and System administration passwords, use the following steps to create new password. A lost password cannot be recovered, instead a new username and password must be created with a non-graceful PXE boot.

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 82.

Step 2 Reset the password.



CHAPTER 6

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*) and feature packages 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

Upgrading the system is the process of installing a new version of the Cisco IOS XR operating system on the router. The router comes preinstalled 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 VM. However, during system upgrade, the software that runs on both the XR VM and the System Admin VM get upgraded.

Note 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 you insert a line card on a router that is running a lower version than the one the line card supports, the line card fails to boot. You must first upgrade the router to a software version that supports the line card, insert the line card and iPXE boot the line card.

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

Note

- Ensure that you have adequate disk space.
- Run the **fsck** command to check the status of the file system, for a successful IOS XR upgrade. You must run the **fsck** command in the System Admin EXEC mode to install a System Admin package, and in the XR EXEC mode to install the XR package.
- All install commands are applicable in both the System Admin EXEC mode and in XR EXEC mode. System Admin install operations are done from XR EXEC mode.

Perform a system upgrade by installing a base package–Cisco IOS XR Unicast Routing Core Bundle. To install this bundle, run the **install** command. The filename for the Cisco IOS XR Unicast Routing Core Bundle bundle is *ncs5500-mini-x.iso*.

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

Do not reload the router during an upgrade operation.

Note To enable hardware programming after upgrading the chassis from an older software version to IOS XR Release 7.6.x or later through ISSU, initiate a chassis reload. The chassis reload is mandatory, if you must enable a maximum transmission unit (MTU) value of 9646 on applicable interfaces.

Cisco IOS XR supports RPM signing and signature verification for Cisco IOS XR RPM packages in the ISO and upgrade images. All RPM packages in the Cisco IOS XR ISO and upgrade images are signed to ensure cryptographic integrity and authenticity. This guarantees that the RPM packages haven't been tampered with and the RPM packages are from Cisco IOS XR. The private key, which is used for signing the RPM packages, is created and securely maintained by Cisco.

Upgrading Features

Upgrading features is the process of deploying new features and software patches on the router. Perform a feature upgrade by installing packages. Perform a software patch installation 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 part of the base software version and is a mandatory RPM, and hence can't be removed. However, you can add and remove optional RPMs such as OSPF as required.

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

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

Use the **install** commands to install packages and SMUs. For more information about the install process, see Install Packages, on page 51.

Note

- Ensure that you have adequate disk space.
- Run the **fsck** command to check the status of the file system, for a successful IOS XR upgrade. You must run the **fsck** command in the System Admin EXEC mode to install a System Admin package, and in the XR EXEC mode to install the XR package.
- All install commands are applicable in both the System Admin EXEC mode and in XR EXEC mode. System Admin install operations are done from XR EXEC mode.

There are separate packages and SMUs for the XR VM and the System Admin VM. They can be identified by their filenames.

The XR and System Admin packages and SMUs can be activated from XR and System Admin VMs.

You can alternatively perform a cross VM operation, by activating or deactivating the System Admin packages and SMUs from XR.

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

Third-Party SMUs

Consider these points while activating and deactivating third-party SMUs:

- To activate a third-party SMU, you should have a corresponding base package.
- When you activate a third-party SMU, the corresponding third-party base package state is inactive, this is an expected behavior.
- To deactivate a third-party SMU, ensure that you activate the corresponding third-party base package. Third-party SMUs deactivated explicitly might lead to triages to the install team.

Note All SMUs are bundled together with the base package in a TAR file

Note All Cisco RPMs have the platform name in the filename. For example, **ncs5500**-sysadmin.

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, preactivation 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 less time. As a result, the router downtime is considerably reduced.
- It performs a disk-space check that is required for a successful operation. This quantifies the disk-space deficit, and provides you possible alternatives to free up space in the filesystem.
- It performs a package compatibility check. This ensures that all the required installation packages are available. For any package compatibility check error, details of the package and version are logged.

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on installing prepared packages on other Cisco NCS 540 router variants, see the *Install XR7 OS on NCS 540 Series Routers* chapter.

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.

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

For details, see Install Packages, on page 51.

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 **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
```

Step 4 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 5 **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 6 **install activate**

Example:

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

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

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

Activations 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 7 **show install active**

Example:

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

Displays packages that are active.

```
Node 0/RP0/CPU0 [RP]
Boot Partition: xr_lv70
Active Packages: 24
ncs5500-xr-6.0.0 version=6.0.0 [Boot image]
ncs5500-k9sec-1.0.0.0-r600
ncs5500-mgbl-2.0.0.0-r600
ncs5500-mpls-1.0.0.0-r600
ncs5500-mpls-te-rsvp-1.0.0.0-r600
ncs5500-infra-2.0.0.2-r600.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.2-r600.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.5-r600.CSCxr90016
ncs5500-iosxr-fwding-2.0.0.1-r600.CSCxr55555
ncs5500-iosxr-fwding-2.0.0.6-r600.CSCxr90017
ncs5500-dpa-1.0.0.1-r600.CSCxr90002
ncs5500-dpa-1.0.0.2-r600.CSCxr90004
ncs5500-dpa-fwding-1.0.0.1-r600.CSCxr90005
ncs5500-k9sec-1.0.0.1-r600.CSCxr80008
ncs5500-os-support-1.0.0.1-r600.CSCxr90013
ncs5500-os-support-1.0.0.2-r600.CSCxr90014
ncs5500-fwding-1.0.0.2-r600.CSCxr90011
ncs5500-fwding-1.0.0.5-r600.CSCxr90019
ncs5500-fwding-1.0.0.1-r600.CSCxr90010
ncs5500-fwding-1.0.0.4-r600.CSCxr90018
ncs5500-mgbl-2.0.0.2-r600.CSCxr80009
ncs5500-mpls-1.0.0.1-r600.CSCxr33333
ncs5500-mpls-te-rsvp-1.0.0.2-r600.CSCxr33335
```

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

Step 8 **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.
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.

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. You can also include SMUs in an upgrade operation along with mini ISO.

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

- Ensure that you have adequate disk space.
- Run the **fsck** command to check the status of the file system, for a successful IOS XR upgrade. You must run the **fsck** command in the System Admin EXEC mode to install a System Admin package, and in the XR EXEC mode to install the XR package.
- All install commands are applicable in both the System Admin EXEC mode and in XR EXEC mode. System Admin install operations are done from XR EXEC mode.

Note

- The system upgrade is supported only from XR EXEC mode.
- While the System Admin package can be executed using **install** commands in the System Admin EXEC mode and XR EXEC mode, the XR package can only be executed using the install commands in XR EXEC mode. All **install** commands are applicable in both these modes.
- While the System Admin SMUs can be installed in System Admin EXEC mode and XR EXEC mode, the XR SMUs can only be installed through the XR EXEC mode.
- Install operation over IPv6 is not supported.

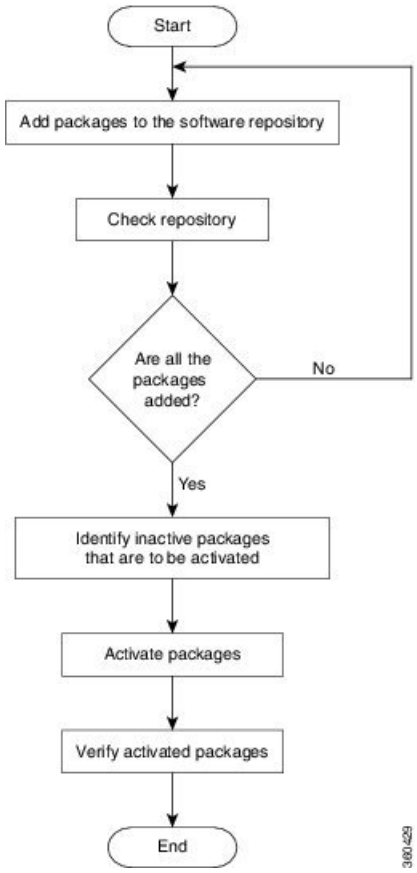
Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on installing packages on other Cisco NCS 540 router variants, see the *Install XR7 OS on NCS 540 Series Routers* chapter.

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

Step 1 Execute one of these:

- **install add source** *<http or shttp transfer protocol>/package_path/ filename1 filename2 ...*
- **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-r731.x86_64.rpm
ncs5500-mgbl-1.0.0.0-r732.x86_64.rpm
```

or

```
RP/0/RP0/CPU0:router#install add source sftp://root@8.33.5.15:/auto/ncs/package/
ncs55000-mcast-1.0.0.0-731.x86_64.rpm ncs5500-iosxr-mpls-1.0.0.0-732.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-1.0.0.0-<release-number>.x86_64.rpm
```

or

```
RP/0/RP0/CPU0:router#install add source sftp://root@8.33.5.15:/auto/ncs/package/
ncs55000-mcast-1.0.0.0-<release-number>.x86_64.rpm
ncs5500-iosxr-mpls-1.0.0.0-<release-number>.x86_64.rpm
```

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

The software files are unpacked from the package, validated, and then 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 when all files are unpacked.

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

Step 2 **show install request**

Example:

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

(Optional) Displays the operation ID of the add operation and its status. The operation ID can be later used to execute the **activate** command.

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

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, see Install Packages, on page 51 Step Step 2, on page 54. This command can also be run from the Sys 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, as this is the default. The **install activate** command runs in the background, and the EXEC prompt is returned.

You can run the activate operation either through the synchronous mode or by selecting the `sync` option from the CLI.

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 ID 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. When activation completes, the system reloads automatically. For restart SMU activation, the SMU takes effect once the processes impacted by the SMU are restarted.

If the SMU has dependency on both XR VM and System Admin VM, perform the reload after activating the SMU in both VMs so that they take effect simultaneously. To reload the router, use the **hw-module location all reload** command from the System Admin EXEC mode.

Step 6 **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-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.

Table 1: Example: 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	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.

Step 7 **install commit**

Example:

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

Commits the Host, XR, and System Admin newly active software.

Note On Multi-SDR mode, you can use the **install commit sdr** to commit just the sdr from where the CLI is being triggered. For more information, see Secure Domain Router Commands.

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 57.

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.

Uninstall Packages

Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

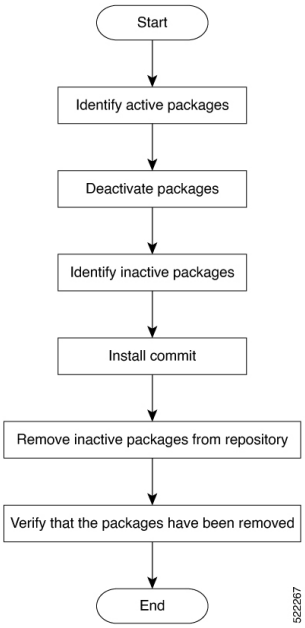
For information on deleting packages on other Cisco NCS 540 router variants, see the *Delete Optional Packages* section in the *Install XR7 OS on NCS 540 Series Routers* chapter.

Complete this task to uninstall a package. All router functionalities that are part of the uninstalled package are deactivated. Packages that are added in the XR VM cannot be uninstalled from the System Admin VM. However, the cross VM operation allows System Admin packages to be deactivated from XR as well.

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

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

Figure 3: Uninstalling Packages Workflow



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

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 version=6.0.0 [Boot image]
ncs5500-k9sec-1.0.0.0-r600
ncs5500-mgbl-2.0.0.0-r600
ncs5500-mpls-1.0.0.0-r600
ncs5500-mpls-te-rsvp-1.0.0.0-r600
ncs5500-infra-2.0.0.2-r600.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.2-r600.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.5-r600.CSCxr90016
ncs5500-iosxr-fwding-2.0.0.1-r600.CSCxr55555
ncs5500-iosxr-fwding-2.0.0.6-r600.CSCxr90017
ncs5500-dpa-1.0.0.1-r600.CSCxr90002
ncs5500-dpa-1.0.0.2-r600.CSCxr90004
ncs5500-dpa-fwding-1.0.0.1-r600.CSCxr90005
ncs5500-k9sec-1.0.0.1-r600.CSCxr80008
ncs5500-os-support-1.0.0.1-r600.CSCxr90013
ncs5500-os-support-1.0.0.2-r600.CSCxr90014
ncs5500-fwding-1.0.0.2-r600.CSCxr90011
ncs5500-fwding-1.0.0.5-r600.CSCxr90019
ncs5500-fwding-1.0.0.1-r600.CSCxr90010
ncs5500-fwding-1.0.0.4-r600.CSCxr90018
ncs5500-mgbl-2.0.0.2-r600.CSCxr80009
ncs5500-mpls-1.0.0.1-r600.CSCxr33333
ncs5500-mpls-te-rsvp-1.0.0.2-r600.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 commit**

Step 5 **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.

You can also use the **install remove inactive all** to remove all inactive packages from XR and System Admin.

Step 6 **show install repository**

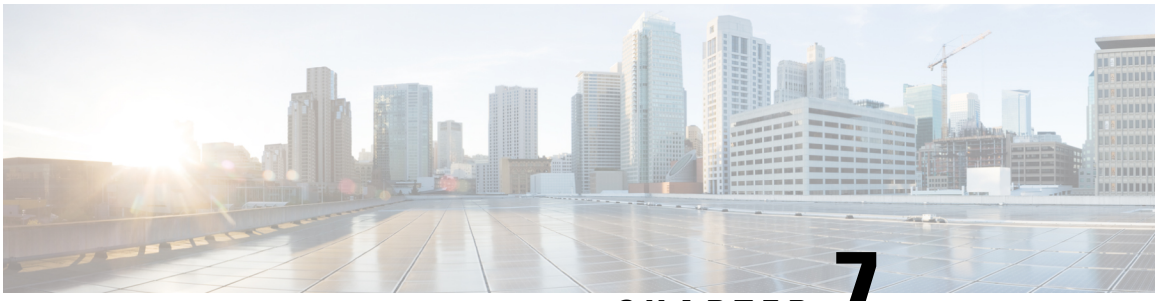
Example:

```
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. .

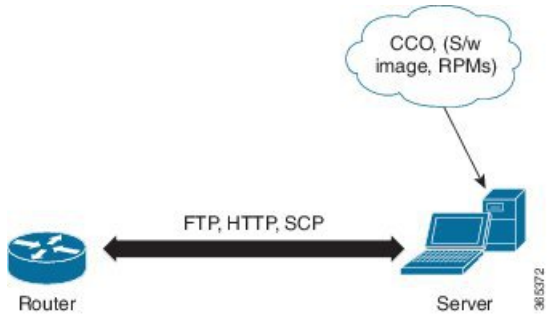


CHAPTER 7

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 downloaded 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 router. Then, you manually identify 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 command to identify and install dependent RPMs automatically.

The command **install source** adds and activates packages. The command **install replace** adds and activates packages in a given golden ISO (GISO).

Note

1. Cisco IOS XR Version 6.0.2 and later does not provide third party and host package SMUs as part of automatic dependency management (**install source** command). The third 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. From Cisco IOS XR Version 6.5.2 onwards, it is possible to update the `mini.iso` file by using the **install source** command.

The rest of this chapter contains these sections:

• Downgrade an RPM, on page 64

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 **install source** command. When this 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 **install source** command is:

install source *repository* **[rpm]**

Four scenarios in which you can use the **install source** command are:

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

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

  ```
  install source [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.

```
install source 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.)

  ```
  install source [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.

  ```
  install source [repository] ncs5500-mpls-1.0.2.0-r710.x86_64.rpm
  ```

- **When an SMU is specified**

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

  ```
  install source [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 6.5.2 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.

  ```
  install source 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.

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

Upgrade Base Software Version

You can upgrade to a newer version of the base software when it becomes available. To upgrade to the latest base software version, use the **install source** 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 source** command is:

```
install source repository
```

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.

Note Default routes (0.0.0.0/0) cannot be copied onto Linux due to TPA implementation.

You can use the **install source** 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 source [repository] version <version> asr9k-mini-x64-<version>.iso
  ```

  For example,

  ```
  install source repository version 7.0.1 asr9k-mini-x64-7.0.1.iso
  ```

  You can also automatically fetch the .mini file and RPMs of the required release and proceed with the upgrade.

  ```
  install source repository asr9k-mini-x64-7.0.1.iso
  ```

- **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 source repository version 6.2.2
  ncs5500-mpls-1.0.2.0-r623.x86_64.rpm
  ```

Downgrade an RPM

An RPM can be downgraded after it is activated. RPMs are of the following types:

- **Hostos RPM:** The RPM contains `hostos` in the name.

  For example:

  - <platform>-sysadmin-hostos-6.5.1-r651.CSChu77777.host.arm
  - <platform>-sysadmin-hostos-6.5.1-r651.CSChu77777.admin.arm
  - <platform>-sysadmin-hostos-6.5.1-r651.CSChu77777.host.x86_64
  - <platform>-sysadmin-hostos-6.5.1-r651.CSChu77777.admin.x86_64

- **Non-hostos RPM:** The RPM does not contain `hostos` in the name.

  For example:

  - <platform>-sysadmin-system-6.5.1-r651.CSCvc12346

To deactivate the RPMs, perform the following steps:

- **Downgrade Hostos RPM**
  - Scenario 1: To downgrade to version 06 from the active version 09:
    1. Download the version 06 hostos RPMs, and add the RPMs.

       ```
       install add source [repository]
       <platform>-sysadmin-hostos-6.5.1.06-r65108I.CSChu44444.host.arm
       <platform>-sysadmin-hostos-6.5.1.06-r65108I.CSChu44444.admin.arm
       <platform>-sysadmin-hostos-6.5.1.06-r65108I.CSChu44444.host.x86_64
       <platform>-sysadmin-hostos-6.5.1.06-r65108I.CSChu44444.admin.x86_64
       ```

    2. Activate the downloaded RPMs.

       ```
       install activate [repository]
       <platform>-sysadmin-hostos-6.5.1.06-r65108I.CSChu44444.host.arm
       <platform>-sysadmin-hostos-6.5.1.06-r65108I.CSChu44444.admin.arm
       <platform>-sysadmin-hostos-6.5.1.06-r65108I.CSChu44444.host.x86_64
       <platform>-sysadmin-hostos-6.5.1.06-r65108I.CSChu44444.admin.x86_64
       ```

    3. Commit the configuration.

       ```
       install commit
       ```

  - Scenario 2: Deactivate hostos RPM by activating base RPM, consider version 09 is active:
    1. Activate the base RPM.

       ```
       install activate <platform>-sysadmin-hostos-6.5.1.08I-r65108I.admin.arm
       <platform>-sysadmin-hostos-6.5.1.08I-r65108I.host.arm
       <platform>-sysadmin-hostos-6.5.1.08I-r65108I.admin.x86_64
       <platform>-sysadmin-hostos-6.5.1.08I-r65108I.host.x86_64
       ```

       For example, if RPM `ncs5500-sysadmin-hostos-6.5.1-r651.CSChu44444.host.arm` is the RPM installed, then `ncs5500-sysadmin-hostos-6.5.1-r651.host.arm` is its base RPM.
    2. Commit the configuration.

```
install commit
```

The downgrade for third-party RPMs is similar to the hostos RPMs. To downgrade a SMU, activate the lower version of the SMU. If only one version of SMU is present, the base RPM of the SMU must be activated.

Note Hostos and third-party RPMs cannot be deactivated. Only activation of different versions is supported.

- **Downgrade Non-Hostos RPM**

  1. Deactivate the RPM to downgrade to earlier version of RPM.

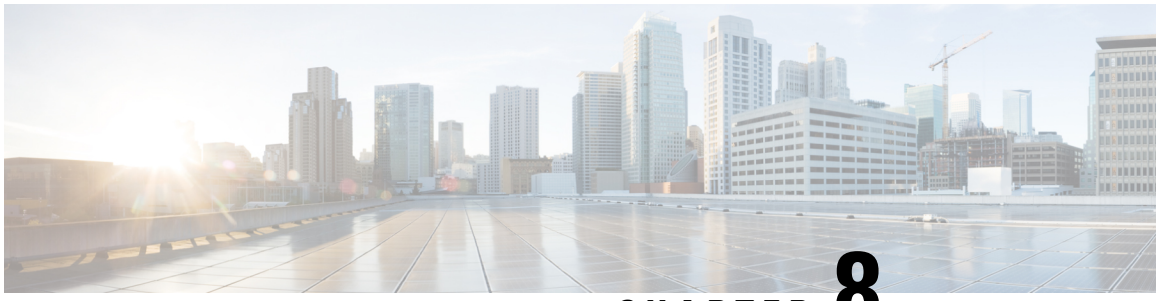
     ```
     install deactivate <platform>-<rpm-name>
     ```

  2. Check the active version of the RPM.

     ```
     show install active
     ```

  3. Commit the configuration.

     ```
     install commit
     ```



CHAPTER 8

Customize Installation using Golden ISO

Golden ISO (GISO) is a customized ISO that a user can build to suit the installation requirement. The user can customize the installable image to include the standard base image with the basic functional components, and add additional RPMs, SMUs and configuration files based on requirement.

The ease of installation and the time taken to seamlessly install or upgrade a system plays a vital role in a cloud-scale network. An installation process that is time-consuming and complex affects the resiliency and scale of the network. The GISO simplifies the installation process, automates the installation workflow, and manages the dependencies in RPMs and SMUs automatically.

GISO is built using a build script `gisobuild.py` available on the github location Github location.

When a system boots with GISO, additional SMUs and RPMs in GISO are installed automatically, and the router is pre-configured with the XR configuration in GISO. For more information about downloading and installing GISO, see Install Golden ISO, on page 71.

The capabilities of GISO can be used in the following scenarios:

- Initial deployment of the router
- Software disaster recovery
- System upgrade from one base version to another
- System upgrade from same base version but with additional SMUs
- Install update to identify and update dependant packages

Limitations

The following are the known problems and limitations with the customized ISO:

- GISO image size more than 1.8 GB is not supported.
- Building and booting GISO for asynchronous package (a package of different release than the ISO) is not supported.

- Verifying the XR configuration is not supported in the GISO build script `gisobuild.py`.
- Renaming a GISO build and then installing from the renamed GISO build is not supported.
- Install operation over IPv6 is not supported.

Customize Installation using Golden ISO

Golden ISO (GISO) is a customized ISO that a user can build to suit the installation requirement. The user can customize the installable image to include the standard base image with the basic functional components, and add additional RPMs, SMUs and configuration files based on requirement.

The ease of installation and the time taken to seamlessly install or upgrade a system plays a vital role in a cloud-scale network. An installation process that is time-consuming and complex affects the resiliency and scale of the network. The GISO simplifies the installation process, automates the installation workflow, and manages the dependencies in RPMs and SMUs automatically.

GISO is built using a build script `gisobuild.py` available on the github location Github location.

When a system boots with GISO, additional SMUs and RPMs in GISO are installed automatically, and the router is pre-configured with the XR configuration in GISO. For more information about downloading and installing GISO, see Install Golden ISO, on page 71.

The capabilities of GISO can be used in the following scenarios:

- Initial deployment of the router
- Software disaster recovery
- System upgrade from one base version to another
- System upgrade from same base version but with additional SMUs
- Install update to identify and update dependant packages

Limitations

The following are the known problems and limitations with the customized ISO:

- GISO image size more than 1.8 GB is not supported.
- Building and booting GISO for asynchronous package (a package of different release than the ISO) is not supported.
- Verifying the XR configuration is not supported in the GISO build script `gisobuild.py`.
- Renaming a GISO build and then installing from the renamed GISO build is not supported.
- Install operation over IPv6 is not supported.

Golden ISO Workflow

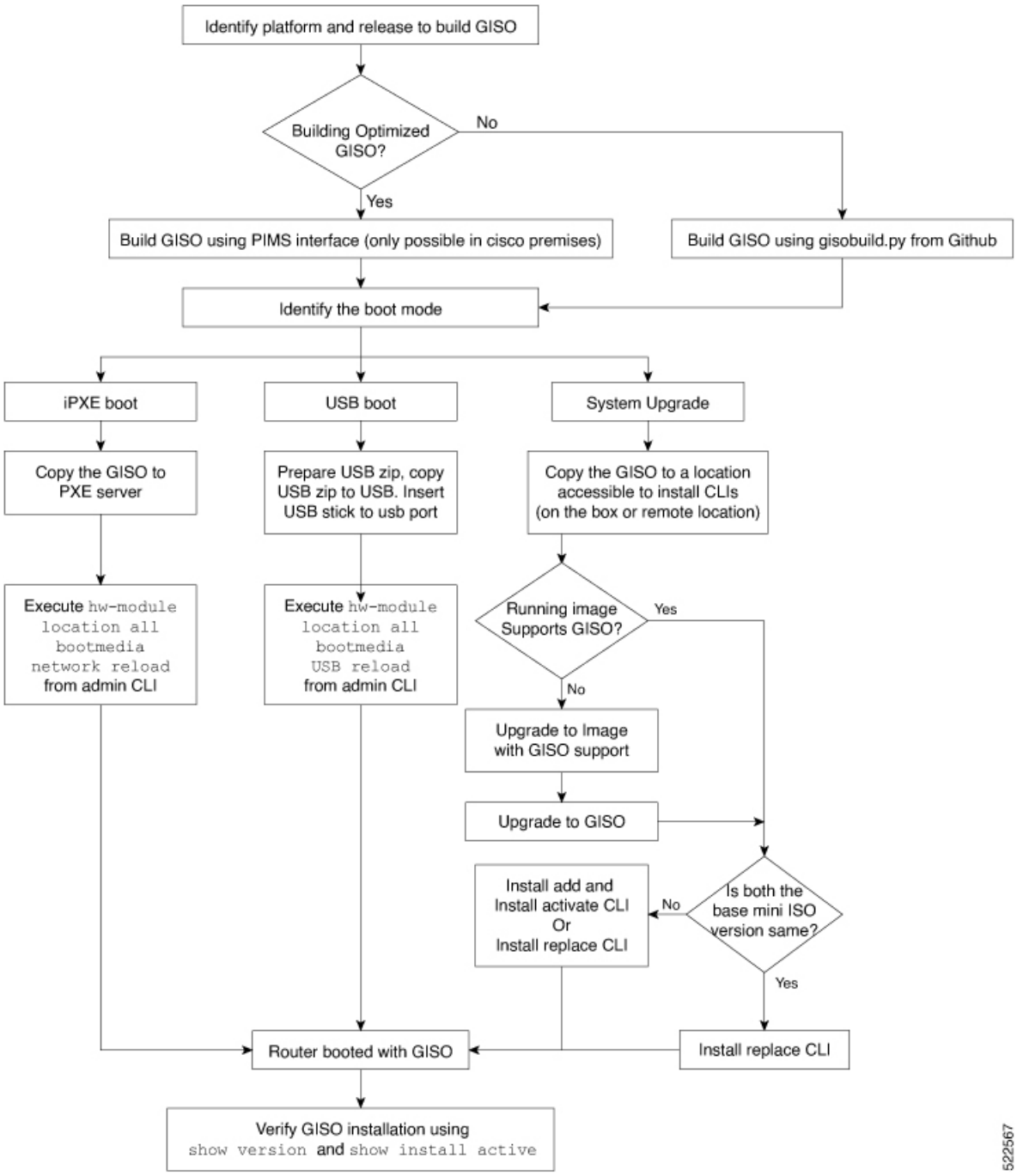
Note This document is applicable only for the following Cisco NCS 540 router variants:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For all other Cisco NCS 540 router variants, see the *Build a Golden ISO* section in the *Install XR7 OS on NCS 540 Series Routers* chapter.

The following image shows the workflow for building and installing golden ISO.

Figure 5: Golden ISO Workflow



Build Golden ISO

The customized ISO is built using Cisco Golden ISO (GISO) build script `gisobuild.py` available on the Github location.

The GISO build script supports automatic dependency management, and provides these functionalities:

- Builds RPM database of all the packages present in package repository.
- Scans the repositories and selects the relevant Cisco RPMs that matches the input iso.
- Skips and removes third-party RPMs that are not SMUs of already existing third-party base package in mini-x.iso.
- Displays an error and exits build process if there are multiple base RPMs of same release but different versions.
- Performs compatibility check and dependency check for all the RPMs. For example, the child RPM ncs5500-mpls-te-rsvp is dependent on the parent RPM ncs5500-mpls . If only the child RPM is included, the Golden ISO build fails.

Install Golden ISO

Golden ISO (GISO) automatically performs the following actions:

- Installs host and system admin RPMs.
- Partitions repository and TFTP boot on RP.
- Creates software profile in system admin and XR modes.
- Installs XR RPMs. Use **show install active** command to see the list of RPMs.
- Applies XR configuration. Use **show running-config** command in XR mode to verify.

Step 1 Download GISO image to the router using one of the following options:

- **PXE boot:** when the router is booted, the boot mode is identified. After detecting PXE as boot mode, all available ethernet interfaces are brought up, and DHClient is run on each interface. DHClient script parses HTTP or TFTP protocol, and GISO is downloaded to the box.

  When you bring up a router using the PXE boot mode, existing configurations are removed. To recover smart licensing configurations like Permanent License Reservation (PLR), enable these configurations after the router comes up.

```
Router#configure
Router(config)#license smart reservation
Router(config)#commit
```

- **USB boot or Disk Boot:** when the USB mode is detected during boot, and GISO is identified, the additional RPMs and XR configuration files are extracted and installed.
- **System Upgrade:** when the system is upgraded, GISO can be installed using **install add**, **install activate**, or using **install replace** commands.

Important To replace the current version and packages on the router with the version from GISO, note the change in command and format.

- In versions prior to Cisco IOS XR Release 6.3.3, 6.4.x and 6.5.1, use the **install update** command:

```
install update source <source path> <Golden-ISO-name> replace
```

- In Cisco IOS XR Release 6.5.2 and later, use the **install replace** command.

```
install replace <absolute-path-of-Golden-ISO>
```

Note To create a Bootable External USB Disk, do the following:

- Ensure that the USB Boot Disk has a minimum storage of 8GB, and that you have root/admin or appropriate permission to create bootable disk on linux machine.

a. Copy and execute usb-install script on the Linux machine to create a bootable external USB.

```
Router#admin

Router#./linux/misc/scripts/create_usb_zip ncs5500 ncs5500-goldenk9-x.iso-7.5.01.v1

  adding: EFI/ (stored 0%)
  adding: EFI/boot/ (stored 0%)
  adding: EFI/boot/grub.cfg (deflated 66%)
  adding: EFI/boot/bootx64.efi (deflated 67%)
  adding: boot/ (stored 0%)
  adding: boot/install-image.iso (deflated 1%)
Zip file created - usb_boot.zip
Router# ls -ltr usb_boot.zip
-rw-r--r-- 1 user eng 1448680576 Sep 14 04:13 usb_boot.zip
Router#
```

b. Reset the RSP/RP and plug in bootable USB to RSP/RP's front panel. The USB will get detected in ROMMON. Note that when the system is in ROMMON, and if you add a front panel external USB, the USB will not be detected until the RSP/RP is reset.

The options to upgrade the system are as follows:

- **system upgrade from a non-GISO (image that does not support GISO) to GISO image:** If a system is running a version1 with an image that does not support GISO, the system cannot be upgraded directly to version2 of an image that supports GISO. Instead, the version1 must be upgraded to version2 mini ISO, and then to version2 GISO.
- **system upgrade in a release from version1 GISO to version2 GISO:** If both the GISO images have the same base version but different labels, **install add** and **install activate** commands does not support same version of two images. Instead, using **install source** command installs only the delta RPMs. System reload is based on restart type of the delta RPMs.

  Using **install replace** command performs a system reload, irrespective of the difference between ISO and the existing version.
- **system upgrade across releases from version1 GISO to version2 GISO:** Both the GISO images have different base versions. Use **install add** and **install activate** commands, or **install replace** command to perform the system upgrade. The router reloads after the upgrade with the version2 GISO image.

Step 2 Run the **show install repository all** command in System Admin mode to view the RPMs and base ISO for host, system admin and XR.

```
sysadmin-vm:0_RP0#show install repository all
Admin repository
--------------------
ncs5500-sysadmin-6.2.2
ncs5500-sysadmin-hostos-6.2.2-r622.CSCcv10001.admin.x86_64
ncs5500-sysadmin-hostos-6.2.2-r622.CSCcv10001.admin.arm
ncs5500-sysadmin-system-6.2.2-r622.CSCcv10005.x86_64
ncs5500-sysadmin-system-6.2.2-r622.CSCcv10005.arm
....
XR repository
------------------
ncs5500-iosxr-mgbl-3.0.0.0-r622.x86_64
ncs5500-xr-6.2.2
....
Host repository
--------------------
host-6.2.2
```

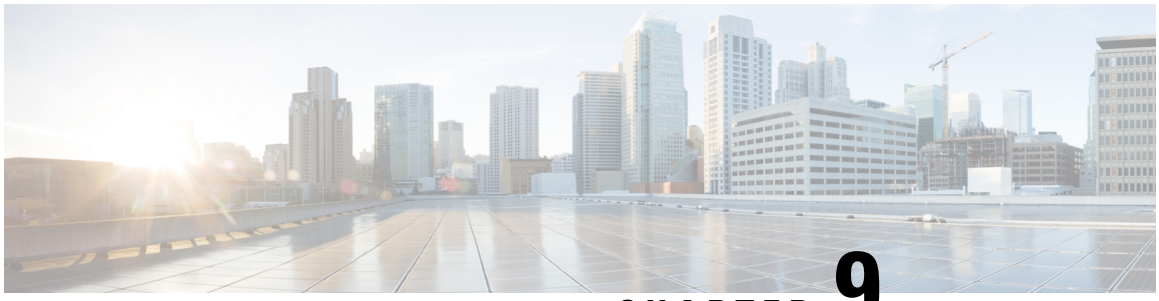
Step 3 Run the **show install package <golden-iso>** command to display the list of RPMs, and packages built in GISO.

Note To list RPMs in the GISO, the GISO must be present in the install repository.

```
Router#show install package ncs5500-goldenk9-x64-6.2.2

This may take a while ...
    ISO Name: ncs5500-goldenk9-x64-6.2.2
    ISO Type: bundle
    ISO Bundled: ncs5500-mini-x64-6.2.2
    Golden ISO Label: temp
    ISO Contents:
        ISO Name: ncs5500-xr-6.2.2
        ISO Type: xr
        rpms in xr ISO:
            iosxr-os-ncs5500-64-5.0.0.0-r622
            iosxr-ce-ncs5500-64-3.0.0.0-r622
            iosxr-infra-ncs5500-64-4.0.0.0-r622
            iosxr-fwding-ncs5500-64-4.0.0.0-r622
            iosxr-routing-ncs5500-64-3.1.0.0-r6122

        ISO Name: ncs5500-sysadmin-6.2.2
        ISO Type: sysadmin
        rpms in sysadmin ISO:
            ncs5500-sysadmin-topo-6.2.2-r622
            ncs5500-sysadmin-shared-6.2.2-r622
            ncs5500-sysadmin-system-6.2.2-r622
            ncs5500-sysadmin-hostos-6.2.2-r622.admin
        ...

        ISO Name: host-6.2.2
        ISO Type: host
        rpms in host ISO:
            ncs5500-sysadmin-hostos-6.2.2-r622.host

        Golden ISO Rpms:
            xr rpms in golden ISO:
                ncs5500-k9sec-x64-2.2.0.1-r622.CSCxr33333.x86_64.rpm
                openssh-scp-6.6p1.p1-r0.0.CSCtp12345.xr.x86_64.rpm
                openssh-scp-6.6p1-r0.0.xr.x86_64.rpm
                ncs5500-mpls-x64-2.1.0.0-r622.x86_64.rpm
                ncs5500-k9sec-x64-2.2.0.0-r622.x86_64.rpm
```

```
sysadmin rpms in golden ISO:
    ncs5500-sysadmin-system-6.2.2-r622.CSCcv11111.x86_64.rpm
    ncs5500-sysadmin-system-6.2.2-r622.CSCcv11111.arm.rpm
    openssh-scp-6.6p1-r0.0.admin.x86_64.rpm
    openssh-scp-6.6p1-r0.0.admin.arm.rpm
    openssh-scp-6.6p1.p1-r0.0.CSCtp12345.admin.x86_64.rpm
    openssh-scp-6.6p1.p1-r0.0.CSCtp12345.admin.arm.rpm
    ncs5500-sysadmin-hostos-6.2.2-r622.CSCcv10001.admin.x86_64.rpm
    ncs5500-sysadmin-hostos-6.2.2-r622.CSCcv10001.admin.arm.rpm

host rpms in golden ISO:
    openssh-scp-6.6p1-r0.0.host.x86_64.rpm
    openssh-scp-6.6p1-r0.0.host.arm.rpm
    openssh-scp-6.6p1.p1-r0.0.CSCtp12345.host.x86_64.rpm
    openssh-scp-6.6p1.p1-r0.0.CSCtp12345.host.arm.rpm
```

The ISO, SMUs and packages in GISO are installed on the router.



CHAPTER 9

Disaster Recovery

Note This document is applicable only for the following variants of the Cisco NCS 540 router variants:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

For information on booting the other Cisco NCS 540 router variants using iPXE or USB drive, see the *Setup Cisco NCS 540 Series Routers with XR7 OS* chapter.

The topics covered in this chapter are:

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

- You 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.

Note The NCS-5501-SE PID supports a USB device with a storage capacity of 128 GB (max).

- 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 75.

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:
  a. Run the **show controller card-mgr inventory summary** command and identify the active RP with the Master chip.
  b. Insert the USB drive to the active RP.
  c. 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.

  a. Insert the USB drive.
  b. Connect to the console.
  c. Power the router.
  d. Press **Esc** or **Del** to pause the boot process and get the RP to BIOS menu.
  e. 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 cancel the 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 the Router 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 78.

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 VM 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.

Note While ZTP executes, intermediate configuration is created to control interface addressing and routing information. When the configuration file is downloaded, this immediate configuration is removed and downloaded configuration will be applied. But, when the script file is downloaded intermediate configuration is kept for scripts to communicate with remote hosts. Once the script is ended, the final configuration needs to be applied to the router using the **commit replace** command. This ensures that the intermediate configuration is replaced. If the **commit replace** command is not applied after the script execution, intermediate configuration will remain and the final configuration will not take effect.

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
```

Note For the following variants of Cisco NCS 540 series routers, use the **reload bootmedia network location all noprompt** command for iPXE boot process:

- N540-28Z4C-SYS-A/D
- N540X-16Z4G8Q2C-A/D
- N540-12Z20G-SYS-A/D
- N540X-12Z16G-SYS-A/D

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]
```

Note The following variants of Cisco NCS 540 series routers do not support the **sysadmin-vm:0_RP0** prompt:

- N540-28Z4C-SYS-A/D
- N540X-16Z4G8Q2C-A/D
- N540-12Z20G-SYS-A/D
- N540X-12Z16G-SYS-A/D

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
```

Disaster Recovery Using Manual iPXE Boot

Manually booting the system using iPXE can be used to reinstall a clean system in case of a corrupt install or recover lost password. However, all the disks will be wiped out and the configuration will be removed.

Step 1 Press **Del** or **Esc** key to enter the Boot manager.

Step 2 Use the arrow keys (up, down) to select **UEFI: Built-in EFI IPXE** to enable iPXE boot. The iPXE boot launches the auto boot.

If the standby RP is being recovered and an active RP is present, the image is pulled from the active RP and auto boot is launched. In case of a single RP, or the other RP is in BIOS or unavailable, iPXE iteratively tries to configure the available interfaces in a loop. The following message is displayed at the end of every iteration:

```
Press Ctrl-B for the iPXE command line...
```

To manually boot using iPXE, press **Ctrl-B** keys to reach the iPXE command line.

Step 3 Identify the management interface. If the management interface is connected properly and is UP, it displays `Link:up` in the following output:

Example:

```
iPXE> ifstat
net0: 00:a0:c9:00:00:00 using i350-b on PCI01:00.0 (closed)
  [Link:up, TX:0 TXE:0 RX:0 RXE:0]
net1: 00:a0:c9:00:00:01 using i350-b on PCI01:00.1 (closed)
  [Link:up, TX:0 TXE:0 RX:0 RXE:0]
net2: 00:a0:c9:00:00:02 using i350-b on PCI01:00.2 (closed)
  [Link:down, TX:0 TXE:0 RX:0 RXE:0]
  [Link status: Down (http://ipxe.org/38086193)]
net3: 00:a0:c9:00:00:03 using i350-b on PCI01:00.3 (closed)
  [Link:down, TX:0 TXE:0 RX:0 RXE:0]
  [Link status: Down (http://ipxe.org/38086193)]
net4: 00:00:00:00:00:04 using dh8900cc on PCI02:00.1 (closed)
  [Link:down, TX:0 TXE:0 RX:0 RXE:0]
  [Link status: Down (http://ipxe.org/38086193)]
net5: 00:00:00:00:00:05 using dh8900cc on PCI02:00.2 (closed)
  [Link:down, TX:0 TXE:0 RX:0 RXE:0]
  [Link status: Down (http://ipxe.org/38086193)]
net6: 04:62:73:08:57:86 using dh8900cc on PCI02:00.3 (closed)
  [Link:up, TX:0 TXE:0 RX:0 RXE:0]

iPXE> set net6/ip 10.x.x.y
iPXE> set net6/netmask 255.x.x.x
iPXE> set net6/gateway 10.x.x.x
iPXE>
iPXE> ifopen net6

iPXE> ping 10.x.x.z
64 bytes from 10.x.x.z: seq=1
64 bytes from 10.x.x.z: seq=2
Finished: Operation canceled (http://ipxe.org/0b072095)

iPXE> boot http://10.x.x.z/<dir-to-iso>/ncs5500-mini-x.iso-<version>_IMAGE
http://10.x.x.z/<dir-to-iso>/ncs5500-mini-x.iso-<version>_IMAGE... ok
```

Choose the net interface that shows `Link:up`. If there are multiple interfaces that show the status as UP, identify the management interface with MAC address.

iPXE also supports HTTP, TFTP and FTP. For more information, see https://ipxe.org/cmd.

Note Keep the standby RP in BIOS while installing the active RP.

After installing the mini ISO image, the system reboots. After successful reboot, specify the root username and password. Once you get back to the XR prompt, you can load the configuration and install remaining packages.