System Setup and Software Installation Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.0.x

First Published: 2019-08-30

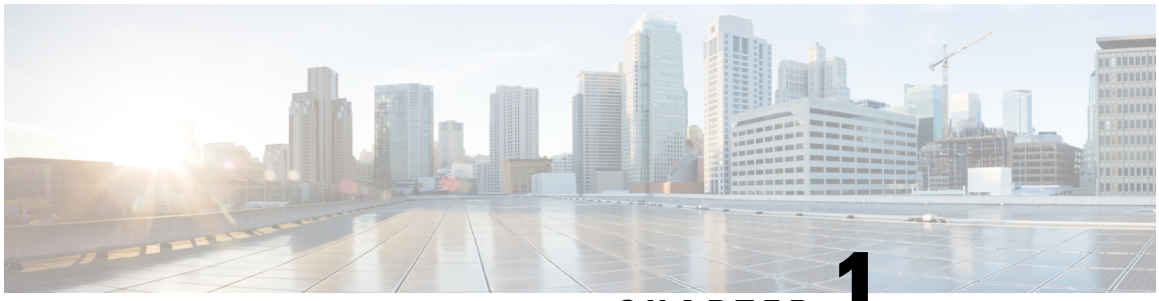
Last Modified: 2019-12-09

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

PART I

Setup System and Install IOS XR Software



CHAPTER 1

Overview of the Router

The Cisco NCS 540 system is a high fault-resilient platform, which provides next generation data-center switching environment with high bandwidth and low latency.

Cisco NCS 540 system provides:

- High performance (300 Gbps full-duplex switching)
- Flexible network interface (10GbE, 25GbE, 40GbE, 50GbE, and 100GbE interfaces as well as ILKN interfaces)
- Traffic manager and in-band management
- Flexible and microcode-programmable packet processor
- Label Switched Router (LSR) and possible Light Label switched Edge Router (LER) features and functionality with limited hardware scale and software functionality.

Note Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:

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

These variants of the NCS 540 Series Routers run on the Cisco IOS XR7 operating system. For information about setting up the routers, see Setup Cisco NCS 540 Series Routers with XR7 OS, on page 73. For information about installing the XR7 OS on NCS 540 series routers, see Install XR7 OS on NCS 540 Series Routers, on page 89.

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.

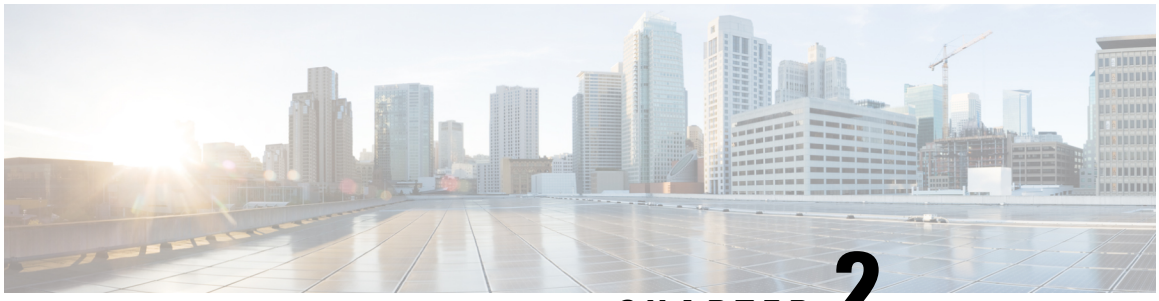
The command modes are applicable for the Cisco NCS540 Series Routers. This table lists the command modes for the LXCs.

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#`

System 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 2

Bring-up the Router

After installing the hardware, boot the router. Connect to the XR console port and power on the router. The router completes the boot process using the pre-installed operating system (OS) image. If no image is available within the router, the router can be booted using 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.

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 Entry Module (PEM) and 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.

Setup Root User Credentials

When the router boots for the first time, the system prompts the user to configure root credentials (username and password). These credentials are configured as the root user on the XR (root-lr) console, the System Admin VM (root-system), and as disaster-recovery credentials.

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

When starting the router for the first time, or after a reimage, 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 username and password must be safeguarded as it has the superuser privileges. It is used to access the complete router configuration.

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

Reenter the password for the root user. The password is not accepted if it does not match the password that is entered in the previous step. 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 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
$6$RS5kn1r/ww.DDn1.$eDFxhqTEYa6hqTs3MODQt11mBp4cMgdQqt.syC/J83lQIl1yJT9vd2W8zEHfBKz4.z4FyImRdzwvKTqAMuyBA0

!
```

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

SUMMARY STEPS

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

DETAILED STEPS

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

Step 2 **admin**

Example:

The 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 3 (Optional) **exit**

Return to the XR mode from the System Admin mode.

Configure the Management Port

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

Before you begin

- Consult your network administrator or system planner to procure IP addresses and a subnet mask for the management interface.
- Physical port Ethernet 0 and Ethernet 1 on RP are the management ports. Ensure that the port is connected to management network.

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

SUMMARY STEPS

1. **configure**
2. **interface MgmtEth** *rack/slot/port*
3. (Optional) **vrf** *vrf-id*
4. **ipv4 address** *ipv4-address subnet-mask*
5. **ipv4 address** *ipv4 virtual address subnet-mask*
6. **no shutdown**
7. **exit**
8. **router static address-family ipv4 unicast** *0.0.0.0/0 default-gateway*
9. Use the **commit** or **end** command.

DETAILED STEPS

Step 1 **configure**

Example:

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

Enters 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 (Optional) **vrf** *vrf-id*

Example:

```
RP/0/RP0/CPU0:router(config-sg-tacacs+)# vrf vrf-id
```

Specifies the Virtual Private Network (VPN) routing and forwarding (VRF) reference.

Step 4 **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 5 **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 6 **no shutdown**

Example:

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

Places the interface in an "up" state.

Step 7 **exit**

Example:

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

Exits the Management interface configuration mode.

Step 8 **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 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

Connect to the management port to the ethernet network. With a terminal emulation program, establish a SSH or telnet connection to the management interface port using its IP address. Before establishing a telnet session,

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

Perform Clock Synchronization with NTP Server

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

Before you begin

Configure and connect to the management port.

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **configure**

Example:

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

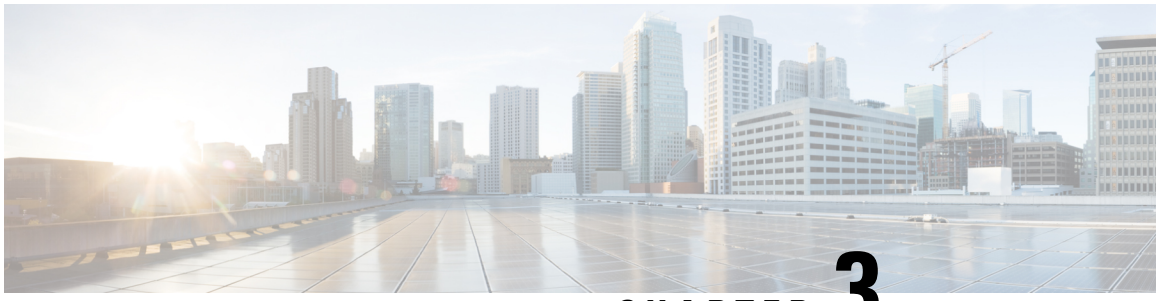
Enters mode.

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 3

Perform Preliminary Checks

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

Verify 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 hw-module fpd**

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:

```
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/RP0     N540-24Z8Q2C-M   OPERATIONAL    OPERATIONAL   NSHUT
0/FT0     N540-FAN   OPERATIONAL    N/A     NSHUT
0/FT1     N540-FAN   OPERATIONAL    N/A     NSHUT
0/FT2     N540-FAN   OPERATIONAL    N/A     NSHUT
0/FT3     N540-FAN   OPERATIONAL    N/A     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.

Step 3 **show hw-module fpd**

Example:

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

Displays the list of hardware modules detected on the router.

```
RP/0/RP0/CPU0:Router#show hw-module fpd
FPD Versions
=================
Location Card type      HWver FPD device ATR Status Running Programd
------------------------------------------------------------------------------
0/RP0    N540-24Z8Q2C-M 0.5   MB-MIFPGA      CURRENT 0.04    0.04
0/RP0    N540-24Z8Q2C-M 0.5   Bootloader     CURRENT 1.07    1.07
0/RP0    N540-24Z8Q2C-M 0.5   CPU-IOFPGA     CURRENT 0.03    0.03
0/RP0    N540-24Z8Q2C-M 0.5   MB-IOFPGA      CURRENT 0.16    0.16
RP/0/RP0/CPU0:ios#
```

Verify Node Status

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **show platform**

Example:

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

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

```
RP/0/RP0/CPU0:<router>#show platform
Node   Type  State  Config state
--------------------------------------------------------------------------------
0/RP0/CPU0 N540-X-24Z8Q2C-M(Active) IOS XR RUN NSHUT
0/RP0/NPU0 Slice UP
0/FT0  N540-FAN OPERATIONAL  NSHUT
0/FT1  N540-FAN OPERATIONAL  NSHUT
0/FT2  N540-FAN OPERATIONAL  NSHUT
0/FT3  N540-FAN OPERATIONAL  NSHUT
```

Verify that all RPs are listed and their state is OPERATIONAL. This indicates that the XR console is operational on the cards.

Step 2 **admin**

Example:

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

Enters mode.

Step 3 **show platform**

Example:

```
#show platform
```

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

This is an example for single-chassis system:

```
RP/0/RP0/CPU0:<router>#sh platform
Thu Mar 29 06:50:06.788 UTC
Location  Card Type  HW State  SW State  Config State
------------------------------------------------------------------------------
0/RP0  N540-X-24Z8Q2C-M OPERATIONAL  OPERATIONAL  NSHUT
0/FT0  N540-FAN   OPERATIONAL  N/A    NSHUT
0/FT1  N540-FAN   OPERATIONAL  N/A    NSHUT
0/FT2  N540-FAN   OPERATIONAL  N/A    NSHUT
0/FT3  N540-FAN   OPERATIONAL  N/A    NSHUT
```

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

Hardware states:

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

Software states:

- OPERATIONAL—Software is operating normally and is fully functional
- SW_INACTIVE—Software is not completely operational
- FAILED—Software is operational but the card has experienced some internal failure

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) 2013-2017 by Cisco Systems, Inc.

Build Information:
Built By : <user>
Built On : <date and time stamp>
Build Host : iox-lnx-030
Workspace : /x.x.x/ncs540/ws
Version : <release-version>
Location : /opt/cisco/XR/packages/

cisco NCS-540 () processor
System uptime is 1 day, 16 hours, 18 minutes
```

What to do next

Verify the result to ascertain whether a system upgrade or additional package installation is required. If that is required, refer to the tasks in the chapter Perform System Upgrade and Install Feature Packages, on page 33.

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:

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.

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.

In the above result:

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

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

Verify 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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **admin**

Example:

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

Enters mode.

Step 2 **show sdr**

Example:

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

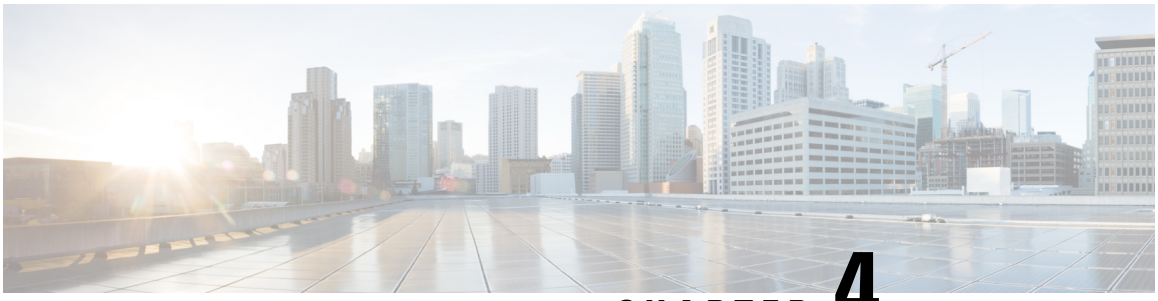
Displays the SDR information for every node.

```
RP/0/RP0/CPU0:router#show  sdr
Type                 NodeName       NodeState      RedState       PartnerName
------------------------------------------------------------------------------
LC                   0/0/CPU0       IOS XR RUN     N/A            N/A
RP                   0/RP0/CPU0     IOS XR RUN     ACTIVE         NONE
Slice                0/RP0/NPU0     UP             N/A            N/A
N540-X-24Z8Q2C-M     0/RP0          OPERATIONAL                   N/A
N540-FAN             0/FT0          OPERATIONAL                   N/A
N540-FAN             0/FT1          OPERATIONAL                   N/A
N540-FAN             0/FT2          OPERATIONAL                   N/A
N540-FAN             0/FT3          OPERATIONAL                   N/A
```

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.



CHAPTER 4

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.

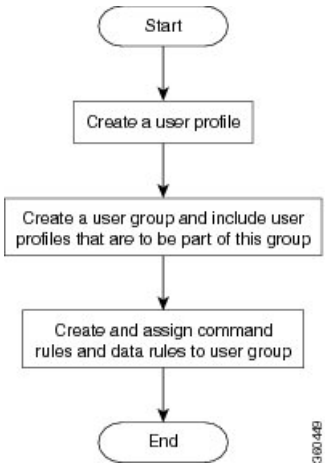
Note If any user on XR is deleted, the local database checks whether there is a first user on System Admin VM.

- 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 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.

SUMMARY STEPS

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

What to do next

- Create user group that includes the user created in this task. See Create a User Group in System Admin VM, on page 23.
- Create command rules that apply to the user group. See Create Command Rules, on page 25.
- Create data rules that apply to the user group. See Create Data Rules, on page 28.

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.

SUMMARY STEPS

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

6. 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 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. See Create Command Rules, on page 25.
- Create data rules. See Create Data Rules, on page 28.

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 23.

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 28.

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 23.

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.

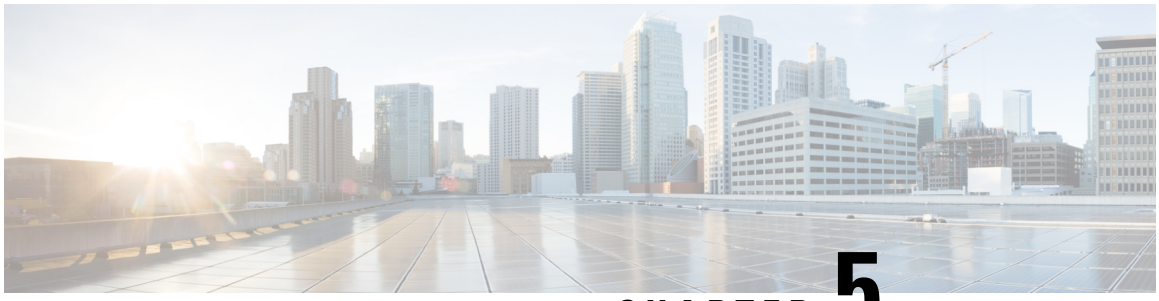
When you need to make use of the disaster recovery username, you need to enter it as *username***@localhost**.

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.



CHAPTER 5

Perform System Upgrade and Install Feature Packages

The system upgrade and package installation processes are executed using **install** commands on the router. The processes involve adding and activating the iso images (*.iso*) 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

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

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.

System upgrade is done by installing a base package–Cisco IOS XR Unicast Routing Core Bundle.

The filename for this bundle is *ncs540-mini-x.iso*.

Install this ISO image using **install** commands. For more information about the install process, see Workflow for Install Process, on page 36.

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

Do not reload the router during an upgrade operation.

Note Ensure that you perform a chassis reload to enable hardware programming if a chassis upgrade through ISSU to IOS XR Release 7.6.x and later from an earlier software version. The chassis reload is mandatory, if you must enable a maximum 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 have not 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.

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

Upgrading Features

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

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

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

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

- ncs540-isis-1.0.0.0-r701.x86_64.rpm
- ncs540-k9sec-1.1.0.0-r701.x86_64.rpm
- ncs540-li-1.0.0.0-r701.x86_64.rpm
- ncs540-mcast-1.0.0.0-r701.x86_64.rpm
- ncs540-mgbl-1.0.0.0-r701.x86_64.rpm
- ncs540-mini-x-7.0.1.iso
- ncs540-mpls-1.0.0.0-r701.x86_64.rpm
- ncs540-mpls-te-rsvp-1.0.0.0-r701.x86_64.rpm

- ncs540-ospf-1.0.0.0-r701.x86_64.rpm

Package and SMU installation is performed using **install** commands. For more information about the install process, see Install Packages, on page 36.

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 activationg 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

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

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, **ncs540**-sysadmin.

Workflow for Install Process

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

For installing a package, see Install Packages, on page 36. For uninstalling a package, see Uninstall Packages, on page 43.

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.

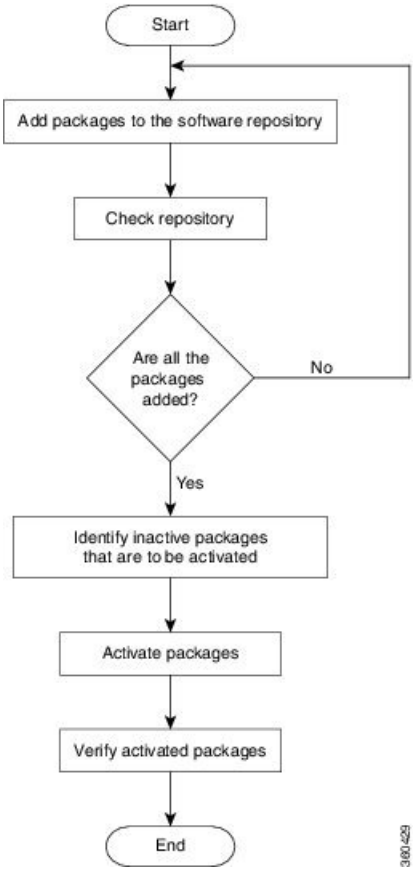
Note Only the following Cisco NCS 540 router variants support the System Admin mode:

- 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. For details about configuring the management port, see Configure the Management Port, on page 7.
- Copy the package to be installed either on the router's hard disk or on a network server to which the router has access.

SUMMARY STEPS

1. Execute one of these:
   - **install add source** *<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 ...*
2. **show install request**
3. **show install repository**

4. **show install inactive**
5. Execute one of these:
   - **install activate** *package_name*
   - **install activate id** *operation_id*
6. **show install active**
7. **install commit**

DETAILED STEPS

Step 1 Execute one of these:

- **install add source** *<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:/ncs540-mpls-te-rsvp-1.0.0.0-<release-number>.x86_64.rpm
ncs540-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/
```

```
RP/0/RP0/CPU0:router#install add source
/harddisk:/ncs540-mpls-te-rsvp-1.0.0.0-<release-number>.x86_64.rpm
ncs540-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/
ncs540-mcast-1.0.0.0-<release-number>.x86_64.rpm
 ncs540-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 as soon as possible.

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 ncs540-mcast-1.0.0.0-<release-number>.x86_64.rpm
ncs540-mpls-1.0.0.0-<release-number>.x86_64.rpm
```

The *operation_id* is that of the **install add** operation. This command can also be run from System Admin mode. The package configurations are made active on the router. As a result, new features and software fixes take effect. This operation is performed in asynchronous mode, 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 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. Upon activation completion, 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.

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

Step 7 **install commit**

Example:

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

Commits the 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.

Installing Packages: Related Commands

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

What to do next

- Ensure that you commit the upgrade using **install commit**.
- 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 43.

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

Install Prepared Packages

- 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 reduced.

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.

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.
- Performs 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.
- Performs 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.

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.

SUMMARY STEPS

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

DETAILED STEPS

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

For details, see Install Packages, on page 36.

Step 2 **show install repository**

Example:

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

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

Step 3 Execute one of these:

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

Example:

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

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

Step 4 **show install prepare**

Example:

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

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

Step 5 **install activate**

Example:

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

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

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

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 6 **show install active**

Example:

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

Displays packages that are active.

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

Step 7 **install commit**

Example:

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

Installing Packages: Related Commands

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

What to do next

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

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

Uninstall Packages

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

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

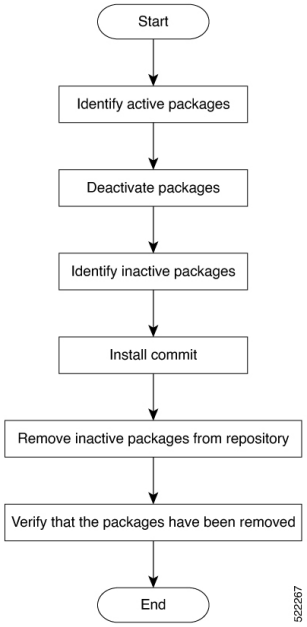
For information on deleting packages on other Cisco NCS 540 router variants, see the *Delete Optional Packages* section in the *Install XR7 OS on NCS 540 Series Routers* chapter.

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.

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **show install active**

Example:

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

Displays active packages. Only active packages can be deactivated.

Step 2 Execute one of these:

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

Example:

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:

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**

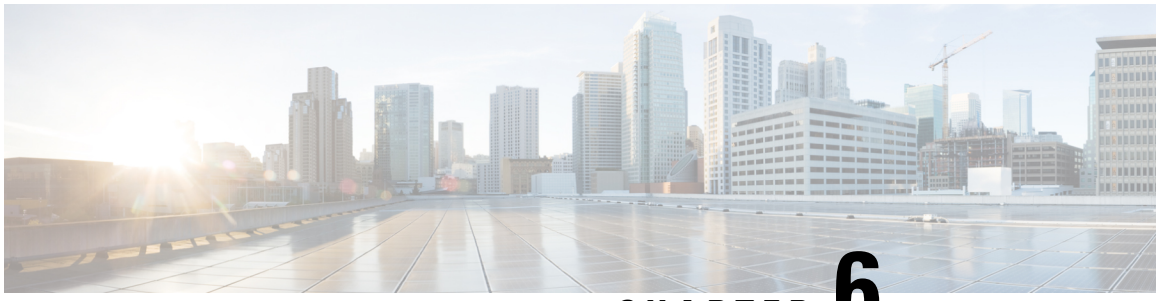
Example:

```
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 6

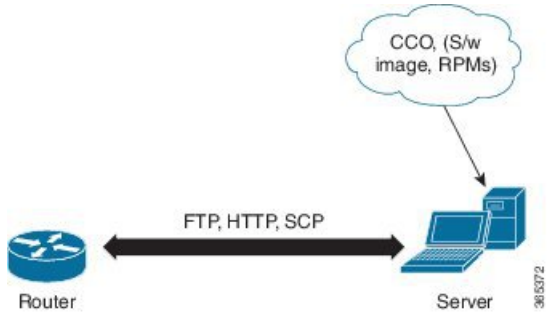
Manage Automatic Dependency

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

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

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

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



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

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

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

Note 1.
2.

The rest of this chapter contains these sections:

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 update install source** command. When the **install update install source** 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 update install source** command is:

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

Four scenarios in which you can use the **install update 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 update source install source [repository]

- **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.)

- **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.

- **When an SMU is specified**

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

Upgrade Base Software Version

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

Note SMUs are not upgraded as part of this process.

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

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

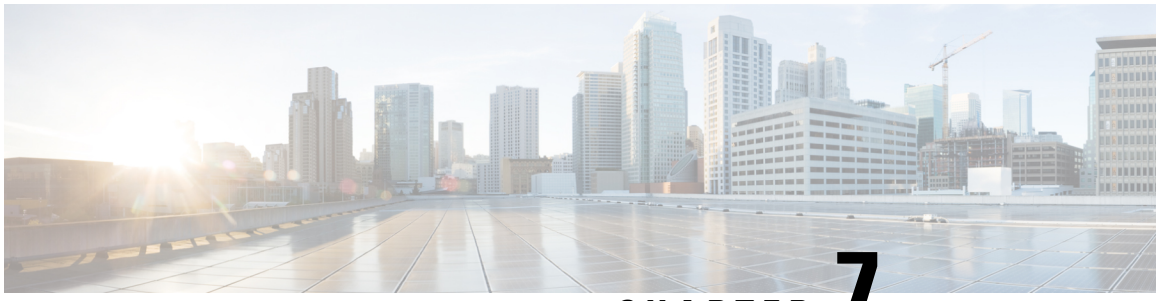
Note VRF and TPA on dataport is not supported. If the server is reachable only through non-default VRF interface, the file must already be retrieved using ftp, sfp, scp, http or https protocols.

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

- **The version number is specified**

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

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



CHAPTER 7

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 55.

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:

- 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

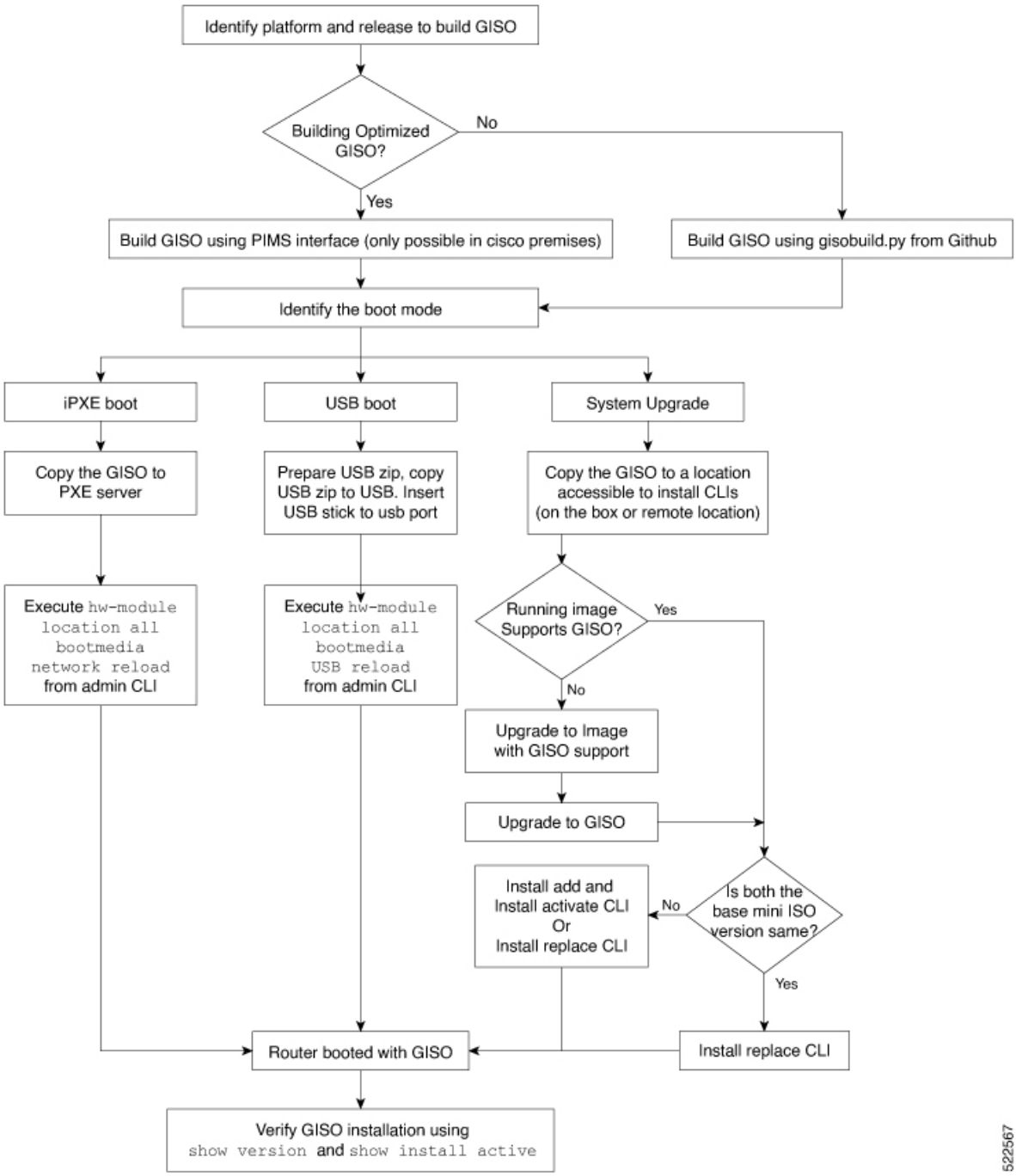
Note This document is applicable only for the following Cisco NCS 540 router variants:

- 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 Using Script

To build GISO, provide the following input parameters to the script:

- Base mini-x.iso (mandatory)

- XR configuration file (optional)
- one or more Cisco-specific SMUs for host, XR and System admin (optional)
- one or more third-party SMUs for host, XR and System admin (optional)
- Label for golden ISO (optional)
- Optional RPMs

Note To successfully add k9sec RPM to GISO, change the permission of the file to `644` using the **chmod** command.

```
chmod 644 [k9 sec rpm]
```

To build GISO, perform the following steps:

Before you begin

- To upgrade from a release that did not support GISO to a release supporting GISO version, it is mandatory to first upgrade to mini ISO with GISO support.
- The system where GISO is built must meet the following requirements:
  - System must have Python version 3.6 and later.
  - System must have free disk space of minimum 12 GB.
  - Verify that the Linux utilities `mount`, `rm`, `cp`, `umount`, `zcat`, `chroot`, `mkisofs` are present in the system. These utilities will be used by the script. Ensure privileges are available to execute all of these Linux commands.
  - Kernel version of the system must be later than 3.16 or later than the version of kernel of Cisco ISO.
  - Verify that a `libyaml rpm` supported by the Linux kernel is available to successfully `import yaml` in the tool.
  - User should have proper permission for security rpm(k9sec-rpm) in rpm repository, else security rpm would be ignored for Golden ISO creation.
- The system from where the `gisobuild.py` script is executed must have root credentials.

Step 1 Copy the script `gisobuild.py` from the Github location to an offline system or external server where the GISO will be built. Ensure that this system meets the pre-requisites described above in the *Before You Begin* section.

Step 2 Run the script `gisobuild.py` and provide parameters to build the golden ISO off the router.

Example:

```
[directory-path]$ gisobuild.py [-h] [-i <mini-x.iso>] [-r <rpm repository>]
[-c <config-file>] [-l <giso label>] [-m] [-v]
```

Note The `-i` option is mandatory, and either or both `-r` or `-c` options must be provided.

The corresponding GISO and build logs are available under the specified `out_directory` path. The default directory is `/output_gisobuild`.

where:

- -i is the path to mini-x.iso
- -r is the path to RPM repository
- -c is the path to XR config file
- -l is the golden ISO label
- -h shows the help message
- -v is the version of the build tool `gisobuild.py`
- -m is to build the migration tar to migrate from IOS XR to IOS XR 64 bit

Note It is recommended to build GISOs with a label name.

The corresponding GISO and build logs are available under the specified directory in `out_directory`. If a directory is not specified, the files are placed in `/output_gisobuild` directory.

Note The GISO script does not support verification of XR configuration.

What to do next

Install the GISO image on the router.

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.
- **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.

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.

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.

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

Install Replace with Golden ISO

Step 1 **install replace** *<GISO-location>* [**commit** | **noprompt**]

Example:

```
Router#install replace harddisk:/<giso-image>.iso
 ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Install operation 11 started by root:
exec-timeout is suspended.
No install operation in progress at this moment
Label = More_Pkgs
ISO <giso-iso-image>.iso in input package list. Going to upgrade the system to

version <new-giso-image>.
System is in committed state
Current full-label: <giso-image>_R_Commit
Current only-label: R_Commit
Current label: R_Commit
Updating contents of golden ISO
Scheme : localdisk
Hostname : localhost
Username : None
SourceDir : /ws
Collecting software state..
Getting platform
Getting supported architecture
Getting active packages from XR
Getting inactive packages from XR
Getting list of RPMs in local repo
Getting list of provides of all active packages
Getting provides of each rpm in repo
Getting requires of each rpm in repo
Fetching .... <giso-image>.iso
Label within GISO: More_Pkgs
Skipping <platform>-mgbl-3.0.0.0-<release>.x86_64.rpm from GISO as it's active
Adding packages
        <platform>-golden-x-<release>-<Label>.iso
RP/0/RP0/CPU0:Jun 20 14:43:59.349 UTC: sdr_instmgr[1164]: %INSTALL-INSTMGR-2-OPERATION_SUCCESS :

Install operation 12 finished successfully
Install add operation successful
Activating <platform>-golden-x-<release>-<Label>
Jun 20 14:44:05 Install operation 13 started by root:
  install activate pkg <platform>-golden-x-<release>-<Label> replace noprompt
Jun 20 14:44:05 Package list:
Jun 20 14:44:05     <platform>-golden-x-<release>-<Label>.iso
Jun 20 14:44:29 Install operation will continue in the background
exec-timeout is resumed.
Router# Install operation 13 finished successfully
Router: sdr_instmgr[1164]: %INSTALL-INSTMGR-2-OPERATION_SUCCESS :

Install operation 13 finished successfully


Router#install replace <path-to-image> <platform-name-golden-x-<version>-<label>.iso
Tue Mar 17 08:07:15.176 UTC
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Mar 17 08:07:24 Install operation 46 started by root:
Mar 17 08:07:24   install replace source <path-to-image> <platform-name-golden-x-<version>-<label>.iso
Mar 17 08:07:24 No install operation in progress at this moment
```

```
Mar 17 08:07:24 Checking system is ready for install operation
Mar 17 08:07:24 'install replace' in progress
Mar 17 08:07:24 Label = GISO_IMAGE_XRV9K_<version>
Mar 17 08:07:24 ISO xrv9k-goldenk9-x-<version>-<label>.iso in input package list. Going to upgrade
the system to version <new-version>
Mar 17 08:07:25 Scheme : http
Mar 17 08:07:25 Hostname : 10.x.x.x
Mar 17 08:07:25 Collecting software state..
Mar 17 08:07:25 Getting platform
Mar 17 08:07:25 Getting supported architecture
Mar 17 08:07:25 Getting active packages from XR
Mar 17 08:07:25 Getting inactive packages from XR
Mar 17 08:07:28 Getting list of RPMs in local repo
Mar 17 08:07:28 Getting list of provides of all active packages
Mar 17 08:07:28 Getting provides of each rpm in repo
Mar 17 08:07:28 Getting requires of each rpm in repo
Mar 17 08:07:36 Fetching .... xrv9k-goldenk9-x-<version>-<label>.iso
Mar 17 08:08:02 Adding packages
        xrv9k-goldenk9-x-<version>-<label>.iso
Router:Mar 17 08:09:03.487 UTC: sdr_instmgr[1281]: %INSTALL-INSTMGR-2-OPERATION_SUCCESS : Install
operation 47 finished successfully
Mar 17 08:09:03 Install add operation successful
Mar 17 08:09:08 Activating xrv9k-goldenk9-x-<version>-<label>
Mar 17 08:09:10 Install operation 46 started by root:
  install activate pkg xrv9k-goldenk9-x-<version>-<label> replace
Mar 17 08:09:10 Package list:
Mar 17 08:09:10     xrv9k-goldenk9-x-<version>-<label>
This install operation will reload the system, continue?
 [yes/no]:[yes] yes
Mar 17 08:10:30 Install operation will continue in the background
Mar 17 08:10:30 Activate operation ID is: 46 for 'install source' ID:46

Router# Install operation 46 finished successfully
%INSTALL-INSTMGR-2-OPERATION_SUCCESS : Install operation 46 finished successfully
sdr_instmgr[1150]: %INSTALL-INSTMGR-2-SYSTEM_RELOAD_INFO : The whole system will be reloaded to
complete install operation 46
```

Important For versions earlier than Cisco IOS XR Release 6.5.2, use the following command:

install update source *<absolute-path-of-Golden-ISO>* **replace**

For example,

```
Router#install update source harddisk:/ <giso-image>.iso replace
```

The version and label of the newly added GISO is compared with the version and label of the currently active version. If a mismatch is identified, a new partition is created and the full package is installed. After installation, the system reloads with the image and packages from the newly added GISO.

Note Activating or deactivating on a system that has a valid label invalidates the label. This action is irreversible. For example, running **show version** command on the system displays the label `6.3.3_633rev1005`. If any SMU is activated or deactivated on the system, the label `633rev1005` is invalidated, and the `show version` command displays only `6.3.3` as the label.

Step 2 **show version**

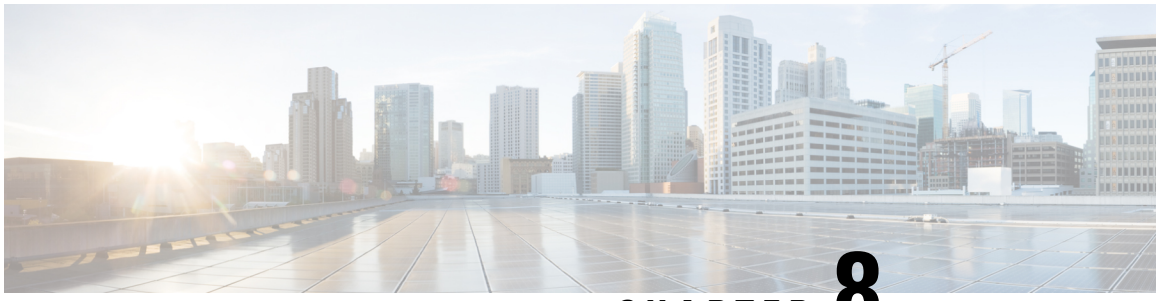
Example:

```
Router#show version
Wed Jun 20 15:06:37.915 UTC
Cisco IOS XR Software, Version <new-giso-image>
Copyright (c) 2013-2018 by Cisco Systems, Inc.
```

```
Build Information:
Built By     : <user>
Built On     : <date>
Build Host   : <host-name>
Workspace    : <workspace-name>
Version      : <version>
Location    : <path>
Label        : <label-name>

cisco <platform> () processor
System uptime is 3 hours 51 minutes
```

The system loads with the image and packages from the newly added GISO.



CHAPTER 8

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 64GB (max). USB 2.0 and USB 3.0 are supported.

Caution We recommend that you do not use Kingston USB 3.0 memory cards with 64GB storage capacity as this might cause a hardware error.

- 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 *ncs540-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 the Bootable USB Drive

Before you begin

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 reimaged with the version available on the USB drive.

Create a bootable USB drive. See Create a Bootable USB Drive Using Compressed Boot File.

Step 1 Plug in the bootable USB drive with the required image to an Active RP USB port on the router.

Step 2 Use one of the two methods to boot the router from the USB:

- Method 1

  Perform the following steps when you are unable to access the router console:

a. As the router reloads, you must press the ESC key to enter the **Boot Manager** window. A message, **Esc is pressed. Go to boot options.** is displayed.

b. In the next screen, select **Boot Manager**.

c. In the **Boot Manager** screen, select the USB drive from the list of boot devices and press **Enter**.

```
Cisco BIOS Setup Utility - Copyright (C) 2019 Cisco Systems, Inc

Boot Override
UEFI: Micron_M600_MTFDDAT064MBF, Partition 4
UEFI: Built-in iPXE
URFI: Built-in Shell
URFI: Built-in Grub
EFI USB Device (Sandisk)
UEFI: IPv4 0 Intel® I210 Gigabit Network Con
UEFI: IPv4 0 Intel® Ethernet Connection x552
UEFI: IPv4 1 Intel® Ethernet Connection x552
UEFI: IPv4 2 Intel® Ethernet Connection x552
UEFI: IPv4 3 Intel® Ethernet Connection x552
```

The router boots the image from the USB drive, and installs the image onto the hard disk. The router boots from the hard disk after the installation is successful.

- Method 2

USB based image boot can also be used when the router needs to be clean booted with a new image version.

a. At the **Sysadmin VM** prompt, execute the **hw-module location all bootmedia usb reload** command.

The router boots the image from the USB drive, and installs the image onto the hard disk. After image installation is successful, the router automatically boots from this newly installed image on the hard disk.

Note Clean boot results in previous logs, image, and config being removed. No user intervention is required for selecting the USB boot device during the boot to initiate the USB based recovery.

Step 3 After the booting is completed, specify the root-system **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 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.

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.

Ensure that the above configuration is successful.

- Use serial number of the router: 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 64.

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>/";
  } else
{
  # Auto-provision request, so provide ZTP script or configuration
  filename "http://<ip-address>/<script-directory-path>/";
  #filename "http://<ip-address>/<script-directory-path>/
  }
}
```

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 during installation, and then download and execute 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.

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/


http://10.37.1.235/ ... 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 Use the arrow keys (up, down) to select **UEFI: Built-in EFI IPXE** to enable iPXE boot. The iPXE boot launches the auto boot.

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

Step 2 Identify the management interface. If the management interface is connected properly and is UP, it displays `Link:up` in the following output:

Example:

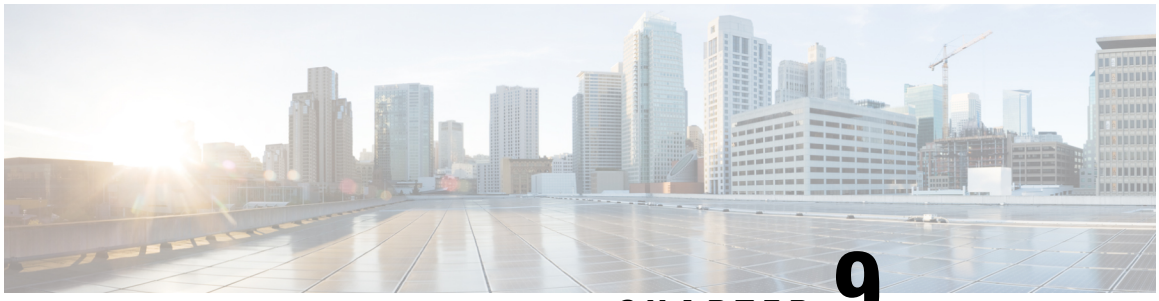
Choose the net interface that shows `Link:up`. If there are multiple interfaces that show the status as UP, identify the management interface with MAC address.

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

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.

PART II

Setup System and Install IOS XR7 Software



CHAPTER 9

Setup Cisco NCS 540 Series Routers with XR7 OS

The following variants of Cisco NCS 540 series routers run on XR7 OS:

- N540-28Z4C-SYS-A
- N540-28Z4C-SYS-D
- N540X-16Z4G8Q2C-A
- N540X-16Z4G8Q2C-D
- N540-12Z20G-SYS-A
- N540-12Z20G-SYS-D
- N540X-12Z16G-SYS-A
- N540X-12Z16G-SYS-D
- N540-FH-CSR-SY

XR7 OS provides significant architectural enhancements to Cisco IOS XR in these areas:

- **Modularity:** Decoupled hardware and software; disintegrated software with the flexibility to consume software packages based on requirement
- **Programmability:** Cloud scale enhancement with model-drivel APIs at all layers
- **Manageability:** Simplified software management and installation that is based on Linux tools

For more information about installing the router, see *Cisco NCS 540 Series Hardware Installation Guide*.

This document helps you set up the Cisco NCS 540 series router. You will bring-up the router, run a health check of the system, create user profiles, and assign privileges.

- Bring-up the Cisco NCS 540 Series Router, on page 74
- Perform Preliminary Checks with Cisco NCS 540 Series Router, on page 81
- Create Users and Assign Privileges on the Cisco NCS 540 Series Router, on page 86

Bring-up the Cisco NCS 540 Series Router

Connect to the console port on a Route Processor (RP) of the router, and power ON the router. By default, this console port connects to the XR console. If necessary, after configuration, establish subsequent connections through the management port.

The following table shows the console settings:

Table 1: Console Settings

Baud rate (in bps)	Parity	Stop bits	Data bits
115200	None	2	8

The baud rate is set by default and cannot be changed.

The router can be accessed using remote management protocols, such as SSH, Telnet, SCP and FTP. SSH is included in the software image by default, but telnet is not part of the software image. You must manually install the telnet optional package to use it.

After booting is complete, you must create a username and password. This credential is used to log on to the XR console, and get to the router prompt.

You can start or stop the console by using the following keyboard shortcuts:

- To start the console, press Ctrl + q.
- To stop the console, press Ctrl + s.

Note that by using Ctrl + s, the console output will be locked and you will need to initiate a Ctrl + q sequence to restore the console prompt.

The router completes the boot process using the pre-installed operating system (OS) image. If no image is available within the router, the router can be booted using iPXE boot or an external bootable USB drive.

Boot the Cisco NCS 540 Series Router Using Manual iPXE

Manually boot the router using iPXE if the router fails to boot when powered ON. An alternate method is to Boot the Cisco NCS 540 Series Router Using USB Drive.

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

You need a server running HTTPS, HTTP, or TFTP. Bring-up the PXE prompt using the following steps:

Step 1 Power ON the router.

Step 2 Press Esc or Del keys continuously (quick and repeated press and release) to pause the boot process, and get to the BIOS menu.

Step 3 Select `Boot Manager`, and then select `Built-in iPXE` option.

Step 4 When PXE boot starts reaching for a PXE server, press **Ctrl+B** keys to break into the PXE prompt.

Step 5 Add the following configuration for the router. This is required for the router to connect with the external server to download, and install the image. You can use HTTP, HTTPS or TFTP server.

Example:

```
iPXE> ifopen net0                    #Open the interface connecting outside world
iPXE> set net0/ip 10.0.0.2           #Configure the ip address of your router

iPXE> set net0/gateway 10.0.0.1      #configure the GW
iPXE> set net0/netmask 255.0.0.0     #Configure the Netmask
iPXE> ping 10.0.0.1                  #Check you can reach GW
iPXE> ping 192.0.2.0                 #check you can reach to your server running tftp or http or
https
iPXE> boot http://192.0.2.0/<directory-path>540l-x64.iso    #Copy the image on the http/https/tftp
server in any path and then point to download the image from there.
```

Note To rectify errors while typing the command, use **Ctrl+H** keys to delete a character.

If a PXE server is configured to run a DHCP server, it assigns an IP address to the Ethernet Management interface of the router. This provides a channel to download the image that is required to re-image a router in case of a boot failure.

```
Router#reload bootmedia network location all
Proceed with reload? [confirm]
```

Note Use the **force** option to perform an ungraceful reload of the specified location or hardware module. When **force** option is used along with the **all** location, the chassis undergoes an ungraceful reload. Use the **noprompt** option to avoid the prompt to confirm the operation. The **force** option is not recommended, and should not be used during regular operations.

Boot the Cisco NCS 540 Series Router Using USB Drive

Boot the router using USB drive if the router fails to boot when powered ON. An alternate method is to Boot the Cisco NCS 540 Series Router Using Manual iPXE.

Before you begin

Have access to a USB drive with a storage capacity that is between 8GB (min) and 32 GB (max). USB 2.0 and USB 3.0 are supported.

Caution We recommend that you do not use Kingston USB 3.0 memory cards with 64GB storage capacity as this might cause a hardware error.

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

Step 1 Copy the bootable file to a USB disk.

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 If you are unable to boot from a USB drive, remove and insert the drive again. If the drive is inserted correctly, and still fails to read from the 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.

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. To check if the disk is formatted as FAT32, right click on the USB disk, and view the properties.
b) Copy the compressed boot file in .zip format from the image file to the USB drive. This .zip file can be downloaded from the Cisco Software Download center.
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 contents of the compressed boot file by unzipping it inside the USB drive. This converts the USB drive to a bootable drive.

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

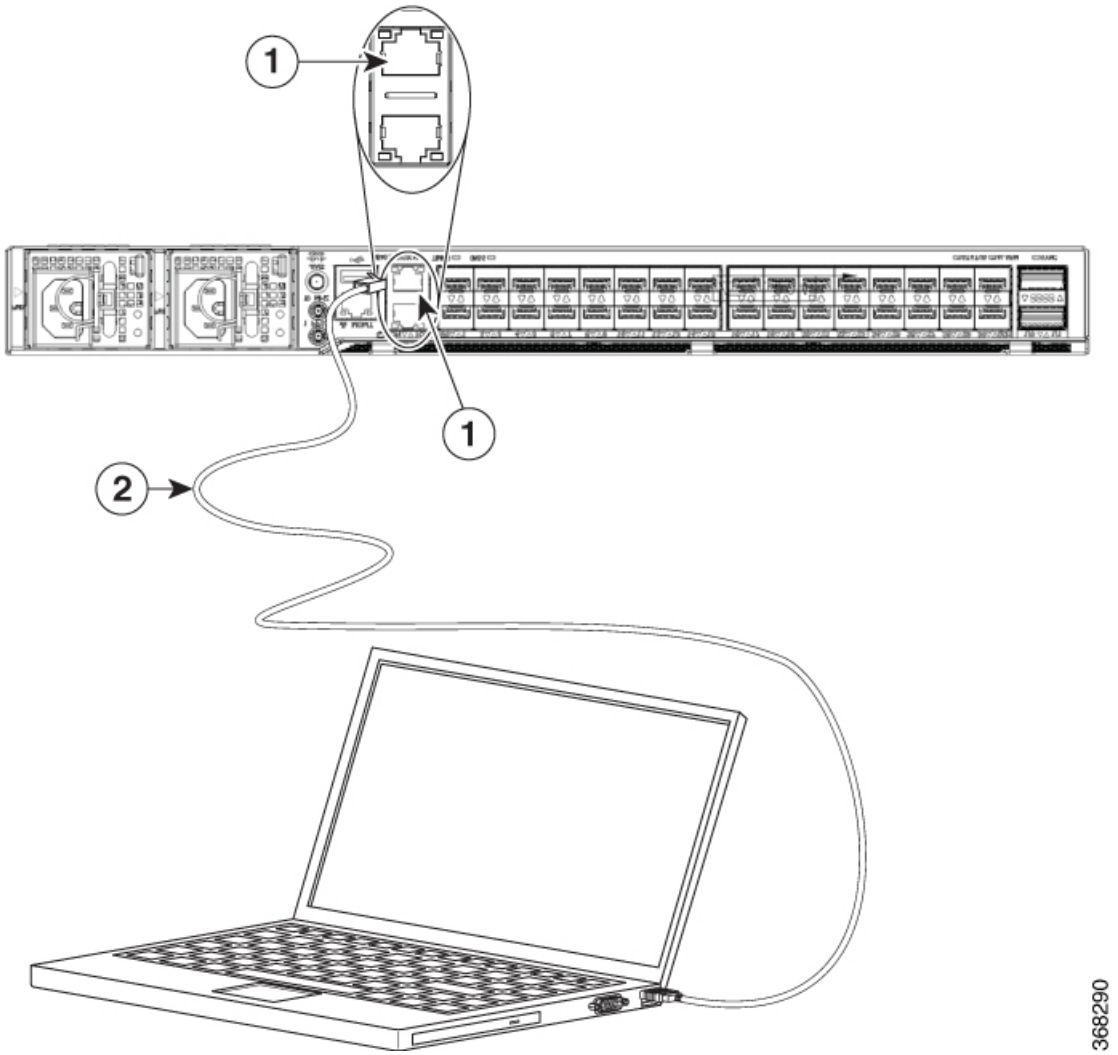
e) Eject the USB drive from your local machine.

Step 2 Use the bootable USB drive to boot the router or upgrade its image using one of the following methods:

Note Insert the USB drive in the USB port of the ACTIVE RP.

- **Boot menu**

Figure 6: Connecting the USB Console Cable to the Route Processor



1	RJ45 Port	2	USB Type-A console cable

a. Insert the USB drive, and connect to the console.

b. Power ON the router.

c. Press Esc or Del to pause the boot process, and get the RP to the BIOS menu.

d. Select `Boot Manager`, and then select the `USB` option from the boot menu.

```
Cisco BIOS Setup Utility - Copyright (C) 2019 Cisco Systems, Inc

Boot Override
UEFI: Micron_M600_MTFDDAT064MBF, Partition 4
UEFI: Built-in iPXE
URFI: Built-in Shell
URFI: Built-in Grub
UEFI: USB Flash Memory1.00, Partition 1
```

The system boots the image from the USB drive, and installs the image onto the hard disk. The router boots from the hard disk after installation.

- **XR CLI**

  Use this method if you can access the XR prompt.

  a. Insert the USB device in the active RP.

  b. Access the XR prompt and run the command:

```
Router#reload bootmedia usb noprompt

Welcome to GRUB!!
Verifying (hd0,msdos1)/EFI/BOOT/grub.cfg...
(hd0,msdos1)/EFI/BOOT/grub.cfg verified using Pkcs7 signature.
Loading Kernel..
Verifying (loop)/boot/bzImage...
(loop)/boot/bzImage verified using attached signature.
Loading initrd..
Verifying (loop)/boot/initrd.img
```

  Use the **force** option to perform an ungraceful reload of the specified location or hardware module. When **force** option is used along with the **all** location, the chassis undergoes an ungraceful reload. Use the **noprompt** option to avoid the prompt to confirm the operation. The **force** option is not recommended, and should not be used during regular operations.

  The system boots the image from the USB and installs the image onto the hard disk. The router boots from the hard disk after installation.

Note Execute the `install commit` command before proceeding to the next install iteration, while performing cyclic upgrade and downgrade tests.

Configure the Management Port on the Cisco NCS 540 Series Router

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.

Note We recommend that you use a Virtual Private Network (VPN) routing and the forwarding (VRF) on the Management Ethernet interface.

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 the management network.

Step 1 Configure a VRF.

Example:

```
Router#conf t
Router(config)#vrf <vrf-name>
Router(config-vrf)#exit
```

Step 2 Enter interface configuration mode for the management interface of the RP.

Example:

```
Router(config)#interface mgmtEth 0/RP0/CPU0/0
```

Step 3 Assign an IP address and a subnet mask to the interface.

Example:

```
Router(config-if)#ipv4 address 10.10.10.1/8
```

Step 4 Configure the Management Ethernet interface under the VRF.

Example:

```
Router(config-if)#vrf <vrf-name>
```

Step 5 Exit the management interface configuration mode.

Example:

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

Step 6 Assign a virtual IP address and a subnet mask to the interface. The virtual address is primarily used for out-of-band management over the Management Ethernet interface.

Example:

```
Router(config)#ipv4 virtual address vrf <vrf-name> 10.10.10.1/8
```

Step 7 Place the interface in `UP` state.

Example:

```
Router(config)#no shutdown
```

Step 8 Specify the IP address of the default-gateway to configure a static route; this is used for communications with devices on other networks.

Example:

```
Router(config)#router static vrf <vrf-name> address-family ipv4 unicast 0.0.0.0/0 10.10.10.1
```

Step 9 Commit the configuration.

Example:

```
Router(config)#commit
```

Step 10 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.

Synchronize Router Clock with NTP Server

Synchronize the XR clock with that of an NTP server to avoid a deviation from true time.

NTP uses the concept of a `stratum` to describe how many NTP hops away a machine is from an authoritative time source. A `stratum 1` time server typically has an authoritative time source (such as a radio or atomic clock, or a GPS time source) directly attached to the server. A `stratum 2` time server receives its time through NTP from a `stratum 1` time server, and so on.

Note The Cisco implementation of NTP does not support stratum 1 service.

Before you begin

Configure and connect to the management port.

Step 1 Enter the XR configuration mode.

Example:

```
Router#configure
```

Step 2 Synchronize the console clock with the specified sever.

Example:

```
Router(config)#ntp server <NTP-source-IP-address>
```

The NTP source IP address can either be an IPv4 or an IPv6 address. For example:

IPv4:

```
Router(config)#ntp server 192.0.2.0
```

IPv6:

```
Router(config)#ntp server 2001:DB8::1
```

Note The NTP server can also be reachable through a VRF if the Management Ethernet interface is in a VRF.

Step 3 Commit the configuration.

Example:

```
Router(config-ntp)#commit
```

Step 4 Verify that the clock is synchronised with the NTP server.

Example:

```
Router#show ntp status
Clock is synchronized, stratum 3, reference is 192.0.2.0
nominal freq is 1000000000.0000 Hz, actual freq is 1000000000.0000 Hz, precision is 2**24
reference time is E12B1B02.8BB13A2F (08:42:42.545 UTC Tue Sep 17 2019)
clock offset is -3.194 msec, root delay is 4.949 msec
root dispersion is 105.85 msec, peer dispersion is 2.84 msec
loopfilter state is 'FREQ' (Drift being measured), drift is 0.0000000000 s/s
system poll interval is 64, last update was 124 sec ago
authenticate is disabled
```

Perform Preliminary Checks with Cisco NCS 540 Series Router

After successfully logging into the console, you must perform some preliminary checks to verify the correctness of the default setup. Correct any issues that arise before proceeding with further configurations.

Verify Software Version on Cisco NCS 540 Series Router

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. Installing the newer version of the software provides the latest feature set on the router.

You can view the overview of the running software. This includes the following information:

- Image name and version
- User who built the image
- Time the image was built
- Build workspace
- Build host
- ISO label

Note If any modifications are made to the running software on the booted ISO, only the IOS XR version is displayed in the label field and not the label included in the ISO.

- Copyright information
- Hardware information

Display the version of the Cisco IOS XR software, and its various software components that are installed on the router.

```
Router#show version
Cisco IOS XR Software, Version 7.0.1 LNT
Copyright (c) 2013-2019 by Cisco Systems, Inc.

Build Information:
 Built By     : xyz
 Built On     : Sat Jun 29 22:45:27 2019
 Build Host   : iox-lnx-064
 Workspace    : ../7.0.1/NCS540L/ws/
 Version      : 7.0.1
 Label        : 7.0.1

cisco NCS540L
System uptime is 41 minutes
```

Verify Status of Hardware Modules on Cisco NCS 540 Series Router

Hardware modules such as RPs, LCs, fan trays, and power modules are installed on the router. The firmware on various hardware components of the router must be compatible with the Cisco IOS XR image installed.

Incompatibility may cause the router to malfunction. Verify that all hardware and firmware modules are installed correctly and are operational.

Before you begin

Ensure that all required hardware modules are installed on the router.

Step 1 View the status of the system.

Example:

```
Router#show platform
Node            Type                         State            Config state
--------------------------------------------------------------------------
0/RP0/CPU0      N540X-16Z4G8Q2C-A(Active)  IOS XR RUN        NSHUT
0/FT0           N540-X-BB-FAN              OPERATIONAL       NSHUT
```

Step 2 View the list of hardware and firmware modules detected on the router.

Example:

```
Router#show hw-module fpd
                                                                 FPD Versions
                                                                 ================
Location   Card type              HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/RP0/CPU0 N540-28Z4C-SYS-A       0.1   IoFpga               CURRENT    1.29    1.29
0/RP0/CPU0 N540-28Z4C-SYS-A       0.1   IoFpgaGolden      B  CURRENT            1.29
0/RP0/CPU0 N540-28Z4C-SYS-A       0.1   Primary-BIOS      S  CURRENT    1.09    1.09
0/RP0/CPU0 N540-28Z4C-SYS-A       0.1   StdbyFpga         S  CURRENT    0.29    0.29
0/RP0/CPU0 N540-28Z4C-SYS-A       0.1   StdbyFpgaGolden  BS  NEED UPGD           0.00
0/RP0/CPU0 N540-28Z4C-SYS-A       0.1   TamFw             S  NEED UPGD  4.09    2.04
0/RP0/CPU0 N540-28Z4C-SYS-A       0.1   TamFwGolden      BS  NEED UPGD           0.00
```

```
Router#show hw-module fpd
Fri May 28 13:53:23.325 UTC
Auto-upgrade:Disabled
Attribute codes: B golden, P protect, S secure
                               FPD Versions
                               ================
Location Card type             HWver FPD device ATR Status Running Programd Reload Loc
-------------------------------------------------------------------------------------------
0/RP0/CPU0 N540X-6Z18G-SYS-A   0.2   IoFpga     CURRENT     0.13      0.13   0/RP0
0/RP0/CPU0 N540X-6Z18G-SYS-A   0.2   IoFpgaGolden B         NEED UPGD 0.00   0/RP0
0/RP0/CPU0 N540X-6Z18G-SYS-A   0.2   Prim-BootLoader CURRENT 10.07   10.07   0/RP0
0/RP0/CPU0 N540X-6Z18G-SYS-A   0.2   StdbyFpga S CURRENT    0.28      0.28   0/RP0
0/RP0/CPU0 N540X-6Z18G-SYS-A   0.2   StdbyFpgaGolden BS     NEED UPGD 0.25   0/RP0
0/RP0/CPU0 N540X-6Z18G-SYS-A   0.2   TamFw S    CURRENT     6.05      6.05   0/RP0
0/RP0/CPU0 N540X-6Z18G-SYS-A   0.2   TamFwGolden BS         CURRENT   6.05   0/RP0
```

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

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

- FPD Device—Name of the hardware component, such as IO FPGA, IM FPGA, or BIOS

  Note Golden FPDs are not field upgradable.

- Status—Upgrade status of the firmware. The different states are:

Status	Description
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. We recommend that you to perform an upgrade of the firmware version.
RLOAD REQ	The upgrade is complete, and the ISO image requires a reload.
UPGD DONE	The firmware upgrade is successful.
UPGD FAIL	The firmware upgrade has failed.
UPGD PREP	The FPD firmware is preparing for upgrade.
BACK IMG	The firmware is corrupt. Reinstall the firmware.
UPGD SKIP	The upgrade is 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
- Programd—Version of the FPD programmed on the module

Step 3 If necessary, upgrade the required firmware.

Example:

```
Router#upgrade hw-module location all fpd all
```

Alarms are created showing all modules that needs to be upgraded.

```
Active Alarms
------------------------------------------------------------------------------------------------------------------
Location      Severity     Group        Set Time                    Description
------------------------------------------------------------------------------------------------------------------

0/6/CPU0       Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/10/CPU0      Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/RP0/CPU0     Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/RP1/CPU0     Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/FC0          Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
0/FC1          Major       FPD_Infra    09/16/2019 12:34:59 UTC     One Or More FPDs Need Upgrade Or
 Not In Current State
```

Note BIOS and IOFPGA upgrades require a power cycle of the router for the new version to take effect.

Step 4 After the modules are upgraded verify the status of the modules.

Example:

```
Router#show hw-module fpd
                                                                          FPD Versions
                                                                          ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   IoFpga               CURRENT    1.29    1.29
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   IoFpgaGolden      B  CURRENT            1.29
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   Primary-BIOS      S  CURRENT    1.09    1.09
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   StdbyFpga         S  CURRENT    0.29    0.29
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   StdbyFpgaGolden  BS  RLOAD REQ          0.01
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   TamFw             S  RLOAD REQ   2.04   2.05
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   TamFwGolden      BS  RLOAD REQ          0.01
```

The status of the upgraded nodes show that a reload is required.

Step 5 Reload the individual nodes that required an upgrade.

Example:

```
Router#reload location <node-location>
```

Step 6 Verify that all nodes that required an upgrade show an updated status of `CURRENT` with an updated FPD version.

Example:

```
Router#show hw-module fpd
                                                                          FPD Versions
                                                                          ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   IoFpga               CURRENT    1.29    1.29
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   IoFpgaGolden      B  CURRENT            1.29
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   Primary-BIOS      S  CURRENT    1.09    1.09
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   StdbyFpga         S  CURRENT    0.29    0.29
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   StdbyFpgaGolden  BS  CURRENT            0.01
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   TamFw             S  CURRENT    2.05    2.05
0/RP0/CPU0 N540-28Z4C-SYS-A      0.1   TamFwGolden      BS  CURRENT            0.01
```

Verify Interface Status on the Cisco NCS 540 Series Router

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.

View the interfaces discovered by the system.

Example:

```
Router#show ipv4 interfaces brief
Interface                      IP-Address      Status          Protocol Vrf-Name
-------------------------------------------------------------------------------HundredGigE0/0/0/0
             unassigned      Shutdown        Down     default
HundredGigE0/0/0/1             unassigned      Shutdown        Down     default
HundredGigE0/0/0/2             unassigned      Shutdown        Down     default
HundredGigE0/0/0/3             unassigned      Shutdown        Down     default
HundredGigE0/0/0/4             unassigned      Shutdown        Down     default
HundredGigE0/0/0/5             unassigned      Shutdown        Down     default
HundredGigE0/0/0/6             unassigned      Shutdown        Down     default
```

```
HundredGigE0/0/0/7             unassigned      Shutdown        Down     default
------------------------ <snip> ---------------------------------TenGigE0/0/0/18/0
unassigned      Up              Up       default
TenGigE0/0/0/18/1              unassigned      Up              Up       default
TenGigE0/0/0/18/2              unassigned      Up              Up       default
TenGigE0/0/0/18/3              unassigned      Up              Up       default
MgmtEth0/RP0/CPU0/0            10.10.10.1      Up              Up       default
```

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, and that the interfaces are created according to the type of interface modules displayed in **show platform** command.

Verify Node Status on Cisco NCS 540 Series Router

Each card on the router represents a node.

Verify the operational status of the node.

Example:

```
Router#show platform
Node            Type                          State            Config state
--------------------------------------------------------------------------------
0/RP0/CPU0      N540X-16Z4G8Q2C-A(Active)  IOS XR RUN        NSHUT
0/FT0           N540-X-BB-FAN              OPERATIONAL       NSHUT
```

Displays the status of nodes present in the chassis.

Verify that the software state of all RPs, LCs, and the hardware state of FCs, FTs, and power modules are listed, and their state is `OPERATIONAL`. This indicates that the XR console is operational on the cards.

The platform states are described in the following table:

Card Type	State	Description
All	UNKNOWN	Error – Internal card record is not available
All	IDLE	Error – Card state is not initialized
All	DISCOVERED	Card is detected
All	POWERED_ON	Card is powered on
RP, LC	BIOS_READY	Card BIOS is up
RP, LC	IMAGE_INSTALLING	Image is being downloaded or installed
RP, LC	BOOTING	Image is installed and the software is booting up
RP, LC	IOS_XR_RUN	Software is operating normally and is functional
RP, LC	IOS_XR_INITIALIZING	Software is initializing

Card Type	State	Description
FC, FT, PT, PM	OPERATIONAL	Card is operating normally and is functional
RP, LC, FC	RESET	Card is undergoing reset
RP, LC	REIMAGE	Card is pending reimage
RP, LC, FC	SHUTTING_DOWN	Card is shutting down as a result of a fault condition, user action or configuration
RP, LC, FC	SHUT_DOWN	Card is shutdown due to a fault condition, user action or configuration
FC	ONLINE	RP is able to access this remote card
LC	DATA_PATH_POWERED_ON	Forwarding complex is powered ON
RP (Active)	SHUTTING_REMOTE_CARDS	Active RP card is in the process of shutting down other cards as part of a chassis reset
RP (Standby), LC, FC	WAITING_FOR_CHASSIS_RESET	Card is shutdown and is waiting for the chassis to be reset
RP, LC	WDOG_STAGE1_TIMEOUT	Card CPU failed to reset the hardware watchdog
RP, LC	WDOG_STAGE2_TIMEOUT	Hardware watchdog has timed out waiting for the card CPU to reset itself
RP, LC, FC	FPD_UPGRADE	One or more FPD upgrades are in progress
FC	CARD_ACCESS_DOWN	RP is unable to access this remote card

Create Users and Assign Privileges on the Cisco NCS 540 Series Router

Users are authenticated using a username and a password. The authentication, authorization, and accounting (AAA) commands help with these services:

- create users, groups, command rules, or data rules
- change the disaster-recovery password

XR has its AAA separate from Linux. XR AAA is the primary AAA system. A user created through XR can log in directly to the EXEC prompt when connected to the router. A user created through Linux can connect to the router, but arrive at the bash prompt. The user must log in to XR explicitly in order to access the XR EXEC prompt.

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. A user can have full read-write access to 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. To gain an understanding about AAA, and to explore the AAA services, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 540 Series Routers*.

Create a User Profile

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

In this task, you create a user, `user1`, password for this user, `pw123`, and assign the user to a group `root-lr`.

Step 1 Enter the XR configuration mode.

Example:

```
Router#config
```

Step 2 Create a new user.

Example:

```
Router(config)#username user1
```

Step 3 Create a password for the new user.

Example:

```
Router(config-un)#password pw123
```

Step 4 Assign the user to group `root-lr`.

Example:

```
Router(config-un)#group root-lr
```

All users have `read` privileges. However, users can be assigned to `root-lr` usergroup. These users inherit the `write` privileges where users can create configurations, create new users, and so on.

Step 5 Commit the configuration.

Example:

```
Router(config-un)#commit
```

What to do next

With the router set up, you can manage your system, install software packages, and configure your network.

Create a User Group

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

The router supports a maximum of 32 user groups.

In this task, you create a group name, `group1`, and assign a user, `user1` to this group.

Before you begin

Create a user profile. See Create a User Profile, on page 87.

Step 1 Enter the XR configuration mode.

Example:

```
Router#config
```

Step 2 Create a new user group, `group1`.

Example:

```
Router#(config)#group group1
```

Step 3 Specify the name of the user, `user1` to assign to this user group.

Example:

```
Router#(config-GRP)#username user1
```

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

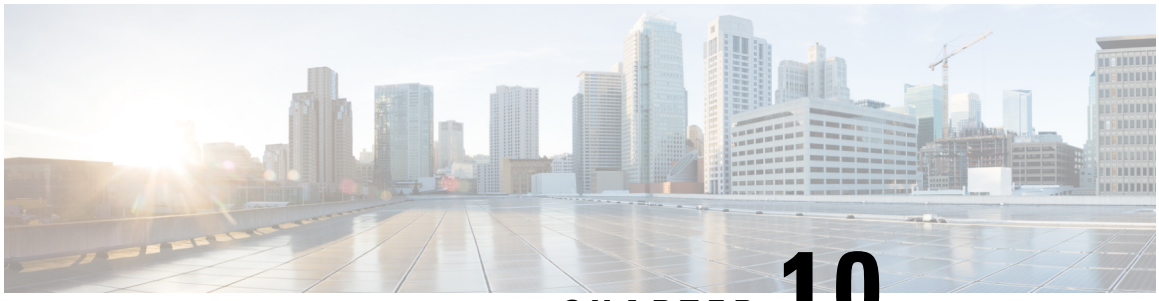
Step 4 Commit the configuration.

Example:

```
Router#commit
```

What to do next

With the router set up, you can manage your system, install software packages, and configure your network.



CHAPTER 10

Install XR7 OS on NCS 540 Series Routers

This section describes the concepts and procedures for upgrading or downgrading your system, installing optional packages, and obtaining bug fixes for the Cisco NCS 540 series routers.

Cisco NCS 540 series routers use the XR7 framework. This framework refers to a set of architectural enhancements to the Cisco IOS XR software around the capabilities of modularity, simplified platform infrastructure, and programmability at various software layers.

The Cisco IOS XR software is composed of a base image (ISO) that provides the XR infrastructure, and a TAR file. The TAR file is made up of a set of packages (also called RPMs). These packages comprise mandatory and optional RPMs that can be deployed based on specific requirements. This software modularity approach provides a flexible consumption model that allows you to install a subset of IOS XR packages on devices based on your individual requirements. All critical components are modularized as packages so that you can select the features that you want to run on your router. For example, components like CDP and Telnet are modularized as packages and separated from the base image. These packages can be individually installed, upgraded or removed based on your requirements.

XR7 install is Dandified Yum- or DNF-based software package manager that is used to install, update, and remove packages on the RPM-based Linux distributions. The package manager is used to automatically compute dependencies and determine the actions required to install packages.

Note For information on how to download the system upgrade procedures document, see the *About Cisco IOS XR Software Upgrade and Downgrade Guide*.

The Cisco NCS 540 router variants that support XR7 in Cisco IOS XR Release 7.0.1 are:

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

Supported Packages

The base ISO image is contained within a `.tar` file. Additional optional packages (RPMs) are provided as modular software deliverables to align with diverse use cases and their deployments across the network.

Note You can create a golden ISO (GISO) with optional packages and bug fixes based on your requirement. Contact Cisco Support to build a GISO.

The software deliverables include:

- ISO image containing the base install image - `ncs540l-x64-7.0.1.iso`
- Tar file containing optional RPMs - `NCS540l-iosxr-7.0.1.tar`
- ZIP file for USB boot - `ncs540l-usb_boot-7.0.1.zip`

The software deliverables can be downloaded from Cisco Software Download center.

Optional Package	Included in ISO by Default
ncs540l-netflow	Yes
ncs540l-mcast	Yes
BGP	Yes
CDP	No
EIGRP	No
IPSLA	Yes
IS-IS	Yes
LLDP	Yes
MCAST	Yes
MPLS-OAM	Yes
Netflow	Yes
OSPF	Yes
Perfmgmt	Yes
RIP	No
Telnet	No

Optional Package	Included in ISO by Default
Track	Yes

Note The telnet package is not part of the ISO image. You must manually install the telnet optional package to use telnet for client or server. This applies to all packages that are not part of the ISO image.

SSH is part of the ISO image.

Install operation over IPv6 is not supported.

Software Deliverables and Terminologies

This section provides an understanding of the terms that are associated with installing the software.

- **Package:** The primary mechanism for changing the install image on a system. A package, also known as an RPM, contains the software and metadata. A package is in `.rpm` format. A package can be mandatory or optional. Mandatory packages are part of the install image and cannot be removed. Optional packages are not required for the software to work, but can be installed to provide additional functionalities, and can be installed or removed based on requirement.
- **ISO image:** A bootable image that contains the installable files of the base operating system (OS). The image contains the IOS XR (XR7) infrastructure for fixed and distributed platforms in the form of base ISO image, mandatory RPMs. An ISO image is in `.iso` format.
- **Golden ISO (GISO):** A customizable ISO image that is built to contain preferable packages to suit diverse installation requirements. GISO can be customized to include a standard base image with the basic functional components, additional RPMs, bug fixes, and configuration files based on your requirement. GISO can also include a custom image version. From IOS XR Release 7.5.x and later, you can build your GISO image without support from Cisco by using the Build a Golden ISO feature.
- **Source:** A location where packages can be installed from. The source can be a repository, local directory or a local tar file.
- **Repository:** A directory of RPMs and their metadata that a package manager uses to query the packages.
- **Active package:** A package whose software is currently running on the system.
- **Committed package:** A package that is committed and remains active following a system reload.
- **Atomic Change:** Every packaging operation is contained within an atomic change. Atomic changes may contain multiple packaging operations. During an atomic change, any changes to install IOS XR software will not be visible to the system. To make the changes visible to the system, the atomic change must be applied.
- **Top-level package:** Each block of software has a top-level package and various partition-level packages. The top-level package can be installed or upgraded directly, whereas the partition-level packages cannot be changed directly. The partition-level packages are installed or upgraded automatically as dependencies of the top-level package. The top-level package has the name format `xr-<feature>-<release>.x86_64.rpm`, whereas the dependent partition-level packages have the longer name format containing information about the partition. You can also use the standard RPM commands

to check the summary or description metadata of the package, which will identify whether it is a top-level or a partition-level package.

- **Package manager:** An entity that handles the semantics to resolve dependencies in packaging operations.
- **Packaging operations:** The actions performed to change the packages that are installed on the system. The semantics are inherited from the underlying package manager. Examples of packaging operations are upgrade, downgrade, replace, add, or remove packages.
- **Synchronous action:** Synchronous action requests are supported for install actions using CLI command. Specify `synchronous` keyword in the install commands, and the prompt will only be returned when either the request has completed, `Ctrl + C` keys are pressed or a reload occurs. Pressing `Ctrl + C` keys during a synchronous action request will return the prompt to the user but will not halt the install operation. During the synchronous action request, the user is updated with the status of the request whenever it changes.
- **Transaction:** All atomic changes occur within a transaction. If the system reloads during an install transaction, the running software will be reverted to its previous state before the transaction was started. To maintain the software changes carried out during a transaction, you must commit the transaction.
- A complete install operation to modify the system's software requires three phases:
  - Packaging operation
  - **Apply:** This is required to complete an atomic change and make the software change visible to the system.
  - **Commit:** This is required to end a transaction and ensure that all software changes will still be present on router reload.

Note If you perform a manual or automatic system reload without completing the transaction with the **install commit** command, the action will revert the system to the point before the install transaction commenced, including any configuration changes. Only the log is preserved for debugging.

Note In a multinode system, any node reloads that occur during a transaction that are not initiated as part of the install 'apply by reload' phase can result in the reloaded node being in BOOT HOLD state. The node continues to be in the BOOT HOLD state until the transaction is either committed or cancelled.

Workflow for Installing Cisco IOS XR Software

The router is shipped with a pre-installed version of the Cisco IOS XR (XR7) software. When the router is powered ON for the first time, the pre-installed software starts functioning automatically. You configure the router for network capabilities. When a new version of the software is available, you can upgrade the system using these tasks:

Note For instructions to upgrade image-specific software, navigate to the CCO Software Download portal, select the product and refer to the `ncs540-x64-<version>.docs.tar` file for the release.

Obtain Data Models for Install Operation

You can use YANG data models to install and upgrade XR7 software. The data models are packaged with the release image in the `/pkg/yang` directory.

The models are in the `.yang` format. Each data model can be identified as one of the following functionalities:

- `-oper` in the model name indicates an operational model. For example, `Cisco-IOS-XR-install-oper.yang` and `Cisco-IOS-XR-install-augmented-oper.yang` are operational models for the install operation.
- `-cfg` indicates a configuration model. For example, `Cisco-IOS-XR-install-cfg.yang` is a configuration model for the install operation.
- `-act` indicates an action model. For example, `Cisco-IOS-XR-install-augmented-act.yang` and `Cisco-IOS-XR-install-act.yang` are action models for the install operation.

Step 1 View the install-related data models on the router. You can also access the supported data models to install Cisco IOS XR software from the Github repository.

Example:

```
node0_RP0_CPU0:/pkg/yang]$ls -ltr *install*
-rw-r--r--. 1 root root  8646 Jul  2 01:59 Cisco-IOS-XR-install-act.yang
-rw-r--r--. 1 root root  7267 Jul  2 01:59 Cisco-IOS-XR-install-search-act.yang
-rw-r--r--. 1 root root 10664 Jul  2 01:59 Cisco-IOS-XR-install-augmented-act.yang
-rw-r--r--. 1 root root  2511 Jul  2 02:00 Cisco-IOS-XR-um-install-cfg.yang
-rw-r--r--. 1 root root  2270 Jul  2 02:04 Cisco-IOS-XR-install-cfg.yang
-rw-r--r--. 1 root root  6222 Jul  2 02:04 Cisco-IOS-XR-install-oper.yang
-rw-r--r--. 1 root root 14009 Jul  2 02:04 Cisco-IOS-XR-install-augmented-oper.yang
-rw-r--r--. 1 root root 13726 Jul  2 02:04 Cisco-IOS-XR-install-oper-sub1.yang
-rw-r--r--. 1 root root  2440 Jul  2 02:04 Cisco-IOS-XR-install-augmented-oper-sub2.yang
-rw-r--r--. 1 root root 59866 Jul  2 02:04 Cisco-IOS-XR-install-augmented-oper-sub1.yang
```

The following table describes the function of the install-related data models:

Data Model	Description
Cisco-IOS-XR-install-oper	Operational data model to view details that are related to basic package information, active and committed packages, and fixes
Cisco-IOS-XR-install-cfg	Configuration data model to specify the location of the install source
Cisco-IOS-XR-install-act	Action model to perform basic install operations and software upgrade
Cisco-IOS-XR-install-search-act	Action model that contains a collection of YANG definitions for install actions related to searching for package information

Data Model	Description
Cisco-IOS-XR-install-augmented-oper	Augmented operational model that displays information about packaging, atomic changes, and history of the install operation on the router
Cisco-IOS-XR-install-augmented-act	Action model to perform flexible install operations, including controlling the exact timing of system reloads and rolling back to a previous commit
Cisco-IOS-XR-shellutil-copy-act	Action model to copy files on the router from a source location

Step 2 Use a manageability agent like NETCONF or gRPC to connect and communicate with the router. You can send Remote Procedure Calls (RPC) requests to configure or retrieve operational data from the router. The router processes the request and responds to the request through an RPC response. You use the RPCs to send requests to install the software by populating the relevant container and leaf in the data model.

For more information about understanding the data model structure and using data models, see the *Programmability Configuration Guide for Cisco NCS 540 Series Routers*.

Create Repository to Access Files for Installing IOS XR Software

Note If only Golden ISO (GISO) is used, you do not need to create a repository.

To install packages (RPM), code upgrades, and updates in XR7, you need a repository of RPMs for the router to download the RPMs for installation. The repository can be local to the router, or accessed remotely through FTP, HTTP, or HTTPS.

Important The repository must be created specific to each platform and release. Do not create repositories with a mix of platforms and releases.

When the repository is accessed remotely, you must provide a repository URL from where the install files are fetched. The URL contains:

- IP address of the server
- Port number of the server
- (Optional) Virtual Routing and Forwarding (VRF) name

The repository can be configured to be reachable using a non-default VRF table. If the repository is reachable through an address in a VRF, specify the name of the VRF.

The format of the repository URL is one of the following:

- FTP: `ftp://<server>[;<vrf>]/<path-to-repository>`

- HTTP: `http://<server>[;<vrf>]/<path-to-repository>`
- HTTPS: `https://<server>[;<vrf>]/<path-to-repository>`
- Local: `file:///<path-to-repository>`. The path to the repository must be under /harddisk:/ location.

For example, the URL for HTTP server is http://172.16.0.0:3333/.

Note Username and password are not supported for HTTP and FTP repositories.

Create and Configure a Local Repository

The router can serve as repository to host the RPMs. You must be a `root-lr` user with access to the router shell. Remote repository is the recommended method to access the RPMs. However, if remote repository is not your preferred option, then you can use the router as a repository to host the RPMs.

Using a local repository removes the need to setup an external server for software installation. In this method, the image files are copied directly to the router, and used to create a repository locally. However, on the downside, the files for future updates must be copied to each router individually.

This section provides the procedure for setting up a local RPM repository on the router.

Step 1 Create a directory locally on the router's `/harddisk:`. Copy the required RPMs and ISO files (using copy or scp command) from the server to the local directory on the router.

Step 2 Access the shell of the router using `run` command and untar the RPMs.

Example:

```
Router#run
[node:~]$cd <directory-with-rpms>
[node:~]$tar -xvzf <rpm-name>.tgz
```

Step 3 Exit from the shell.

Step 4 Configure the local repository.

Example:

```
Router#config
Router(config)#install repository local-repo url file:///harddisk:/<directory-with-rpms>
Router(config)#commit
<data and time stamp> UTC: config[67543]: Configuration committed by user.
Router(config)#end
```

where, `local-repo` is the repository name, `file:///harddisk:/<directory-with-rpms>` is the local repository URL.

Step 5 Check the contents of the repository.

Example:

```
Router#show install available
Trying to access repositories...
Package               Architecture          Version          Repository
--------------------  ---------------  ------------------ ---------------

xr-ncs540l-core       x86_64        7.0.1v1.0.1-1      local-repo

xr-core               x86_64        7.0.1v1.0.1-1      local-repo
```

Note Only the top-level packages are displayed. The contents of the repository is displayed only when the configured repository is valid and the RPMs are present in the repository. It displays only the packages that are available in the repository and not part of active system.

Create and Configure an External Repository

To create an external repository, use a server that can be reached over HTTP, HTTPS or FTP. The following instructions are applicable to Linux distribution systems.

Using an external repository provides a central common repository to be used across devices. This eliminates the need to copy files for future updates to each router individually. It also serves as a single source when new RPMs (bug fixes, packages, updates) are made available. This is the recommended method to setup a repository.

Note For release 7.0.1, 7.0.2, the external repository is available only through the Management Ethernet interface.

Before you begin

Ensure that you have completed the following tasks:

- Set up your HTTP, HTTPS or FTP server. Ensure that the server is reachable as specified in the note above.
- Install `createrepo` utility on the Linux distribution system (if not installed already).

Step 1 Create a directory on the server and copy all the RPMs to a directory. This directory hosts the repository and must be accessible to the HTTP, HTTPS or FTP server that the router will use to access the repository. For example, `/var/www/html`, is the directory where the repository will be created.

If the RPM files are archived (.tar format) or compressed (.tgz or .gz format), extract the files. The files hierarchically arrange in sub directories under the main directory that is used as a repository.

Step 2 Convert the directory to a repository using `createrepo` utility on the Linux server. This creates a directory named `repodata` with the metadata of all the RPMs.

Example:

```
[node]$createrepo --database /var/www/html/
Saving Primary metadata
Saving file lists metadata
Saving other metadata
Generating sqlite DBs
Sqlite DBs complete

[node]$cd /var/www/html/
[node]$ls
repodata
```

If you add new packages to the repository, change or remove packages from the repository, you must run `createrepo` command again to update the metadata. This ensures that the package manager chooses the correct packages.

Step 3 Configure the external repository.

Example:

```
Router#config
Router(config)#install repository remote-repo url http://10.194.88.104/<directory-with-rpms>
Router(config)#commit
<data and time stamp> UTC: config[67542]: Configuration committed by user 'cisco'.
Router(config)#end
```

For FTP, the repository is configured as follows:

```
Router#config
Router(config)#install repository remote-repo url ftp://10.194.88.104/<directory-with-rpms>
Router(config)#commit
<data and time stamp> UTC: config[67543]: Configuration committed by user 'cisco'.
Router(config)#end
```

where, `remote-repo` is the repository name, `http://10.194.88.104/<directory-with-rpms>` is the HTTP repository URL, and `ftp://10.194.88.104/<directory-with-rpms>` is the FTP repository URL.

Step 4 Verify connectivity to the server, and check the contents of the repository.

Example:

```
Router#show install available
Trying to access repositories...
Package                Architecture          Version          Repository
--------------------  ---------------  ------------------ ---------------

xr-ncs540l-core       x86_64        7.0.1v1.0.1-1      remote-repo

xr-core               x86_64        7.0.1v1.0.1-1      remote-repo
```

Note Only the top-level packages are displayed. The contents of the repository are displayed only when the configured repository is valid and the RPMs with the updated metadata are present in the repository. It displays only the packages that are available in the repository and not part of active system.

Upgrade the Current Active Version of Cisco IOS XR Software

This section shows replacing the current software version with `.iso` image. The instructions in this section also apply to system downgrade.

Upgrade the Current Active Version

In this scenario, you replace the current software with image, apply the changes, and commit the install operation. Committing the changes indicates the end of the current transaction. The updated software is used after the changes are applied, before the install transaction is committed.

A reboot is not always necessary. Bug fixes can be applied using a GISO that contains the current running software and the additional bugfix. These fixes may not require a reboot. Reboots are required for a system version change, if too many processes need restarting, there is configuration in the GISO to apply or if the bugfix is marked as requiring a reload.

From Cisco IOS XR Release 7.5.1, you can use the Automatic Install of Bridging Bug Fix RPMs feature to install any bridging bug fix RPMs that are prerequisite for a system upgrade or a downgrade.

You need to add the required Bridging Bug Fix RPMs into the customized ISO built using Cisco Golden ISO (GISO) build script **gisobuild.py**, by going through the steps in Build a Golden ISO, on page 106. Ensure that you add the required bridging bug fix RPMs into your Golden ISO. The GISO can include bridging Bug Fix

RPMs for multiple releases, and installs only the specific bridging Bug Fix RPMs required for the target release. The bridging bug fix RPMs can be used in the following scenarios:

- To resolve a bug that might stop upgrade.
- The latest version has new prerequisite requirements that are not met by the earlier version.

The **install replace** command adds and applies the highest version of any bridging bugfix RPMs for the currently active XR version.

Step 1 Copy the ISO (or GISO) image to the `/harddisk:` location on the router.

Step 2 Upgrade the system to replace the current software with the .iso image.

Example:

```
Router#install package replace /harddisk:/ncs540l-x64-x.x.x.iso
```

Step 3 Activate the new .iso image on the router by applying the changes.

Example:

```
Router#install apply {reload | restart} [noprompt]
```

Note You can use a single command to perform both the packaging operation and activating the applying the changes using **install replace /harddisk:/ncs540l-x64-x.x.x.iso noprompt** command.

To identify whether a reload is required or only process restart is needed, use either **show install history last transaction verbose** command or **show install request** command.

Include the keyword `noprompt` in the command to enable the system to bypass your permission to reload the router.

Applying the change gives you the flexibility to test the operation of the new software before committing the changes. If you reload the router, the router reverts the software to its previous software state.

All operations that automatically apply the new software are prohibited when an atomic change is already in progress. You must address the current atomic-change before performing this operation. To address the change, apply the current atomic-change, or cancel it with the **install package abort all-since-apply** command.

Step 4 View the install log.

Example:

```
Router#show install log detail
Fri Nov 12 09:43:49.702 UTC
2021-11-12 09:33:47 UTC    Transaction 1 started
2021-11-12 09:33:47 UTC    Atomic change 1.1 started
2021-11-12 09:33:47 UTC    Packaging operation 1.1.1 started
2021-11-12 09:33:47 UTC    Replace


2021-11-12 09:35:58 UTC    Packaging operation 1.1.1 success
2021-11-12 09:36:04 UTC    Apply by reload started
2021-11-12 09:38:48 UTC    Atomic change 1.1 successfully applied by reload
```

Step 5 Verify that the image is activated successfully.

Example:

```
Router#show install request
```

Step 6 Commit the transaction.

Example:

```
Router#install commit
```

Note Any action requests may be run synchronously from the CLI. During this request, you are updated with the status of the request whenever it changes. The following example shows the output from a synchronous action request:

```
Router#install commit synchronous
Starting:
  install commit
Transaction 1
The install operation will continue in the background
Press Ctrl-C to return to the exec prompt. This will not cancel the install operation

Current activity: Initializing ....
Current activity: Commit transaction ......

Transaction 4: 'install commit' completed without error
```

Upgrade the System and Install RPMs

In this scenario, you replace the current software with the `.iso` image and have the possibility to install or remove optional RPMs before applying the changes. You can perform this operation while an atomic-change is already in progress. However, all packaging operations before this command are discarded. The installed software is an exact copy of the software in the ISO after this packaging operation is complete. You can perform all additional packaging operations after this operation and before applying and committing the changes.

Step 1 Copy the ISO (or GISO) image to the `/harddisk:` directory on the router.

Step 2 Upgrade the system to replace the current software with the .iso image.

Example:

```
Router#install package replace /harddisk:/ncs540l-x64-x-x-x.iso
```

Step 3 Install other RPMs (packages) after the system upgrade operation.

a) Configure a repository on the router. For instructions to create a local or a remote repository, see Create Repository to Access Files for Installing IOS XR Software, on page 94.

b) Check the available packages in the repository.

Example:

```
Router#show install available
```

c) Install the RPMs.

Example:

```
Router#install package add <pkg1> <pkg2> <pkgn>
```

Step 4 Check the status of install operation.

Example:

```
Router#show install request

User request: install package add xr-bgp
```

```
State: In progress since <date and timestamp>

Current activity: Package add or other package operation
Next activity: Await user input
Time started: <date and timestamp>
Timeout in: 35m 8s
Locations responded: 0/1

Location    Packaging operation stage  Notification Phase Clients responded
----------  ------------------------- ------------------- ------------------
0/RP0/CPU0   Package operations         None in progress    N/A
```

Note The operation ID is a unique ID for each user request. This ID is constructed from the transaction ID, atomic change ID and packaging operation ID that was already used in the commands. For example, if the request is `install commit`, the operation ID is the transaction ID. If the request includes applying an atomic change but not committing the transaction (for example, `install replace /harddisk:/ncs540_x64.iso`), the operation ID is the atomic change ID. An operation ID of 4.2 indicates a second atomic change in the fourth transaction.

This operation ID is also returned in the action RPC. If an error occurs while the request is initiated, an empty string is returned instead of an operation ID.

When the `State` changes to `Success`, activate the new image.

```
Router#show install request
Wed Sep 14 02:53:21.525 PDT

User request: install package abort latest
Operation ID: 2.1.2
State:        Failure since 2022-09-14 02:48:15 UTC-07:00
Disk space check failed on nodes: 0/0/CPU0. Query 'show install history id 2.1.2 errors' for more
details and next steps

Current activity:    Await user input
Time started:        2022-09-14 02:48:20 UTC-07:00

The following actions are available:
    install package add
    install package remove
    install package upgrade
    install package downgrade
    install package abort latest
    install package abort all-since-apply
    install apply restart
    install apply reload
    install reimage
```

Note The **install apply restart** method has the least impact.

Step 5 Activate the new .iso image or RPM on the router by applying the changes.

Example:

```
Router#install apply {reload | restart} [noprompt]
```

To identify whether a reload is required or only process restart is needed, use either **show install history last transaction verbose** command or **show install request** command.

Include the keyword `noprompt` in the command to enable the system to bypass your permission to reload the router.

Step 6 Verify the image and packages that are activated as part of `install package add` operation is activated successfully.

Example:

```
Router#show install request
```

Step 7 Commit the transaction.

Example:

```
Router#install commit
```

To perform the same step using data models, use the `install-package-replace` RPC on the Cisco-IOS-XR-install-augmented-act data model.

```
<install-replace>
   <file>iso-name</file>
   <source-type>local</source-type>
   <source>directory-containing-iso</source>
   <commit>true</commit>
</install-replace>
```

Upgrade QDD Optical Modules Through CLI

The QDD optics firmware file needs to be copied to the router manually. Contact Cisco Support to check the QDD firmware version, IOS XR release compatibility, and to obtain the QDD optics firmware file.

Limitation: When ports share a common management interface, IOS XR serializes the firmware upgrade. Serializing and deserializing may delay the upgrade process.

Step 1 From the router, copy the QDD firmware file to the hard disk using the following command:

Example: `scp user@10.1.1.1:/home/user/filename harddisk:/`

- When you are using VRF, use the following sample command:

```
scp user@10.1.1.1:/home/user/cl1.bin vrf MGMT harddisk:/

Tue Jan 25 02:57:22.762 UTC
Connecting to 10.1.1.1...
Password:
  Transferred 1484800 Bytes
  1484800 bytes copied in 0 sec (22161194)bytes/sec

RP/0/RP0/CPU0:8808#dir harddisk:/cl1.bin
Tue Jan 25 03:00:47.835 UTC

Directory of harddisk:/cl1.bin
35 -rw-r--r--. 1 1484800 Jan 25 02:57 dp04qsdd_dp04sfp8_161_10_01.ackit

53461500 kbytes total (42983204 kbytes free)
```

- When you are not using VRF, remove the `vrf MGMT` command:

```
scp user@10.1.1.1:/home/user/cl1.bin harddisk:/
```

Step 2 Run the following commands to upgrade the FPD for QDD optical modules:

Multiport upgrade:`upgrade optics port 0,1,2,3,4 filename /harddisk:/cl1.bin location 0/1/CPU0`

Single port upgrade: `upgrade optics port 0 filename /harddisk:/cl1.bin location 0/1/CPU0`

You can check the firmware upgrade progress using the following command: `show optics firmware upgrade port 0,1,1,2,3,4 location 0/1/CPU0`

Install Optional Packages to Provide Additional Functionality

You can install one or more packages (RPM) that are not already present on the system. The packages are not mandatory for the software to function, but provide additional functionality. Based on your requirement, you can install or remove these optional packages. The source file can be a repository name, repository url, local filepath, or path to a tar file.

You must specify only the top-level package name that you want to install. The associated dependencies of this package, in the form of card and partition-specific packages, are included automatically. By default, the latest available version of each package is installed. You can also explicitly install a specific version of a package.

Note All Cisco IOS XR images are signed to ensure the authenticity of the software.

This example shows the options to install the optional package `xr-telnet-7.0.1v1.0.1-1.x86_64.rpm`.

Before you begin

If you are installing the packages from a local directory, ensure that the TAR file `ncs540l-iosxr-7.0.1.tar` is copied to the `harddisk:/` on the router. If you are installing the packages from an RPM repository, ensure you have configured the repository. For more information, see Create Repository to Access Files for Installing IOS XR Software, on page 94.

Step 1 Install one or more optional packages using one of the following options:

- **Option 1:** Install the package from the local directory:

```
Router# install source /harddisk:/files xr-telnet-7.0.1
v1.0.1-1.x86_64.rpm
```

Note The `install source` command automatically applies the changes. Use this command to install optional packages. To upgrade existing packages, see Upgrade the System to Obtain Bug Fixes, on page 107.

- **Option 2:** Install the package from a configured remote repository:

```
Router#install source install-repo xr-telnet
```

Here, `install-repo` is the name of the repository. For repository configuration, see Create Repository to Access Files for Installing IOS XR Software, on page 94.

- **Option 3:** Install the package from a repository URL:

```
Router#install source http://72.16.0.0:3333/remote-repo xr-telnet
```

- **Option 4:** Add the package and apply the change. The package must be available in the repository.

```
Router#install package add xr-telnet-7.0.1v1.0.1-1.x86_64.rpm
Router#install apply {restart | reload}
```

More than one package can be installed using a single packaging operation. Use the following command:

```
Router#install source <path-to-source> <package 1> <package 2> … <package n>
```

For example,

```
Router#install source /harddisk:/files xr-telnet-7.0.1v1.0.0-1.x86_64.rpm
xr-mcast-7.0.1v1.0.0-1.x86_64.rpm
```

To perform this task using data models, use the `install` RPC on the Cisco-IOS-XR-install-act data model. Here is an example with an HTTP repository:

```
<install>
   <packages>
     <packagename>pkg1</packagename>
     <packagename>pkg2</packagename>
     …
     <packagename>pkgn</packagename>
   </packages>
   <source-type>http</source-type>
   <source><path-to-source></source>
</install>
```

Step 2 Commit the operation.

Example:

```
Router#install commit
```

Step 3 Check the status of install operation.

Example:

Delete Optional Packages

You can remove optional packages that you no longer require. An optional package is not mandatory for the operating system to function, and based on your requirement, it can be installed or removed.

Step 1 Remove the optional package.

Example:

```
Router#install package remove <optional-package-name>
```

Step 2 Apply the changes to make the change active.

Example:

```
Router#install apply [reload | restart]
```

Attention To identify whether to reload or restart the system after applying the changes, use either **show install history last transaction verbose** command or **show install request** command.

Step 3 Commit the changes to make the change persistent after a reload operation.

Example:

```
Router#install commit
```

Additional Install Operations

After you upgrade your system, based on your requirement, you can perform additional install operations:

View the Version of Installed Packages

The router is shipped with a pre-installed operating system. You can view the version of the installed software and the active packages. If you have upgraded your system, installed additional packages or bug fixes, you can view the version of the committed packages.

Review the software version information:

- Package name and version
- User who built the package
- Time the package was built
- Build workspace
- Build host
- ISO label:
  - Label is present if GISO boots using PXE boot
  - Label is present if GISO is installed using the `install replace` method
  - Label reverts to default (only release version) if there is any change since the time the image with the label was installed.
  - Label is nullified and reverts to default if an RPM is added or removed on top of an existing GISO.
  - Label is repopulated if an RPM from the GISO is added or removed and a rollback operation is performed.
- Copyright information
- Hardware information

Step 1 View the version of the Cisco IOS XR software, and its various software components that are installed on the router.

Example:

The following example shows the version information for a non-GISO image:

```
Router#show version
Cisco IOS XR Software, Version 7.0.1 LNT
Copyright (c) 2013-2019 by Cisco Systems, Inc.

Build Information:
 Built By     : xyz
 Built On     : Sat Jun 29 22:45:27 2019
 Build Host   : iox-lnx-064
 Workspace    : ../7.0.1
                7.3.1/
                NCS540L/ws/
```

```
 Version      : 7.0.1
 Label        : 7.0.1

cisco NCS540L
System uptime is 41 minutes
```

The following example shows the version information for a GISO image. The customer label is appended to the `Label` field in the GISO image:

```
Router#show version
Cisco IOS XR Software, Version 7.0.1 LNT
Copyright (c) 2013-2019 by Cisco Systems, Inc.

Build Information:
 Built By     : xyz
 Built On     : Sat Jun 29 22:45:27 2019
 Build Host   : iox-lnx-064
 Workspace    : ../7.0.1
                /NCS540L/ws/
 Version      : 7.0.1
 Label        : 7.0.1-CUSTOMER_LABEL

cisco NCS540L
System uptime is 41 minutes
```

You can also use the `get` RPC on the `install.version` data model.

Step 2 View the active packages.

Example:

```
Router#show install active [summary]
Active Packages:    XR: 112    All: 1088
Label:              7.0.1

Optional Packages                          Version
--------------------------           ----------------------
xr-ncs540l-mcast                         7.0.1v1.0.0-1
xr-ncs540l-netflow                       7.0.1v1.0.0-1
xr-bgp                                   7.0.1v1.0.0-1
xr-ipsla                                 7.0.1v1.0.0-1
xr-is-is                                 7.0.1v1.0.0-1
xr-lldp                                  7.0.1v1.0.0-1
xr-mcast                                 7.0.1v1.0.0-1
xr-mpls-oam                              7.0.1v1.0.0-1
xr-netflow                               7.0.1v1.0.0-1
xr-ospf                                  7.0.1v1.0.0-1
xr-perfmgmt                              7.0.1v1.0.0-1
xr-track                                 7.0.1v1.0.0-1
```

You can also use the `get` RPC on the `install.packages.active.node` and the `install.packages.active.node.summary` data models.

To understand the data model structure and its arguments, see the Obtain Data Models for Install Operation, on page 93 topic.

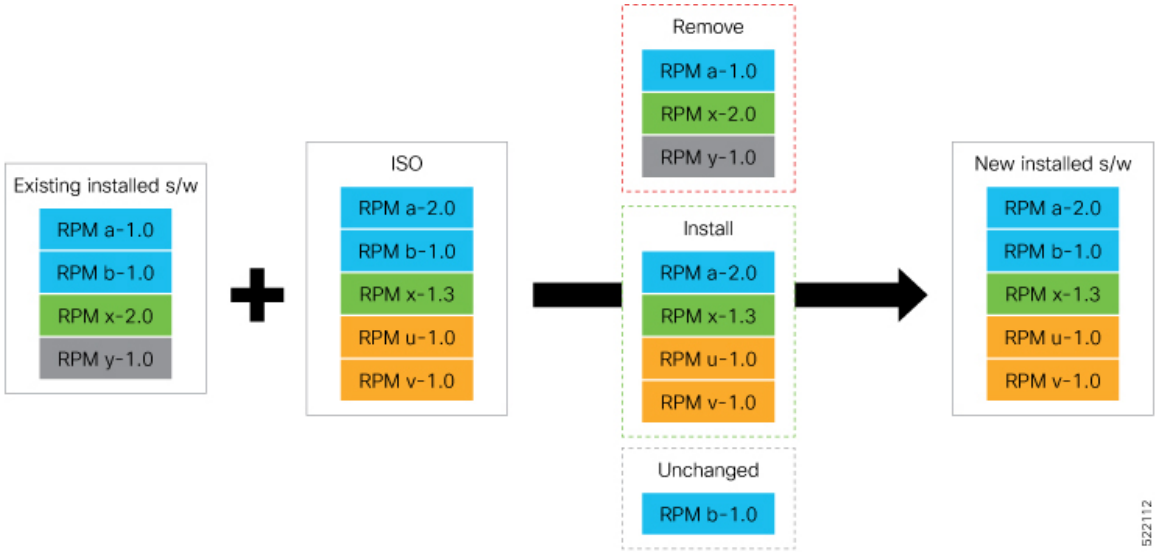
Build a Golden ISO

Golden ISO (ISO) upgrades the router to a version that has a predefined set of RPMs with a single operation. For example, you can create a customized ISO with the base OS package and specific optional RPMs based on your network requirements.

GISO supports automatic dependency management, and provides these functionalities:

- Builds RPM database of all the packages present in package repository.
- Skips and removes Cisco RPMs that do not match the base ISO version.
- Skips and removes third-party RPMs that are not part of already existing third-party base package in the base ISO.

Note Install operation over IPv6 is not supported.



Step 1 Contact Cisco Support to build the GISO image with the set of packages based on your requirement.

Step 2 Copy the GISO image to the `/harddisk:` location on the router.

Step 3 Upgrade the system to replace the current software with the <*platform-architecture*>.iso image, and install the RPMs.

Example:

```
Router#install replace <source location> <giso name.iso>
```

Step 4 View the version information for the GISO image. You can include a label to indicate the runing software version on the router. For example, create a label v1 for the current GISO version. When you rebuild GISO with additional RPMs, you can create a label v2 to distinguish the builds.

Example:

```
Router#show version
Cisco IOS XR Software, Version 7.0.1 LNT
Copyright (c) 2013-2019 by Cisco Systems, Inc.
```

```
Build Information:
 Built By     : xyz
 Built On     : Sat Jun 29 22:45:27 2019
 Build Host   : iox-lnx-064
 Workspace    : ../7.0.1
                /NCS540L/ws/
 Version      : 7.0.1
 Label        : 7.0.1-CUSTOMER_LABEL

cisco NCS540L
System uptime is 41 minutes
```

Upgrade the System to Obtain Bug Fixes

You can upgrade the system to obtain all available bug fixes or choose specific bug fix using bug ID.

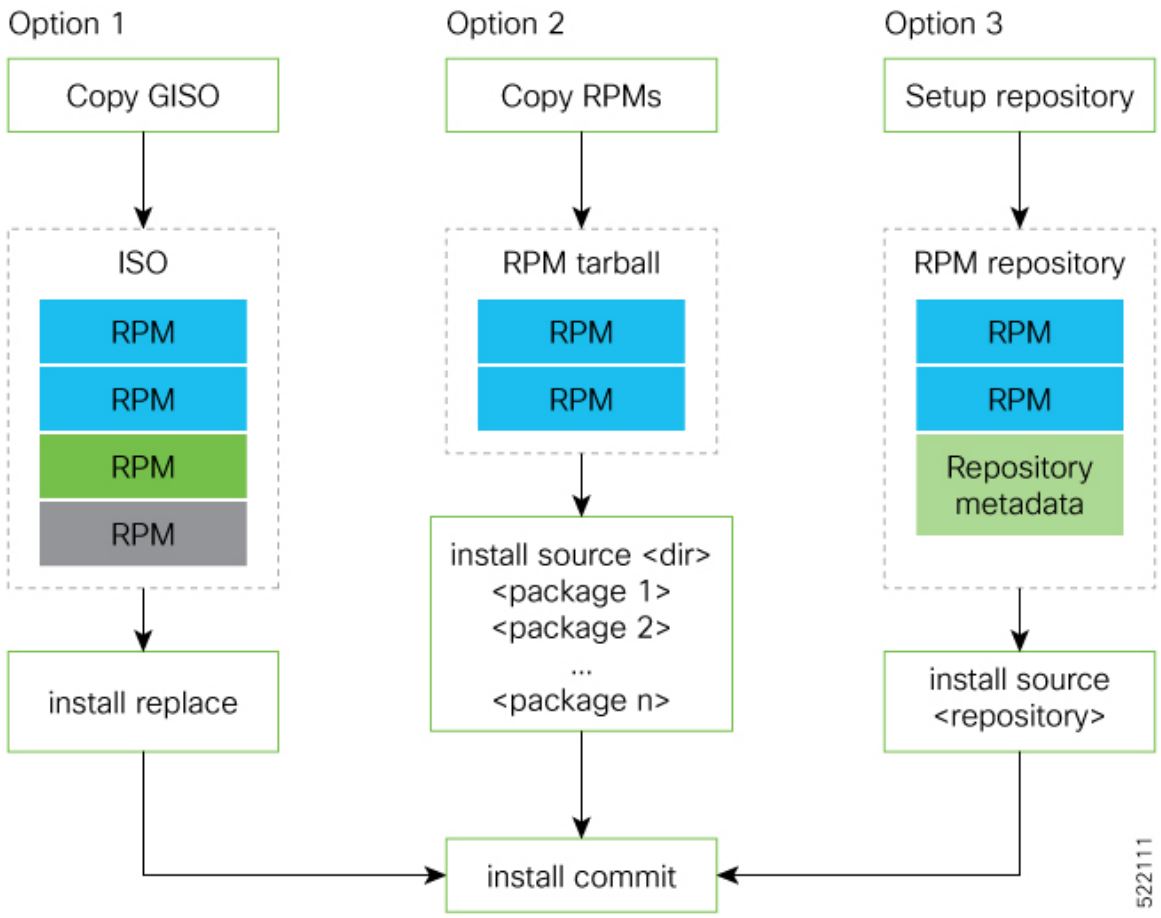
Bug fixes are available as optional RPMs. The bug fixes replace packages in the base ISO without adding up to the image size. For example, even if you add 20 RPMs to the GISO, the GISO file size will remain the same as the initial ISO.

You can download the bug fix RPMs from the Cisco Software Download portal .

From this page, download the latest bug fix RPMs as tarballs to the install repository. Untar the tarball into RPMs.

The `README` file provides the relevant information about the bug fix and also identifies the dependencies, if any, where other bug fix RPMs may be required for a complete fix.

The following image shows the options to install the bug fix RPMs.



The software is split into modular blocks and the package manager infrastructure computes the dependencies between the blocks. Each block of software has a top-level package and various partition-level packages. Bug fixes that span multiple blocks may lead to creating multiple dependent packages that are built as part of earlier bug fixes.

Note We recommend that you leverage the GISO workflow. Contact Cisco Support to build a new GISO with the required bug fixes. The RPMs are present in the initrd, which is the initial RAM disk for the boot loader, and this requires that the package is signed by Cisco. You can install GISO using a single `install replace` operation. For more information about GISO, see the *Build a Golden GISO* section.

However, if you do not prefer using the GISO, here are a few alternative ways to install bug fixes:

- Create tarballs to install one or more bug fixes. For example, if you are installing bug fixes CSCxx11111, CSCyy22222 and CSCzz33333, you can use the individual tarball files and create a single tarball file.
- Use a Dandified Yum- or DNF repository to install, update, or remove relevant bug fixes. See, Create Repository to Access Files for Installing IOS XR Software, on page 94.

Note Use the RPM repository to harvest the benefits of package manager. The package manager queries the available packages, and downloads only those packages and their dependencies that are needed for installation.

Step 1 View the list of available bug fixes.

Example:

```
Router#show install fixes available
Bug Id             Packages                      Repository
-----------    ----------------------------  ----------------
CSCxx12345     xr-540l-core-7.0.1v1.0.1-1      <repository-name>

               xr-core-7.0.1v1.0.1-1           <repository-name>
```

Step 2 Install the bug fix or package using one of the following options:

- Install the package where the bug fix is applied.

  ```
  Router#install package upgrade xr-540l-core-7.0.1v1.0.1-1 xr-core-7.0.1v1.0.1-1
  Packaging operation 1.1.1 started - xr-540l-core-7.0.1v1.0.1-1 xr-core-7.0.1v1.0.1-1
  ```

  This task can also be accomplished using Cisco-IOS-XR-install-augmented-oper data model.

  Apply the changes.

  ```
  Router#install apply [reload | restart]
  ```

  Note To identify if you must reload or restart the system while applying the changes, use one of these two methods:

  - History of last transaction

    ```
    Router#show install history last transaction verbose
    2019-09-11 17:01:46 UTC    Transaction 3 started
    2019-09-11 17:01:46 UTC      Atomic change 3.1 started
    2019-09-11 17:01:46 UTC      Packaging operation 3.1.1 started
    2019-09-11 17:16:46 UTC    Transaction 3 complete

    Least impactful apply method: process restart
    ```

    The command also displays the information about the changes to files and processes because of the install operation, and the package operations carried out on each node.

  - Show install request

    Here, both `install apply restart` and `install apply reload` options are available. In this case, use `install apply restart` command because the impact on the system is the least. But when only an `install apply reload` option is available, then reload is the only option to apply the change.

- Install the optional package. Changes are applied automatically.

  Attention Automatic change may trigger a reload of the router depending on the package that is installed.

  ```
  Router#install source /harddisk:/files xr-540l-core-7.0.1v1.0.1-1.x86_64.rpm
  ```

  Note Packages can also be installed using the package name.

  ```
  Router#install source /harddisk:/files  xr-540l-core
  ```

- This task can also be performed using YANG data models. Use `install` RPC on the Cisco-IOS-XR-install-act data model. Here is an example usage with an HTTP repository:

```
<install>
   <packages>
     <packagename>pkg1</packagename>
   </packages>
   <source-type>http</source-type>
   <source><path-to-source></source>
</install>
```

Step 3 View the state of the packaging operation.

Example:

```
Router#show install request
User request: install package upgrade xr-<platform>-core-<version> xr-core-<version>
Operation ID: 2.1.2
State:        In progress since

Current activity:    Initiate operation
Next activity:       Begin transaction
Time started:        2019-06-25 07:41:06

No per-location information.
```

Step 4 View the log to ensure that the installation is successful.

Example:

```
Router#show install log
2019-06-25 07:41:06 UTC    Transaction 1 started
2019-06-25 07:45:08 UTC    Upgrade (Success)
2019-06-25 07:45:08 UTC    xr-<platform>-core-<version>
2019-06-25 07:45:08 UTC    xr-core-<version>
2019-06-25 07:57:02 UTC    Atomic change 1.1 successfully applied by reload
```

Step 5 View the history of the install operation.

Example:

```
Router#show install history table
  Transaction             Atomic Change           Packaging Operations
--------------------  --------------------------  ----------------------------------
Id   Status           Id  Method   Status      Id  Operation   Inputs Status
--------------------  --------------------------  ----------------------------------
 1   In progress      1   Reload   Success      1   Upgrade        1  Success
```

The command can also be used to view more details if there is a failed operation.

Use **show install history id <operation-id>** command to filter the history of install information by ID. IDs are of the form `<transaction id>.<atomic id>.<packaging id>`.

```
Router#show install history id ?
  WORD Specify an operation ID (e.g. 1, 1.2, 1.2.3)
```

Use **show install history last** command to view the last packaging operation, atomic change, or transaction.

```
Router#show install history last ?
     atomic-change  Show the last atomic change
     package        Show the last packaging operation
     transaction    Show the last transaction
```

Step 6 After the operation is complete, verify that the packages `xr-540l-core-7.0.1v1.0.1-1` and `xr-core-7.0.1v1.0.1-1` are installed and active.

Example:

```
Router#show install active summary
xr-ncs540l-bfd                                          7.0.1v1.0.0-1
xr-ncs540l-bmc                                          7.0.1v1.0.0-1
xr-ncs540l-bundles                                      7.0.1v1.0.0-1
xr-ncs540l-card-support                                 7.0.1v1.0.0-1
xr-ncs540l-core                                         7.0.1v1.0.1-1
xr-ncs540l-x64-core                                     7.0.1v1.0.1-1
xr-core                                                 7.0.1v1.0.1-1
xr-core-calv                                            7.0.1v1.0.0-1
xr-host-core                                            7.0.1v1.0.0-1
xr-ip-core                                              7.0.1v1.0.0-1
xr-spi-core                                             7.0.1v1.0.0-1
```

Example:

Example:

```
Router#show install active summary
```

The version has changed. The version `1.0.1-1` indicates that the bug fix is installed.

This task can also be accomplished using data models. Use the `get` RPC for `install.fixes.active` operation using Cisco-IOS-XR-install-augmented-oper data model.

Step 7 Commit the changes for the changes to persist after a reload operation.

Example:

```
Router#install commit
```

Step 8 View the list of bug IDs for which fixes are committed.

Example:

```
Router#show install fixes committed
```

This task can also be accomplished using data models. Use the `get` RPC for `install.fixes.committed` operation using Cisco-IOS-XR-install-augmented-oper data model.

Step 9 View the list of active bug fix RPMs.

Example:

```
Router#show install fixes active
```

This task can also be accomplished using data models. Use the `get` RPC for `install.fixes.active` operation using Cisco-IOS-XR-install-augmented-oper data model.

Downgrade to a Previously Installed Package

You can downgrade a package to a previously installed version. By default, the subsequent previous version (version previous to the current version) is installed. Also, you can downgrade the software to a specific version of interest. To remove a bug fix RPM from the installed packages, downgrade the package to a version where the fix was not applied.

Note While downgrading, you can choose any previous version, including the base version of the RPM. However, when downgrading a bug fix RPMs, ensure that you also consider all dependencies of the current version.

Bug fix RPM is an upgrade to the existing package. The action of removing a bug fix RPM either removes the entire feature, or fails if the package is mandatory.

Before you begin

Ensure you have access to the previously installed package and its source.

Step 1 Downgrade the package using one of the following options:

- Downgrade the package where the fix was applied. When multiple older versions of the package are present in the configured repositories, the immediate previous version of the package is installed. Use caution when using this command as the current version of the package is removed completely.

  ```
  Router#install package downgrade xr-telnet
  ```

  Apply the changes.

  ```
  Router#install apply [reload | restart]
  ```

  Attention To identify whether to reload the router or restart the affected processes as part of the apply operation, use either **show install history last transaction verbose** command or **show install request** command.

- Install a specific earlier version of the optional package. The changes are applied automatically.

  Attention An automatic change may trigger a reload of the router depending on the package being downgraded.

  ```
  Router#install source <path-to-source> xr-telnet-7.0.1v1.0.0
  ```

- Use `install` RPC on the Cisco-IOS-XR-install-act data model. Here is an example usage with a local repository:

  ```
  <install>
   <packages>
     <packagename>xr-telnet-7.0.1v1.0.0


  </packagename>
   </packages>
     <source>file://<path-to-source>/</source>
  </install>
  ```

  The package version `xr-telnet-7.0.1v1.0.1` is downgraded to `xr-telnet-7.0.1v1.0.0`.

Step 2 Commit the operation.

Example:

```
Router#install commit
```

Roll Back Software to a Previously Saved Installation Point

You can roll your system software back to a previous version. This could be used to discard an ongoing install operation, or to undo an install operation that has already been committed. After each commit operation, the system saves a record of the committed software packages. Each record is a restoration point, and is assigned a unique ID. This ID is known as a transaction ID. You can use the transaction ID to roll back the software to a restoration point associated with this ID. Up to 900MB of space is allowed for rollback points, instead of a specific number of rollback points.

Note

- Use transaction ID 0 to roll back to the software that was present after the system booted for the first time.
- If you commit an install transaction using **install commit** command, the GISO ZTP configuration is saved along with the rest of the software changes. This means that if you use the **install rollback** or **install package rollback** command to revert the software to the state of a previous transaction, the GISO ZTP configuration is also reverted to its previous state. To undo this install operation, as well as the change in GISO ZTP configuration, use **install package abort** command. If there is no GISO ZTP configuration saved at the end of the install transaction, the existing GISO ZTP configuration is reverted to the previous state when the rollback operation of that transaction is applied.

Step 1 View the list of available transaction IDs.

Example:

```
Router# show install rollback list-ids
```

Step 2 Explore the main packages that can be installed if you roll the software back to the specific transaction ID.

Example:

```
Router# show install rollback id <id>
```

Step 3 View the relative changes that are made to the currently installed software if it is rolled back to a transaction ID.

Example:

```
Router# show install rollback id <id> changes
```

To perform these tasks using data models, use the `get` RPC on the Cisco-IOS-XR-install-augmented-oper data model.

```
<rpc>
  <get>
   <filter type="subtree">
      <install xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-install-augmented-oper">
      <rollback/>
     </install>
   </filter>
  </get>
</rpc>
```

Step 4 Roll back to the software associated with the specific transaction ID.

Example:

```
Router# install rollback <id> [commit]
```

If you want to apply the change and roll back to the associated transaction ID, commit the change. You can also include the keyword `noprompt` in the command to enable the system to bypass your permission to reload the router.

Attention This roll back operation installs the previous software and also applies the change automatically. This may reload the router depending on the package that is rolled back.

Alternatively, use the **install package rollback** command to only roll back the package but not apply the changes. You can check whether the router will reload or restart if you apply the change using the **show install history last transaction verbose** command or **show install request** command. Based on the command output, you can take the appropriate action using **install apply reload | restart** command to either reload or restart the system. Use the **install commit** command to commit the transaction.

To perform this task using data models, use the `install-rollback` RPC on the Cisco-IOS-XR-install-augmented-oper data model.

```
<rpc>
 <install-rollback xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-install-augmented-act">
  <commit>true</commit>
   <transaction-id>0</transaction-id>
 </install-rollback>
</rpc>
```

To understand the data model structure and its arguments, see the Access the Install-Related Data Model.

Step 5 Commit the operation.

Example:

```
Router#install commit
```