System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers, IOS XR Release 7.3.x

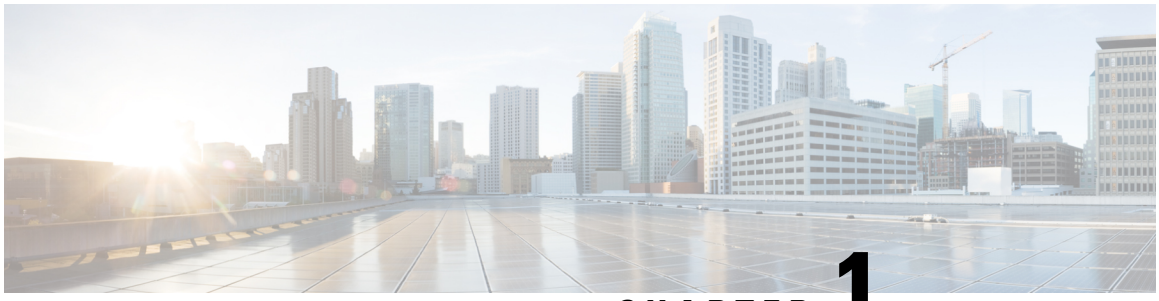
First Published: 2021-10-01

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

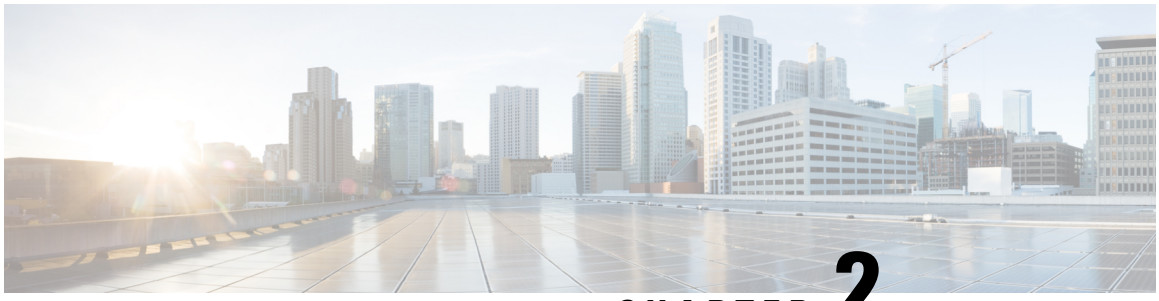
New and Changed Feature Information

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

New and Changed System Setup Features

Feature	Description	Changed in Release	Where Documented
Recover System Using Console Port	With this feature, you can recover access to your router if you lose your admin and root credentials, without having to reimage using iPXE orUSB boot. Recovery involves a router reload, and the user data is securely erased before the router reloads.	Release 7.3.3	Create User Profiles and Assign Privileges, on page 21
Secure Zero Touch Provisioning with Removable Storage Device	With this release, you can securely and seamlessly provision network devices using USB.	Release 7.3.2	Secure ZTP with Removable Storage Device, on page 100
Conforming to US DOD Login Banner Standards	With this release, you can enable a login banner that conforms to the standards of the US DOD login banner.	Release 7.3.1	Create a User Profile in XR VM, on page 26

Feature	Description	Changed in Release	Where Documented
Zero Touch Provisioning with USB	With this release, you can use a removable storage device, (such as a USB drive) containing the raw boot image file thereby enabling the removable storage device to be a self-sufficient bootstrapping solution.	Release 7.3.1	Fresh Boot Using Removable Storage Device, on page 73
Secure Zero Touch Provisioning	With this release, you can securely and seamlessly provision thousands of network devices accurately with out manual intervention.	Release 7.3.1	Securely Provision Your Network Devices, on page 91



CHAPTER 2

Cisco NCS 5500 Product Overview

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

Cisco NCS 5500 system provides:

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

Note The Cisco Network Convergence System (NCS) 5700 Series builds on the Cisco NCS 5500 fixed systems by combining the forwarding ASIC design with the Cisco IOS XR7 OS. The Cisco NCS 5700 series includes the following variants:

- NCS-57B1-6D24
- NCS-57B1-5DSE

These variants of the NCS 5700 series run on the Cisco IOS XR7 operating system. For information about setting up the routers, see Setup Cisco NCS 5700 Series Routers with XR7 OS, on page 121. For information about installing the XR7 OS on NCS 5700 series, see Install XR7 OS on NCS 5700 Series Routers, on page 135.

- Command Modes, on page 3

Command Modes

The router runs on virtualized Cisco IOS XR software. Therefore, the CLI commands must be executed on virtual machines, namely the XR LXC and the System Admin LXC.

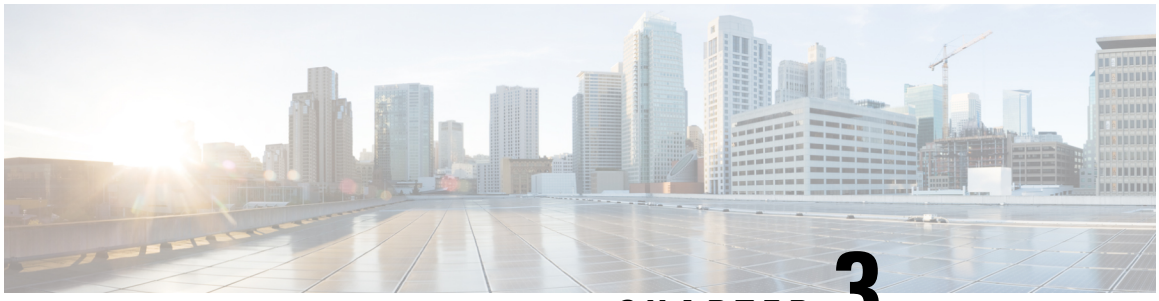
The command modes are applicable for the Cisco NCS 5500 Series Routers. This table lists the command modes for the LXCs.

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

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

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

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



CHAPTER 3

Bring-up the Router

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

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

In a large-scale environment, to provision routers remotely without any manually intervention, we recommend you to use Zero Touch Provisioning (ZTP) mechanism. ZTP offers the following implementation choices worth considering in advance:

- You can use Classic Zero Touch Provisioning, when you want to provision the devices within a secured network. See Provision Network Devices using Zero Touch Provisioning, on page 71.
- You can use Secure ZTP when you must securely provision remote network devices, transverse through public internet for provisioning, or when the devices are from third-party manufacturers. See Securely Provision Your Network Devices, on page 91.

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, 2 stop bits and 8 data bits

- For fixed chassis, the console settings are baud rate 115200 bps, no parity, 2 stop bits and 8 data bits.

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

Step 3 Power on the router.

Connect the power 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.

Before you begin

The boot process must be complete. For details on how to initiate the boot process, see Bring-up the Router, on page 5.

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/
!
```

What to do next

- Configure routing functions from the XR console.
- Configure system administration settings from the System Admin prompt. The System Admin prompt is displayed on accessing the System Admin console. For details on how to get the System Admin prompt, see Access the System Admin Console, on page 7.

Access the System Admin Console

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

SUMMARY STEPS

1. Login to the XR console as the root user.
2. (Optional) Disable the login banner on console port when accessing the System Admin mode from XR mode.
3. **admin**
4. (Optional) **exit**

DETAILED STEPS

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

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

a) **configure**

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

Example:

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

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

c) **commit**

d) **end**

Step 3 **admin**

Example:

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

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

Mon May 22 06:57:29.350 UTC

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

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

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

Step 4 (Optional) **exit**

Return to the XR mode from the System Admin mode.

Configure the Management Port

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

Before you begin

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

SUMMARY STEPS

1. **configure**
2. **interface MgmtEth** *rack/slot/port*
3. (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 global configuration mode.

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

Example:

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

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

Step 3 (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
```

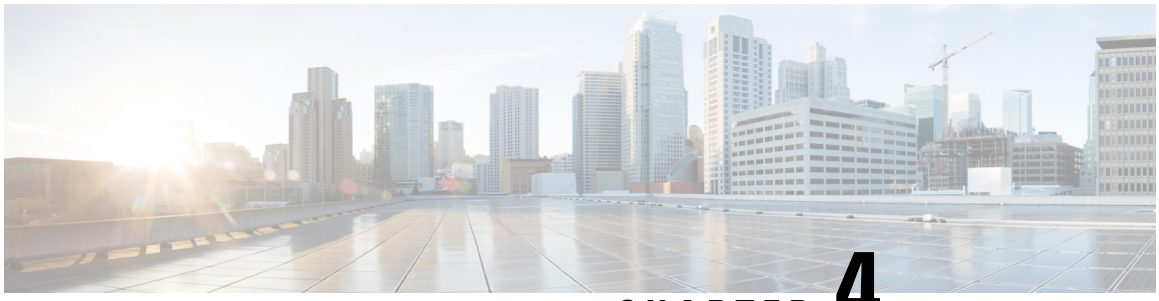
Enters global configuration mode.

Step 2 **ntp server** *server_address*

Example:

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

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



CHAPTER 4

Perform Preliminary Checks

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

Verify Software Version

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

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

SUMMARY STEPS

1. **show version**

DETAILED STEPS

show version

Example:

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

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

Example

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

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

cisco NCS-5500 () processor
System uptime is 3 hours, 42 minutes
```

What to do next

Verify the result to ascertain whether a system upgrade or additional package installation is required. If that is required, refer to the tasks in the chapter Perform System Upgrade and Install Feature Packages, on page 41.

Verify Status of Hardware Modules

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

Before you begin

Ensure that all required hardware modules have been installed on the router.

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **admin**

Example:

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

Enters System Admin EXEC mode.

Step 2 **show platform**

Example:

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

Displays the list of hardware modules detected on the router.

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

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

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

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

Verify Firmware Version

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

SUMMARY STEPS

1. **show hw-module fpd**

DETAILED STEPS

show hw-module fpd

Example:

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

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

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

Displays the list of hardware modules detected on the router.

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

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

- FPD Device- Name of the hardware component such as FPD, CFP, and so on.
- ATR-Attribute of the hardware component. Some of the attributes are:
  - B- Backup Image
  - S-Secure Image
  - P-Protected Image
- Status- Upgrade status of the firmware. The different states are:
  - CURRENT-The firmware version is the latest version.
  - READY-The firmware of the FPD is ready for an upgrade.
  - NOT READY-The firmware of the FPD is not ready for an upgrade.
  - NEED UPGD-A newer firmware version is available in the installed image. It is recommended that an upgrade be performed.
  - RLOAD REQ-The upgrade has been completed, and the ISO image requires a reload.
  - UPGD DONE-The firmware upgrade is successful.
  - UPGD FAIL- The firmware upgrade has failed.

- BACK IMG-The firmware is corrupted. Reinstall the firmware.
- UPGD SKIP-The upgrade has been skipped because the installed firmware version is higher than the one available in the image.

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

What to do next

If it is required to replace a line card or route processor, use one of the two methods:

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

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

Verify SDR Information

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **admin**

Example:

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

Enters mode.

Step 2 **show sdr**

Example:

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

Displays the SDR information for every node.

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

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

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

For a functional SDR, the VM State is "RUNNING". If the SDR is not running on a node, no output is shown in the result, for that location.

What to do next

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

Verify Interface Status

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

SUMMARY STEPS

1. **show ipv4 interface summary**

DETAILED STEPS

show ipv4 interface summary

Example:

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

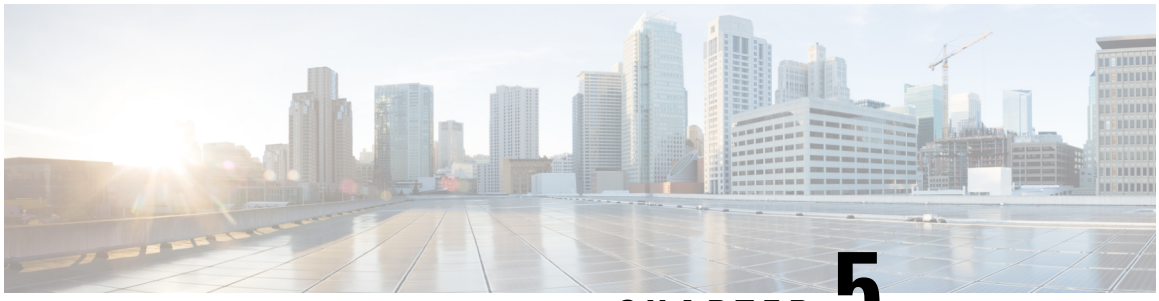
When a router is turned on for the first time, all interfaces are in the 'unassigned' state. Verify that the total number of interfaces displayed in the result matches with the actual number of interfaces present on the router.

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

In the above result:

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

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



CHAPTER 5

Create User Profiles and Assign Privileges

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

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

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

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

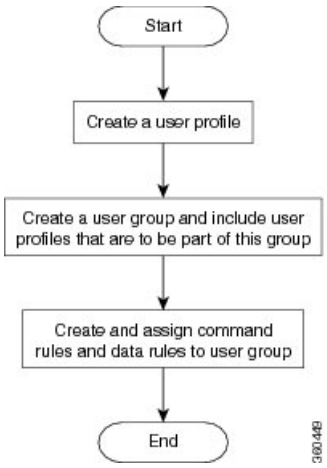
Note If any user on XR is deleted, the local database checks whether there is a first user on System Admin VM.

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

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

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

Figure 1: Workflow for Creating User Profiles



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

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

The topics covered in this chapter are:

Create User Groups

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

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

Configure User Groups in XR VM

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

Before you begin

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

SUMMARY STEPS

1. **configure**
2. **usergroup** *usergroup-name*
3. **description** *string*
4. **inherit usergroup** *usergroup-name*
5. **taskgroup** *taskgroup-name*
6. Repeat Step for each task group to be associated with the user group named in Step 2.
7. Use the **commit** or **end** command.

DETAILED STEPS

Step 1 **configure**

Example:

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

Enters global configuration mode.

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

Example:

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

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

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

Step 3 **description** *string*

Example:

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

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

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

Example:

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

- Explicitly defines permissions for the user group.

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

Example:

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

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

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

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

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

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

end —Prompts user to take one of these actions:

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

Create a User Group in System Admin VM

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 31.
- Create data rules. See Create Data Rules, on page 33.

Create Users

Create new users for the XR VM and System Admin VM.

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

XR VM and System Admin VM User Profile Synchronization

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

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

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

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

Create a User Profile in XR VM

Table 1: Feature History Table

Feature name	Release Information	Feature Description
Enhanced Login Banner Standards	Release 7.3.1	To comply with the US DoD, an option to enable display of login banner is introduced. The login banner provides information such as number of successful and unsuccessful login attempts, time stamp, login method, and so on. The login-history command is introduced.

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

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

Step 1 **configure**

Example:

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

Enters global configuration mode.

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

Example:

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

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

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

Step 3 Do one of the following:

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

Example:

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

or

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

Specifies a password for the user named in Step 2.

- Use the **secret** command to create a secure login password for the user names specified in Step 2.
- Entering **0** following the **password** command specifies that an unencrypted (clear-text) password follows. Entering **7** following the **password** command specifies that an encrypted password follows.
- For the **secret** command, the following values can be entered:
  - **0** : specifies that a secure unencrypted (clear-text) password follows
  - **5** : specifies that a secure encrypted password follows that uses MD5 hashing algorithm
  - **8** : specifies that Type 8 secret that uses SHA256 hashing algorithm follows
  - **9** : specifies that Type 9 secret that uses SCrypt hashing algorithm follows

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

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

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

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

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

Example:

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

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

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

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

Step 6 (Optional) You can enable the display of the US Department of Defense DOD-approved login banner. The banner is displayed before granting access to devices. The banner also ensures privacy and security that is consistent with applicable federal laws. In addition, the system keeps track of logins, right from the system boot, or as soon as the user profile is created.

Note When you reload a router, login notifications get reset.

Enable or disable the login banner using these commands:

Example:

```
Router(config-un)#login-history enable
Router(config-un)#login-history disable
```

Run the `show running-config username user1` command to verify the state of login banner.

```
Router(config-un)# show running-config username NAME1
Fri Jan 29 13:55:28.261 UTC
username NAME1
 group UG1
 secret * **********
 password * ******
 login-history enable
```

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

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

end —Prompts user to take one of these actions:

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

Create a User Profile in System Admin VM

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 24.
- Create command rules that apply to the user group. See Create Command Rules, on page 31.

- Create data rules that apply to the user group. See Create Data Rules, on page 33.

Create Command Rules

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

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

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

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

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

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

Before you begin

Create an user group. See Create a User Group in System Admin VM, on page 24.

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 33.

Create Data Rules

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

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

Before you begin

Create an user group. See Create a User Group in System Admin VM, on page 24.

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

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

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

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

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

SUMMARY STEPS

1. **admin**
2. **config**
3. **aaa disaster-recovery username** *username* **password** *password*
4. Use the **commit** or **end** command.

DETAILED STEPS

Step 1 **admin**

Example:

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

Enters mode.

Step 2 **config**

Example:

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

Enters System Admin Config mode.

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

Example:

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

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

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

Step 4 Use the **commit** or **end** command.

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

end —Prompts user to take one of these actions:

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

Recover Password using PXE Boot

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

Step 1 Boot the router using PXE.

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

To PXE boot a router, see Boot the Router Using iPXE, on page 116.

Step 2 Reset the password.

Recover System From Lost Password

Table 2: Feature History Table

Feature name	Release Information	Feature Description
Recover System Using Console Port	Release 7.3.3	With this feature, you can recover access to your router if you lose your admin and root credentials, without having to reimage using iPXE orUSB boot. Recovery involves a router reload, and the user data is securely erased before the router reloads.

If you lose your admin and root user credentials, the router becomes inaccessible. You can recover the system using a router reimage using iPXE or USB boot. However, this approach is not scalable.

With the Recover System Using Console Port feature, you can recover access to your router if you lose your admin and root credentials. This does not require you to reimage using iPXE orUSB boot. The system is recovered to its initial state with the current running software. The installed software and SMUs are retained after the system is recovered. The process complies with the Cisco Product Security Baseline (PSB) where user data is securely erased before recovering the router.

Note The Recover System Using Console Port feature must be configured and ready, to recover the system in the event of a disaster.

The following data that are generated at run-time are erased:

- XR and admin configuration including the password data
- Cryptographic keys on the disk
- Data on encrypted partition
- Generated core files
- SNMP interface index files
- Third-party application (TPA) software and data
- User files
- Run-time generated logs

Note The data on the line card is not erased.

This feature is disabled by default. Since the router can be recovered through the console, it is crucial to secure the physical access and the console.

The following steps show the process to recover the system if there is a disaster.

Before you begin

Prepare the system with the following requirements:

- Ensure that you have administrator privileges.
- Ensure you have the console access to both DCCO and DCC1 (ILO/VSP or Serial Console).
- Enter the XR configuration mode. Enable the system recovery using console port.

  ```
  Router(config)#system recovery
  ```

  With this command, the functionality to recover the router is enabled. The logs are stored at `/var/log/system_recovery_logs/` location.

Note To disable this feature, use the **no** form of command.

```
Router(config)#no system recovery
```

- Verify using the below CLI to ensure that the feature is enabled:

```
Router#show running-config system recovery
system recovery
```

Step 1 Power cycle the router using an external power cycler.

Step 2 Press `ESC` key and hold both active and standby RPs (RP0 and RP1) in BIOS.

This procedure must be executed on each RP individually on a distributed system.

Step 3 Boot on the standby RP. Press `ESC` or `F2` key to enter the GRUB (bootstrap program) menu.

Step 4 Select the **System-Host-OS-Recovery** option from the menu.

The RP boots in the recovery mode, clears generated files, and reboots.

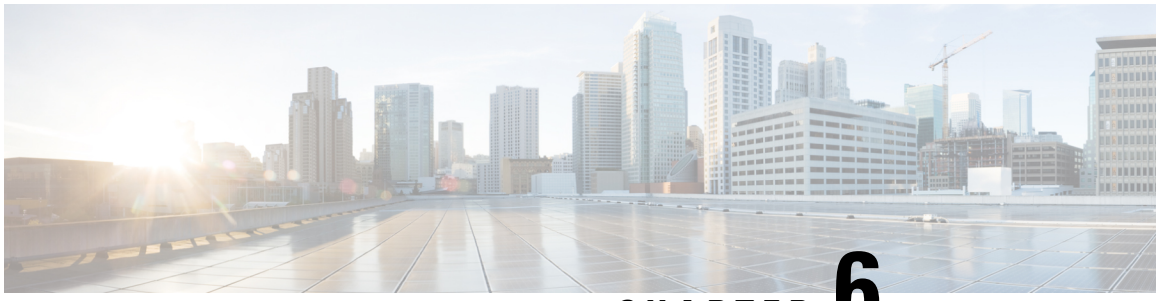
Step 5 Hold the standby RP in BIOS prompt and initiate the recovery on the active RP.

The active RP boots up and the login prompt appears.

Step 6 Boot the standby RP.

After the system boots up, the syslog displays the status of the recovery operation. If the recovery operation fails, the system comes up to an inconsistent state. Power cycle and retry the recovery. If the router recovery is successful, configure the credentials to log in to the router with the pre-existing image.

Note The option to recover the system using console port is disabled on bootup because all previous configurations are erased. The GRUB option applies even without the Recover System Using Console Port feature. However, selecting the GRUB feature without configuring the Recover System Using Console Port feature results in a skipped recovery option during reboot.



CHAPTER 6

Perform System Upgrade and Install Feature Packages

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

The topics covered in this chapter are:

Upgrading the System

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

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

Note If you insert a line card on a router that is running a lower version than the one the line card supports, the line card will fail to boot. You must first upgrade the router to a software version that supports the line card, insert the line card and iPXE boot the line card. For more information, see Boot the Router Using iPXE, on page 111.

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

System upgrade is done by installing a base package–Cisco IOS XR Unicast Routing Core Bundle. The file name for this bundle is *ncs5500-mini-x.iso*. Install this ISO image using **install** commands. For more information about the install process, see Workflow for Install Process, on page 43.

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

Do not reload the router during an upgrade operation.

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, used for signing the RPM packages, is created and securely maintained by Cisco.

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

Upgrading Features

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

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

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

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

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

Feature	Package
infra	ncs5500-infra-1.0.0.0-<*release-number*>.x86_64.rpm
os	ncs5500-os-1.0.0.0-<*release-number*>.x86_64.rpm
routing	ncs5500-routing-1.0.0.0-<*release-number*>.x86_64.rpm
security	ncs5500-security-1.0.0.0-<*release-number*>.x86_64.rpm
os-support	ncs5500-os-support-1.0.0.0-<*release-number*>.x86_64.rpm

Package and SMU installation is performed using **install** commands. For more information about the install process, see Install Packages, on page 44.

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.

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, **ncs5500**-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 44. For uninstalling a package, see Uninstall Packages, on page 52.

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.

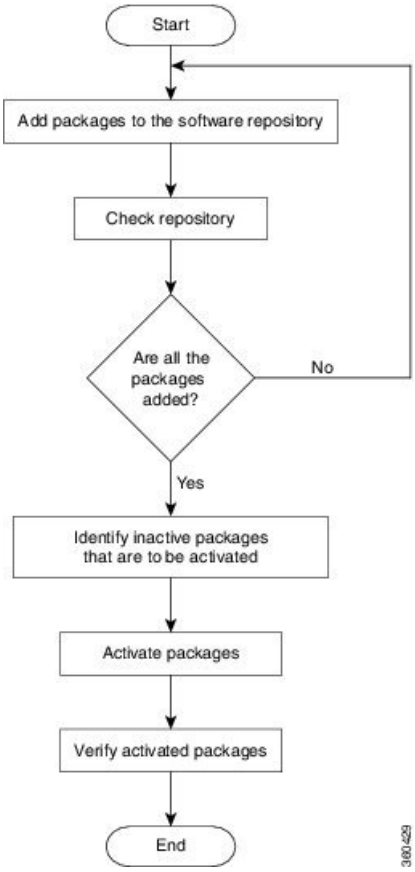
This task is also used to install *.rpm* files. The *.rpm* file contains multiple packages and SMUs that are merged into a single file. The packaging format defines one RPM per component, without dependency on the card type.

Note

- The System Admin package and XR package can be executed using **install** commands in the System Admin EXEC mode and XR EXEC mode. All **install** commands are applicable in both these modes.
- Install operation over IPv6 is not supported.

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 8.
- 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:/ncs5500-mpls-1.0.0.0-r600.x86_64.rpm
ncs5500-mgbl-2.0.0.0-r600.x86_64.rpm
```

or

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

or

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

The software files are unpacked from the package, 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
```

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

Step 3 **show install repository**

Example:

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

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

Step 4 **show install inactive**

Example:

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

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

Step 5 Execute one of these:

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

Example:

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

or

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

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

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

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

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.

Related Commands	Purpose
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 52.

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

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

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

Install Prepared Packages

- 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.

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 44.

Step 2 **show install repository**

Example:

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

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

Step 3 Execute one of these:

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

Example:

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

or

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

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

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

Step 4 **show install prepare**

Example:

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

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

Step 5 **install activate**

Example:

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

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

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

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.

```
Node 0/RP0/CPU0 [RP]
Boot Partition: xr_lv70
Active Packages: 24
ncs5500-xr-6.0.0 version=6.0.0 [Boot image]
ncs5500-k9sec-1.0.0.0-r600
ncs5500-mgbl-2.0.0.0-r600
ncs5500-mpls-1.0.0.0-r600
ncs5500-mpls-te-rsvp-1.0.0.0-r600
ncs5500-infra-2.0.0.2-r600.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.2-r600.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.5-r600.CSCxr90016
```

```
ncs5500-iosxr-fwding-2.0.0.1-r600.CSCxr55555
ncs5500-iosxr-fwding-2.0.0.6-r600.CSCxr90017
ncs5500-dpa-1.0.0.1-r600.CSCxr90002
ncs5500-dpa-1.0.0.2-r600.CSCxr90004
ncs5500-dpa-fwding-1.0.0.1-r600.CSCxr90005
ncs5500-k9sec-1.0.0.1-r600.CSCxr80008
ncs5500-os-support-1.0.0.1-r600.CSCxr90013
ncs5500-os-support-1.0.0.2-r600.CSCxr90014
ncs5500-fwding-1.0.0.2-r600.CSCxr90011
ncs5500-fwding-1.0.0.5-r600.CSCxr90019
ncs5500-fwding-1.0.0.1-r600.CSCxr90010
ncs5500-fwding-1.0.0.4-r600.CSCxr90018
ncs5500-mgbl-2.0.0.2-r600.CSCxr80009
ncs5500-mpls-1.0.0.1-r600.CSCxr33333
ncs5500-mpls-te-rsvp-1.0.0.2-r600.CSCxr33335
```

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

Step 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.

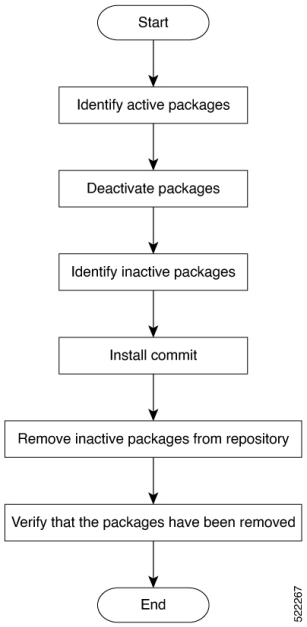
Uninstall Packages

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.

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

Step 2 Execute one of these:

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

Example:

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

or

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

The *operation_id* is the ID from **install add** operation. All features and software patches associated with the package are deactivated. You can specify multiple package names and deactivate them simultaneously.

If you use the operation ID, all packages that were added in the specified operation are deactivated together. You do not have to deactivate the packages individually. If System admin packages were added as a part of the **install add** operation (of the ID used in deactivate) then those packages will also be deactivated.

Step 3 **show install inactive**

Example:

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

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

Step 4 **install commit**

Step 5 **install remove** *package_name*

Example:

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

The inactive packages are removed from the repository.

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

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

Step 6 **show install repository**

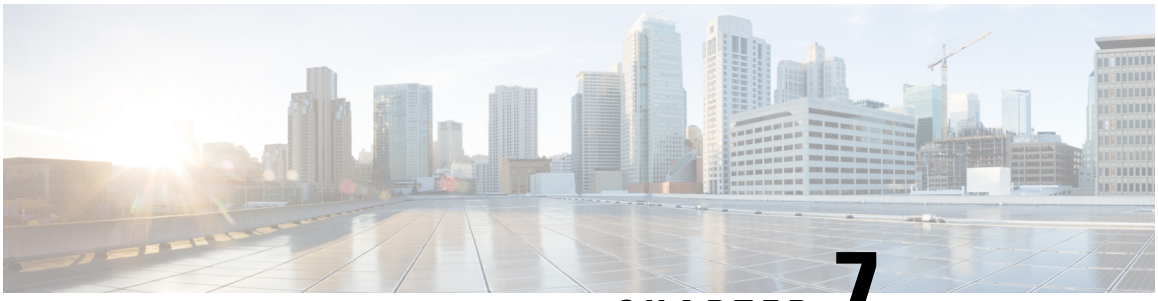
Example:

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

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

What to do next

Install required packages. .

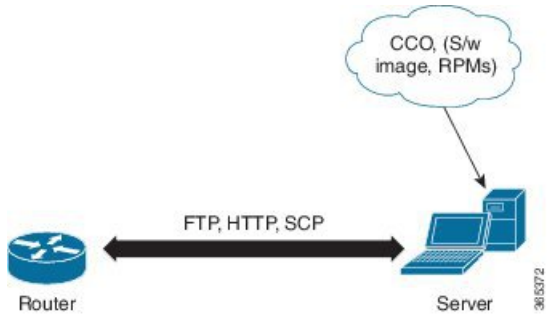


CHAPTER 7

Manage Automatic Dependency

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

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



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

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

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

Note

1. Cisco IOS XR Version 6.0.2 and later does not provide third party and host package SMUs as part of automatic dependency management (**install source** command). The third party and host package SMUs must be installed separately, and in isolation from other installation procedures (installation of SMUs and RPMs in IOS XR or admin containers).
2. From Cisco IOS XR Version 6.5.2 onwards, it is possible to update the `mini.iso` file by using the **install source** command.

The rest of this chapter contains these sections:

• Downgrade an RPM, on page 58

Update RPMs and SMUs

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

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

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

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

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

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

  ```
  install source [repository]
  ```

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

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

- **When a package name is specified**

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

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

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

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

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

- **When an SMU is specified**

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

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

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

  From Cisco IOS XR Version 6.5.2 onwards, if a list of packages (containing the `mini.iso` file) is specified, all the packages in the list and the `mini.iso` file are automatically added as part of the update.

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

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

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

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

Upgrade Base Software Version

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

Note SMUs are not upgraded as part of this process.

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

```
install source repository
```

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

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

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

- **The version number is specified**

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

  ```
  install source [repository] version <version> asr9k-mini-x64-<version>.iso
  ```

  For example,

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

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

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

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

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

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

Downgrade an RPM

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

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

  For example:

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

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

  For example:

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

To deactivate the RPMs, perform the following steps:

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

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

    2. Activate the downloaded RPMs.

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

    3. Commit the configuration.

       ```
       install commit
       ```

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

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

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

```
install commit
```

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

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

- **Downgrade Non-Hostos RPM**

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

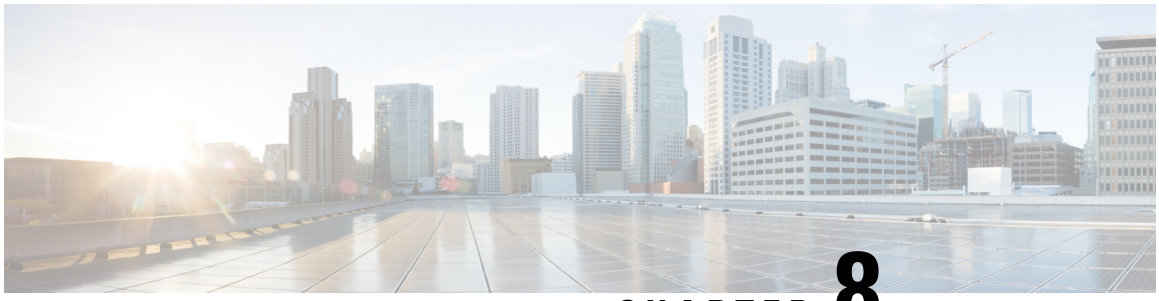
   ```
   install deactivate <platform>-<rpm-name>
   ```

2. Check the active version of the RPM.

   ```
   show install active
   ```

3. Commit the configuration.

   ```
   install commit
   ```



CHAPTER 8

Customize Installation using Golden ISO

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

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

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

When a system boots with GISO, additional SMUs and RPMs in GISO are installed automatically, and the router is pre-configured with the XR configuration in GISO. For more information about downloading and installing GISO, see Install Golden ISO, on page 67.

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

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

Limitations

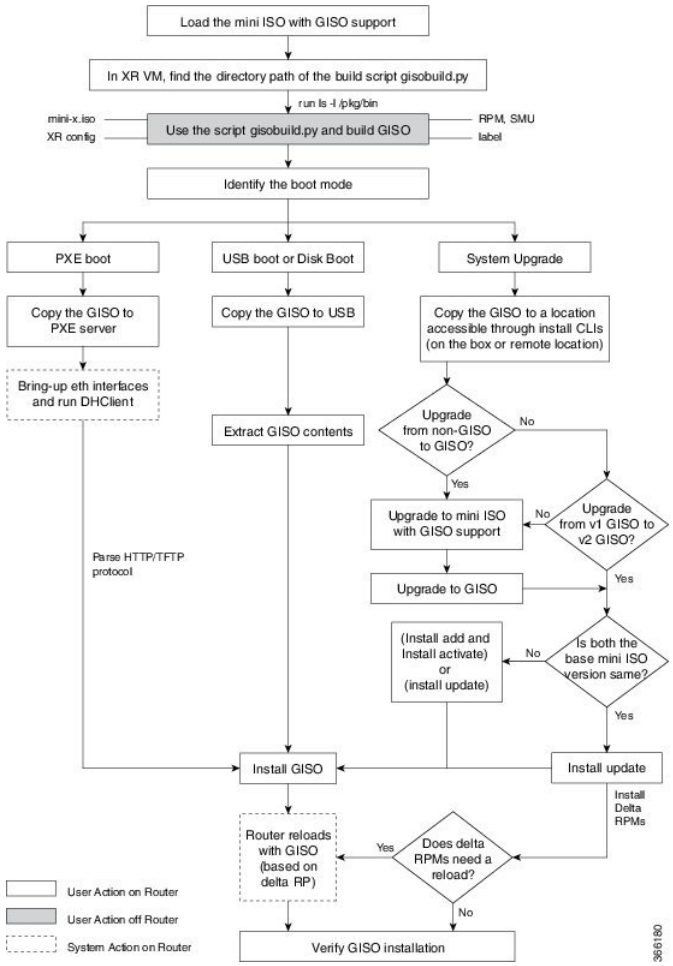
The following are the known problems and limitations with the customized ISO:

- GISO image size more than 1.8 GB is not supported.
- Building and booting GISO for asynchronous package (a package of different release than the ISO) is not supported.
- Verifying the XR configuration is not supported in the GISO build script `gisobuild.py`.

- Renaming a GISO build and then installing from the renamed GISO build is not supported.
- Install operation over IPv6 is not supported.

Golden ISO Workflow

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



Build Golden ISO

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

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

- Builds RPM database of all the packages present in package repository.
- Scans the repositories and selects the relevant Cisco RPMs that matches the input iso.

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

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 (mandatory)
- one or more third-party SMUs for host, XR and System admin (mandatory)
- 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. For NCS 5500 series routers, upgrade to release 6.2.2 or later.
- The system where GISO is built must meet the following requirements:
  - System must have Python version 2.7 and later.
  - System must have free disk space of minimum 3 to 4 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`.

Note NCS5500 routers has two types of cards - x86_64 and arm. System Admin runs on both types of cards, whereas XR runs only on x86_64 card.

```
[directory-path]$ gisobuild.py -i ncs5500-mini-x.iso -r .
-c config-file -l v1

System requirements check [PASS]
Platform: ncs5500 Version: <version>
XR-Config file (/<directory>/config-file) will be encapsulated in GISO.
Scanning repository [/<directory>/ncs5500-giso]...
Building RPM Database...
Total 54 RPM(s) present in the repository path provided in CLI

Skipping following older version of host os rpm(s) from repository:
         ncs5500-sysadmin-hostos-<version>-r<version>.CSCho88888.admin.x86_64.rpm
         ncs5500-sysadmin-hostos-<version>-r<version>.CSCho88888.host.x86_64.rpm
Skipping following older version of spirit-boot rpm(s) from repository:
         ncs5500-spirit-boot-1.0.0.2-r<version>.CSCsb88888.x86_64.rpm
         ncs5500-spirit-boot-1.0.0.1-r<version>.CSCsb77777.x86_64.rpm

Following XR x86_64 rpm(s) will be used for building GISO:
         ncs5500-iosxr-infra-4.0.0.2-r<version>.CSCxr11111.x86_64.rpm
         ncs5500-m2m-1.0.0.0-r<version>.x86_64.rpm
         ncs5500-iosxr-infra-4.0.0.4-r<version>.CSCxr11111.x86_64.rpm
         ncs5500-iosxr-infra-4.0.0.3-r<version>.CSCxr44444.x86_64.rpm
         ncs5500-k9sec-3.1.0.0-r<version>.x86_64.rpm
         ncs5500-iosxr-fwding-4.0.0.2-r<version>.CSCxr22222.x86_64.rpm
         ncs5500-spirit-boot-1.0.0.3-r<version>.CSCsb77777.x86_64.rpm
         ncs5500-k9sec-3.1.0.1-r<version>.CSCxr33333.x86_64.rpm
         ncs5500-iosxr-fwding-4.0.0.1-r<version>.CSCxr22222.x86_64.rpm
         ncs5500-mgbl-3.0.0.0-r<version>.x86_64.rpm
         ncs5500-parser-2.0.0.0-r<version>.x86_64.rpm
         ncs5500-iosxr-mgbl-3.0.0.0-r<version>.x86_64.rpm
         ncs5500-k9sec-3.1.0.2-r<version>.CSCxr33333.x86_64.rpm
         ncs5500-iosxr-infra-4.0.0.1-r<version>.CSCxr44444.x86_64.rpm
         kernel-image-3.14.23-wr7.0.0.3-standard-3.14-r0.1.xr.x86_64.rpm
         openssh-scp-6.6p1-r0.0.xr.x86_64.rpm
         cisco-klm-mifpga-0.1.p1-r0.0.CSCtp11111.xr.x86_64.rpm
         kernel-image-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
         cisco-klm-mifpga-0.1-r0.0.xr.x86_64.rpm
         kernel-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
         kernel-modules-3.14-r0.1.xr.x86_64.rpm
         kernel-modules-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
```

```
Skipping following rpms from repository since they are already present in base ISO:
         ncs5500-mgbl-3.0.0.0-r<version>.x86_64.rpm
         ncs5500-m2m-1.0.0.0-r<version>.x86_64.rpm
         ncs5500-parser-2.0.0.0-r<version>.x86_64.rpm

Following XR rpm(s) will be used for building GISO:
         kernel-modules-3.14-r0.1.xr.x86_64.rpm
         kernel-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
         ncs5500-iosxr-fwding-4.0.0.2-r<version>.CSCxr22222.x86_64.rpm
         ncs5500-iosxr-infra-4.0.0.3-r<version>.CSCxr44444.x86_64.rpm
         ncs5500-iosxr-infra-4.0.0.2-r<version>.CSCxr11111.x86_64.rpm
         kernel-image-3.14.23-wr7.0.0.2-standard-3.14-r0.1.xr.x86_64.rpm
         cisco-klm-mifpga-0.1-r0.0.xr.x86_64.rpm
         cisco-klm-mifpga-0.1.p1-r0.0.CSCtp11111.xr.x86_64.rpm
         ncs5500-iosxr-infra-4.0.0.4-r<version>.CSCxr11111.x86_64.rpm
         ncs5500-iosxr-fwding-4.0.0.1-r<version>.CSCxr22222.x86_64.rpm
         openssh-scp-6.6p1-r0.0.xr.x86_64.rpm
         ncs5500-k9sec-3.1.0.2-r<version>.CSCxr33333.x86_64.rpm
         ncs5500-k9sec-3.1.0.0-r<version>.x86_64.rpm
         kernel-modules-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
         ncs5500-k9sec-3.1.0.1-r<version>.CSCxr33333.x86_64.rpm
         openssh-scp-6.6p1.p1-r0.0.CSCtp11111.xr.x86_64.rpm
         ncs5500-spirit-boot-1.0.0.3-r<version>.CSCsb77777.x86_64.rpm
         ncs5500-iosxr-mgbl-3.0.0.0-r6<version>.x86_64.rpm
         kernel-image-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
         ncs5500-iosxr-infra-4.0.0.1-r<version>.CSCxr44444.x86_64.rpm
         kernel-3.14.23-wr7.0.0.2-standard-3.14-r0.1.xr.x86_64.rpm

        ...RPM compatibility check [PASS]

Following CALVADOS x86_64 rpm(s) will be used for building GISO:
         ncs5500-sysadmin-shared-<version>-r<version>.CSCcv22222.x86_64.rpm
         ncs5500-sysadmin-hostos-<version>-r<version>.CSCho77777.admin.x86_64.rpm
         ncs5500-sysadmin-system-<version>-r<version>.CSCcv11111.x86_64.rpm
         ncs5500-sysadmin-shared-<version>-r62114I.CSCcv33333.x86_64.rpm
         ncs5500-sysadmin-system-<version>-r<version>.CSCcv44444.x86_64.rpm
         kernel-modules-3.14.p1-r0.1.CSCtp11111.admin.x86_64.rpm
         cisco-klm-mifpga-0.1-r0.0.admin.x86_64.rpm
         kernel-image-3.14.23-wr7.0.0.2-standard-3.14-r0.1.admin.x86_64.rpm
         kernel-modules-3.14-r0.1.admin.x86_64.rpm
         kernel-image-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.admin.x86_64.rpm
         kernel-3.14.23-wr7.0.0.2-standard-3.14-r0.1.admin.x86_64.rpm
         kernel-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.admin.x86_64.rpm
         cisco-klm-mifpga-0.1.p1-r0.0.CSCtp11111.admin.x86_64.rpm
         openssh-scp-6.6p1.p1-r0.0.CSCtp11111.admin.x86_64.rpm
         openssh-scp-6.6p1-r0.0.admin.x86_64.rpm
        ...RPM compatibility check [PASS]

Following HOST x86_64 rpm(s) will be used for building GISO:
         ncs5500-sysadmin-hostos-6.2.1.17-r62114I.CSCho77777.host.x86_64.rpm
         cisco-klm-mifpga-0.1.p1-r0.0.CSCtp11111.host.x86_64.rpm
         kernel-image-3.14.23-wr7.0.0.2-standard-3.14-r0.1.host.x86_64.rpm
         kernel-modules-3.14.p1-r0.1.CSCtp11111.host.x86_64.rpm
         kernel-modules-3.14-r0.1.host.x86_64.rpm
         openssh-scp-6.6p1.p1-r0.0.CSCtp11111.host.x86_64.rpm
         cisco-klm-mifpga-0.1-r0.0.host.x86_64.rpm
         kernel-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.host.x86_64.rpm
         kernel-3.14.23-wr7.0.0.2-standard-3.14-r0.1.host.x86_64.rpm
         openssh-scp-6.6p1-r0.0.host.x86_64.rpm
         kernel-image-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.host.x86_64.rpm
        ...RPM compatibility check [PASS]

Building Golden ISO...
Summary .....
```

```
XR rpms:
        kernel-modules-3.14-r0.1.xr.x86_64.rpm
        kernel-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
        ncs5500-iosxr-fwding-4.0.0.2-r<version>.CSCxr22222.x86_64.rpm
        ncs5500-iosxr-infra-4.0.0.3-r<version>.CSCxr44444.x86_64.rpm
        ncs5500-iosxr-infra-4.0.0.2-r<version>.CSCxr11111.x86_64.rpm
        kernel-image-3.14.23-wr7.0.0.2-standard-3.14-r0.1.xr.x86_64.rpm
        cisco-klm-mifpga-0.1-r0.0.xr.x86_64.rpm
        cisco-klm-mifpga-0.1.p1-r0.0.CSCtp11111.xr.x86_64.rpm
        ncs5500-iosxr-infra-4.0.0.4-r<version>.CSCxr11111.x86_64.rpm
        ncs5500-iosxr-fwding-4.0.0.1-r<version>.CSCxr22222.x86_64.rpm
        openssh-scp-6.6p1-r0.0.xr.x86_64.rpm
        ncs5500-k9sec-3.1.0.2-r<version>.CSCxr33333.x86_64.rpm
        ncs5500-k9sec-3.1.0.0-r<version>.x86_64.rpm
        kernel-modules-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
        ncs5500-k9sec-3.1.0.1-r<version>.CSCxr33333.x86_64.rpm
        openssh-scp-6.6p1.p1-r0.0.CSCtp11111.xr.x86_64.rpm
        ncs5500-spirit-boot-1.0.0.3-r<version>.CSCsb77777.x86_64.rpm
        ncs5500-iosxr-mgbl-3.0.0.0-r<version>.x86_64.rpm
        kernel-image-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.xr.x86_64.rpm
        ncs5500-iosxr-infra-4.0.0.1-r<version>.CSCxr44444.x86_64.rpm
        kernel-3.14.23-wr7.0.0.2-standard-3.14-r0.1.xr.x86_64.rpm

CALVADOS rpms:
        ncs5500-sysadmin-shared-<version>-r<version>.CSCcv22222.x86_64.rpm
        ncs5500-sysadmin-hostos-<version>-r<version>.CSCho77777.admin.x86_64.rpm
        ncs5500-sysadmin-system-<version>-r<version>.CSCcv11111.x86_64.rpm
        ncs5500-sysadmin-shared-<version>-r<version>.CSCcv33333.x86_64.rpm
        ncs5500-sysadmin-system-<version>-r<version>.CSCcv44444.x86_64.rpm
        kernel-modules-3.14.p1-r0.1.CSCtp11111.admin.x86_64.rpm
        cisco-klm-mifpga-0.1-r0.0.admin.x86_64.rpm
        kernel-image-3.14.23-wr7.0.0.2-standard-3.14-r0.1.admin.x86_64.rpm
        kernel-modules-3.14-r0.1.admin.x86_64.rpm
        kernel-image-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.admin.x86_64.rpm
        kernel-3.14.23-wr7.0.0.2-standard-3.14-r0.1.admin.x86_64.rpm
        kernel-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.admin.x86_64.rpm
        cisco-klm-mifpga-0.1.p1-r0.0.CSCtp11111.admin.x86_64.rpm
        openssh-scp-6.6p1.p1-r0.0.CSCtp11111.admin.x86_64.rpm
        openssh-scp-6.6p1-r0.0.admin.x86_64.rpm

HOST rpms:
        ncs5500-sysadmin-hostos-<version>-r<version>.CSCho77777.host.x86_64.rpm
        cisco-klm-mifpga-0.1.p1-r0.0.CSCtp11111.host.x86_64.rpm
        kernel-image-3.14.23-wr7.0.0.2-standard-3.14-r0.1.host.x86_64.rpm
        kernel-modules-3.14.p1-r0.1.CSCtp11111.host.x86_64.rpm
        kernel-modules-3.14-r0.1.host.x86_64.rpm
        openssh-scp-6.6p1.p1-r0.0.CSCtp11111.host.x86_64.rpm
        cisco-klm-mifpga-0.1-r0.0.host.x86_64.rpm
        kernel-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.host.x86_64.rpm
        kernel-3.14.23-wr7.0.0.2-standard-3.14-r0.1.host.x86_64.rpm
        openssh-scp-6.6p1-r0.0.host.x86_64.rpm
        kernel-image-3.14.23-wr7.0.0.2-standard-3.14.p1-r0.1.CSCtp11111.host.x86_64.rpm
XR Config file:
router.cfg

        ...Golden ISO creation SUCCESS.
Golden ISO Image Location: /<directory>/ncs5500-goldenk9-x.iso-<version>.v1
Detail logs: <directory>/Giso_build.log-2016-10-01:16:22:48.305211
```

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.

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

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

- **USB boot or Disk Boot:** when the USB mode is detected during boot, and GISO is identified, the additional RPMs and XR configuration files are extracted and installed.

- **System Upgrade** when the system is upgraded, GISO can be installed using **install add**, **install activate**, or using **install replace** commands.

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

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

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

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

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

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

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

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

```
Router#admin

sysadmin-vm:0_RSP0# run chvrf 0 ssh rp0_admin
[sysadmin-vm:0_RSP0:~]$ ssh my_host
[host:~]$ cd /misc/disk1/
[host:~]$ ./usb-install-712-or-latest.sh asr9k-goldenk9-x64-7.0.2-dr.isso /dev/sdc
EFI

Preparing USB stick for EFI
parted gpt: Failed to create partition - continuing ...
Create filesystem on /dev/sdc1
Mounting source iso at //misc/disk1/cdtmp.CnuKnA
Mounting destination /dev/sdc1 at //misc/disk1/usbdev.SSBb4R
Copying image to USB stick
Initrd path is //misc/disk1/cdtmp.CnuKnA/boot/initrd.img
Getting boot
3749342 blocks
Copying boot
Copying initrd.img
Copying signature.initrd.img
Copying certs
Creating grub files
Copying /misc/disk1/asr9k-goldenk9-x64-7.0.2-dr.iso in USB Stick
USB stick set up for EFI boot!
```

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 update** command installs only the delta RPMs. System reload is based on restart type of the delta RPMs.

- **system upgrade across releases from version1 GISO to version2 GISO:** Both the GISO images have different base versions. Use **install add** and **install activate** commands, or **install replace** command to perform the system upgrade. The router reloads after the upgrade with the version2 GISO image.

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

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

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

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

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

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

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

        ISO Name: host-6.2.2
        ISO Type: host
        rpms in host ISO:
```

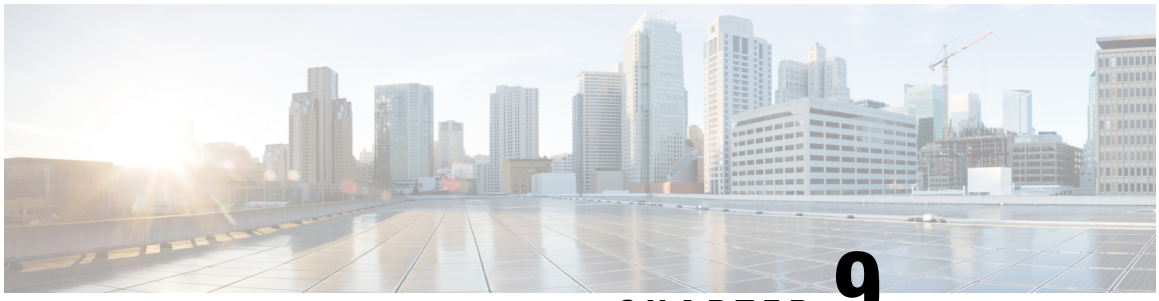
```
    ncs5500-sysadmin-hostos-6.2.2-r622.host

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

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

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

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



CHAPTER 9

Provision Network Devices using Zero Touch Provisioning

Manually deploying network devices in a large-scale environment requires skilled workers and is time consuming.

With Zero Touch Provisioning (ZTP), you can seamlessly provision thousands of network devices accurately within minutes and without any manual intervention. This can be easily defined using a configuration file or script using shell or phyton.

Table 3: Feature History Table

Feature Name	Release Information	Feature Description
Zero Touch Provisioning	Release 7.3.1	With this release, you can seamlessly provision thousands of network devices accurately within minutes and without any manual intervention. This can be easily defined using a configuration file or script using shell or phyton.

Learn about Zero Touch Provisioning

ZTP allows you to provision the network device with day 0 configurations and supports both management ports and data ports.

Note Currently, ZTP only supports single name-server. When the DHCP server has more than one server address configured, ZTP fails to apply the server configuration.

ZTP provides multiple options, such as:

- Automatically apply specific configuration in a large-scale environment.
- Download and install specific IOS XR image.
- Install specific application package or third party applications automatically.
- Deploy containers without manual intervention.
- Upgrade or downgrade software versions effortlessly on thousands of network devices at a time

Benefits of Using ZTP

ZTP helps you manage large-scale service providers infrastructures effortlessly. Following are the added benefits of using ZTP:

- ZTP helps you to remotely provision a router anywhere in the network. Thus eliminates the need to send an expert to deploy network devices and reduces IT cost.
- Automated provisioning using ZTP can remove delay and increase accuracy and thus is cost-effective and provides better customer experience.

  By automating repeated tasks, ZTP allows network administrators to concentrate on more important stuff.
- ZTP process helps you to quickly restore service. Rather than troubleshooting an issue by hand, you can reset a system to well-known working status.

Use Cases

he following are some of the useful use cases for ZTP:

- Using ZTP to install Chef
- Using ZTP to integrate IOS-XR with NSO
- Using ZTP to install Puppet

You can initiate ZTP in one of the following ways:

- **Fresh Boot**: Use this method for devices that has no pre-loaded configuration. See Getting Started with ZTP on a Fresh Boot of a Router. See Zero Touch Provisioning on a Fresh Boot of a Router, on page 73
- **Manual Invocation:** Use this method when you want to forcefully initiate ZTP on a fully configured device. See Manual ZTP Invocation, on page 85.
- **ZTP Bootscript**: Use this method when you want to hard code a script to be executed on every boot. See Configure ZTP BootScript, on page 87 .

When to use Zero Touch Provisioning: Use Zero Touch Provisioning when the devices are in a secured network, but in an insecure network, we recommend you to Securely Provision Your Network Devices, on page 91.

Zero Touch Provisioning on a Fresh Boot of a Router

When you boot the device, the ZTP process initiates automatically if the device does not have a prior configuration.

During the process, the router verifies the list of sources and receives the information of the configuration file accordingly. The following are the sources that can provide the configuration file information.

- Removable storage: A directly attached removable storage device, for example, USB flash drive.
- DHCP server

Fresh Boot Using Removable Storage Device

You can automatically provision a network device using ZTP from a removable storage device such as a USB flash drive. The following are the configuration types available in a removable storage device:

- Device-specific configuration: The device-specific configuration is available in the folder that has a name matching the chassis serial number of the device. The sample path for the device-specific configuration is `/USB-path/xr-config/serial-number/router-cfg`. For example, `/USB-path/xr-config/FOC2102R1D0/router-cfg` `FOC2102R1D0` is the chassis serial number.
- Generic configuration: The generic configuration is available in the `xr-config` folder. The sample path for the generic configuration is./`USB-path/xr-config/router-cfg`

Here is the high-level work flow of the ZTP process using a USB flash drive:

1. When you boot the device, the device verifies if the USB is enabled in the `ztp.ini` file. By default, the USB fetcher is enabled and assigned the highest priority.

   Fetcher defines which port ZTP should use to get the provisioning details. By default, each port has a fetcher priority defined in the *ztp.ini* file.

2. ZTP checks for a USB flash drive on the device If the USB drive isn't available, the ZTP process moves to the next fetcher as defined in the fetcher priority of the `ZTP.ini` file.

3. If a USB flash drive is available, the device scans for the `xr-config` file in the root of the USB mount in the following sequence:

   a. The ZTP process first scans for the `router-cfg` file in the folder that is matching the chassis serial number of the device within the `xr-config` folder and applies the device-specific configuration.

      For example, `/USB-path/xr-config/FOC2102R1D0/router-cfg`

   b. If the device-specific configuration with a serial number isn't available, the ZTP process scans for the `router-cfg` file in the `xr-config` folder and applies a generic configuration.

   c. If the `xr-config` folder isn't available, the ZTP process moves to the next fetcher as defined in the fetcher priority of the `ZTP.ini` file.

4. The device applies the configuration.
5. The network device is now up and running.

Configure ZTP using USB

Follow these steps to configure ZTP using a USB flash drive:

1. Create the configuration file. See Build your Configuration File, on page 75.

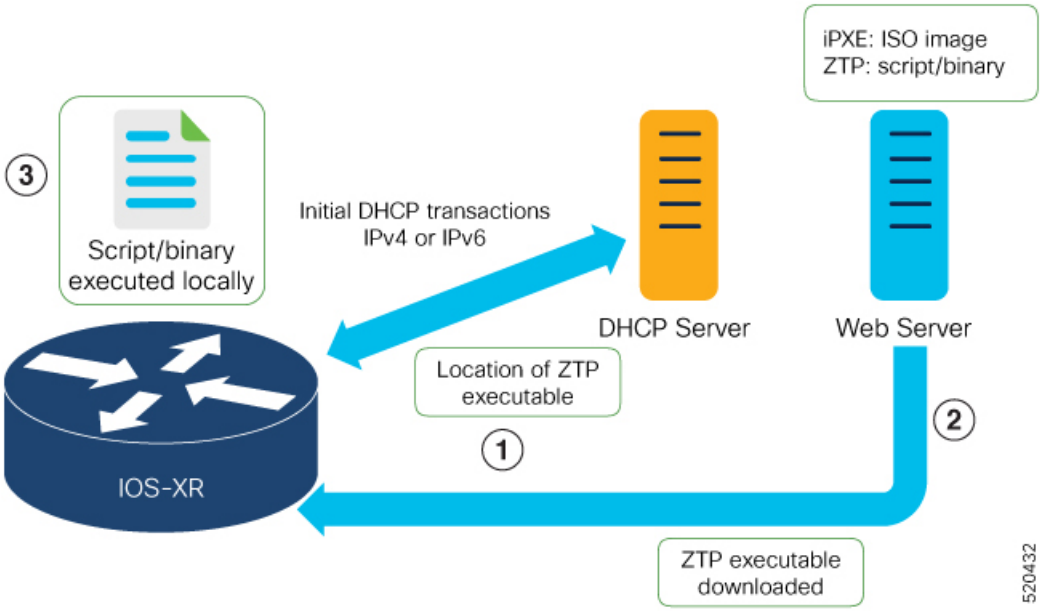
Note When you use a USB flash drive as a source for ZTP, you can't use the script file for provisioning. The scri file isn't supported for USB fetcher.

2. Copy the bootstrapping data to the USB flash drive and mount it on the device.

Fresh Boot Using DHCP

When you boot the device, the ZTP process initiates automatically if the device does not have a prior configuration. During the process, the router receives the details of the configuration file from the DHCP server.

This image depicts the high-level work flow of the ZTP process:



The ZTP process initiates when you boot the network-device with an IOS-XR image. The process starts only on the device that doesn't have a prior configuration.

Here is the high-level work flow of the ZTP process for the Fresh boot:

1. ZTP sends DHCP request to fetch the ZTP configuration file or user script. To help the Bootstrap server uniquely identify the device, ZTP sends below DHCP option

- DHCP(v4/v6) client-id=Serial Number
- DHCPv4 option 124: Vendor, Platform, Serial-Number
- DHCPv6 option 16: Vendor, Platform, Serial-Number

The following is the default sequential flow of the ZTP process:

- ZTP sends IPv4 DHCP request first on all the management port. In case there is a failure, then ZTP sends IPv6 DHCP request on all the management port.
- ZTP sends IPv4 DHCP request first on all the data port. In case there is a failure, then ZTP sends IPv6 DHCP request on all the data port.

  The default sequential flow is defined in configuration file and you can modify the sequence using the configuration file.

2. DHCP server identifies the device and responds with DHCP response using one of the following options:

   DHCP server should be configured to respond with the DHCP options.

   - DHCPv4 using BOOTP filename to supply script/config location.
   - DHCPv4 using Option 67 (bootfile-name) to supply script/config location.
   - DHCPv6 using Option 59 (OPT_BOOTFILE_URL) to supply script/config location
3. The network device downloads the file from the web server using the URI location that is provided in the DHCP response.
4. The device receives a configuration file or script file from the HTTP server.

   Note
   - If the downloaded file content starts with !! IOS XR it is considered as a configuration file.
   - If the downloaded file content starts with #! /bin/bash, #! /bin/sh or #!/usr/bin/python it is conside a script file.
5. The device applies the configuration file or executes the script or binary in the default bash shell.
6. The Network device is now up and running.

Build your Configuration File

Based on the business need, you can use a configuration or script file to initiate the ZTP process.

Note When you use a USB flash drive as a source for ZTP, you cannot use the script file for provisioning. The script file is not supported in the USB fetcher. Fetcher defines which port the ZTP process should use to get the provisioning details as defined in the `ztp.ini` file.

The configuration file content starts with *!! IOS XR* and the script file content starts with *#! /bin/bash, #! /bin/sh or #!/usr/bin/python.*

Once you create the configuration file, apply it to the device using the *ztp_helper* function *xrapply*.

The following is the sample configuration file:

```
!! IOS XR
username root
group root-lr
password 0 lablab
!

hostname ios
alias exec al show alarms brief system active

interface HundredGigE 0/0/0/24
ipv4 address 10.10.10.55 255.255.255.0
no shutdown
!
```

Create User Script

This script or binary is executed in the IOS-XR Bash shell and can be used to interact with IOS-XR CLI to configure, verify the configured state and even run exec commands based on the workflow that the operator chooses.

Build your ZTP script with either shell and python. ZTP includes a set of CLI commands and a set of shell utilities that can be used within the user script.

ZTP Shell Utilities

ZTP includes a set of shell utilities that can be sourced within the user script. `ztp_helper.sh` is a shell script that can be sourced by the user script. `ztp_helper.sh` provides simple utilities to access some XR functionalities. Following are the bash functions that can be invoked:

- **xrcmd**—Used to run a single XR exec command:`xrcmd "show running"`
- **xrapply**—Applies the block of configuration, specified in a file:

  ```
  cat >/tmp/config <<%%
  !! XR config example
  hostname node1-mgmt-via-xrapply
  %%
  xrapply /tmp/config
  ```

- **xrapply_with_reason**—Used to apply a block of XR configuration along with a reason for logging purpose:

  ```
  cat >/tmp/config <<%%
  !! XR config example
  hostname node1-mgmt-via-xrapply
  %%
  xrapply_with_reason "this is a system upgrade" /tmp/config
  ```

- **xrapply_string**—Used to apply a block of XR configuration in one line:

  ```
  xrapply_string "hostname foo\interface HundredGigE0/0/0/24\nipv4 address 1.2.3.44
  255.255.255.0\n"
  ```

- **xrapply_string_with_reason**—Used to apply a block of XR configuration in one line along with a reason for logging purposes:

```
xrapply_string_with_reason ”system renamed again" "hostname venus\n interface
HundredGigE0/0/0/24\n ipv4 address 172.30.0.144/24\n”
```

- **xrreplace**—Used to apply XR configuration replace in XR namespace via a file.

```
cat rtr.cfg <<%%
!! XR config example
hostname node1-mgmt-via-xrreplace
%%
xrreplace rtr.cfg
```

- **xrapply_with_extra_auth**—Used to apply XR configuration that requires authentication, in XR namespace via a file. The **xrapply_with_extra_auth** API is used when configurations that require additional authentication to be applied such as alias, flex groups.

```
cat >/tmp/config <<%%
!! XR config example
alias exec alarms show alarms brief system active
alias exec version run cat /etc/show_version.txt
%%
xrapply_with_extra_auth >/tmp/config
```

- **xrreplace_with_extra_auth**—Used to apply XR configuration replace in XR namespace via a file The **xrreplace_with_extra_auth** API is used when configurations that require additional authentication to be applied such as alias, flex groups

```
cat >/tmp/config <<%%
!! XR config example
alias exec alarms show alarms brief system active
alias exec version run cat /etc/show_version.txt
%%
xrreplace_with_extra_auth >/tmp/config
```

ZTP Helper Python Library

The ZTP python library defines a single Python class called `ZtpHelpers`. The helper script is located at `/pkg/bin/ztp_helper.sh`

ZtpHelpers Class Methods

Following are utility methods of the `ZtpHelpers` class:

- `init(self, syslog_server=None, syslog_port=None, syslog_file=None):`

```
__init__ constructor
:param syslog_server: IP address of reachable Syslog Server
       :param syslog_port: Port for the reachable syslog server
        :param syslog_file: Alternative or addon file for syslog
        :type syslog_server: str
        :type syslog_port: int
        :type syslog_file:str

         All parameters are optional. When nothing is specified during object creation,
 then all logs are sent to a log rotated file /tmp/ztp_python.log (max size of 1MB).
```

- `setns(cls, fd, nstype):`

```
Class Method for setting the network namespace
           :param cls: Reference to the class ZtpHelpers
           :param fd: incoming file descriptor
           :param nstype: namespace type for the sentns call
           :type nstype: int
                  0      Allow any type of namespace to be joined.
                  CLONE_NEWNET = 0x40000000 (since Linux 3.0)
                         fd must refer to a network namespace
```

- `get_netns_path(cls, nspath=None, nsname=None, nspid=None):`

```
Class Method to fetch the network namespace filepath
           associated with a PID or name
           :param cls: Reference to the class ZtpHelpers
           :param nspath: optional network namespace associated name
           :param nspid: optional network namespace associate PID
           :type nspath: str
           :type nspid: int
           :return: Return the complete file path
           :rtype:  str
```

- `toggle_debug(self, enable):`

```
Enable/disable debug logging
           :param enable: Enable/Disable flag
           :type enable: int
```

- `set_vrf(self, vrfname=None):`

```
Set the VRF (network namespace)
           :param vrfname: Network namespace name
                           corresponding to XR VRF
```

- `download_file(self, file_url, destination_folder):`

```
Download a file from the specified URL
           :param file_url: Complete URL to download file
           :param destination_folder: Folder to store the
                                      downloaded file
           :type file_url: str
           :type destination_folder: str
           :return: Dictionary specifying download success/failure
                    Failure => { 'status' : 'error' }
                    Success => { 'status' : 'success',
                                 'filename' : 'Name of downloaded file',
                                 'folder' : 'Directory location of downloaded file'}
           :rtype: dict
```

- `setup_syslog(self):`

  Method to Correctly set sysloghandler in the correct VRF (network namespace) and point to a remote syslog Server or local file or default log-rotated log file.

- `xrcmd(self, cmd=None):`

```
Issue an IOS-XR exec command and obtain the output
           :param cmd: Dictionary representing the XR exec cmd
                       and response to potential prompts
                       { 'exec_cmd': '', 'prompt_response': '' }
           :type cmd: dict
           :return: Return a dictionary with status and output
                    { 'status': 'error/success', 'output': '' }
           :rtype: dict
```

- xrapply(self, filename=None, reason=None):

```
Apply Configuration to XR using a file
           :param file: Filepath for a config file
                        with the following structure:
                        !
                        XR config command
                        !
                        end

           :param reason: Reason for the config commit.
                          Will show up in the output of:
                          "show configuration commit list detail"
           :type filename: str
           :type reason: str
           :return: Dictionary specifying the effect of the config change
                    { 'status' : 'error/success', 'output': 'exec command based on
status'}
                    In case of Error:  'output' = 'show configuration failed'
                    In case of Success: 'output' = 'show configuration commit changes
 last 1'
           :rtype: dict
```

- xrapply_string(self, cmd=None, reason=None):

```
Apply Configuration to XR using  a single line string
           :param cmd: Single line string representing an XR config command
           :param reason: Reason for the config commit.
                          Will show up in the output of:
                          "show configuration commit list detail"
           :type cmd: str
           :type reason: str
           :return: Dictionary specifying the effect of the config change
                    { 'status' : 'error/success', 'output': 'exec command based on
status'}
                    In case of Error:  'output' = 'show configuration failed'
                    In case of Success: 'output' = 'show configuration commit changes
 last 1'
           :rtype: dict
```

- xrreplace(self, filename=None):

```
Replace XR Configuration using a file

           :param file: Filepath for a config file
                        with the following structure:

                        !
                        XR config commands
                        !
                        end
           :type filename: str
           :return: Dictionary specifying the effect of the config change
                    { 'status' : 'error/success', 'output': 'exec command based on
status'}
                    In case of Error:  'output' = 'show configuration failed'
                    In case of Success: 'output' = 'show configuration commit changes
 last 1'
           :rtype: dict
```

Example

The following shows the sample script in phyton

```
[apple2:~]$ python sample_ztp_script.py

###### Debugs enabled ######


###### Change context to user specified VRF ######


###### Using Child class method, setting the root user ######

2016-12-17 04:23:24,091 - DebugZTPLogger - DEBUG - Config File content to be applied  !
                    username netops
                    group root-lr
                    group cisco-support
                    secret 5 $1$7kTu$zjrgqbgW08vEXsYzUycXw1
                    !
                    end
2016-12-17 04:23:28,546 - DebugZTPLogger - DEBUG - Received exec command request: "show
configuration commit changes last 1"
2016-12-17 04:23:28,546 - DebugZTPLogger - DEBUG - Response to any expected prompt ""
Building configuration...
2016-12-17 04:23:29,329 - DebugZTPLogger - DEBUG - Exec command output is ['!! IOS XR
Configuration version = 6.2.1.21I', 'username netops', 'group root-lr', 'group cisco-support',
 'secret 5 $1$7kTu$zjrgqbgW08vEXsYzUycXw1', '!', 'end']
2016-12-17 04:23:29,330 - DebugZTPLogger - DEBUG - Config apply through file successful,
last change = ['!! IOS XR Configuration version = 6.2.1.21I', 'username netops', 'group
root-lr', 'group cisco-support', 'secret 5 $1$7kTu$zjrgqbgW08vEXsYzUycXw1', '!', 'end']


###### Debugs Disabled ######


###### Executing a show command ######

Building configuration...
{'output': ['!! IOS XR Configuration version = 6.2.1.21I',
            '!! Last configuration change at Sat Dec 17 04:23:25 2016 by UNKNOWN',
            '!',
            'hostname customer2',
            'username root',
            'group root-lr',
            'group cisco-support',
            'secret 5 $1$7kTu$zjrgqbgW08vEXsYzUycXw1',
            '!',
            'username noc',
            'group root-lr',
            'group cisco-support',
            'secret 5 $1$7kTu$zjrgqbgW08vEXsYzUycXw1',
            '!',
            'username netops',
            'group root-lr',
            'group cisco-support',
            'secret 5 $1$7kTu$zjrgqbgW08vEXsYzUycXw1',
            '!',
            'username netops2',
            'group root-lr',
            'group cisco-support',
            'secret 5 $1$7kTu$zjrgqbgW08vEXsYzUycXw1',
            '!',
            'username netops3',
            'group root-lr',
            'group cisco-support',
            'secret 5 $1$7kTu$zjrgqbgW08vEXsYzUycXw1',
            '!',
```

```
            'cdp',
            'service cli interactive disable',
            'interface MgmtEth0/RP0/CPU0/0',
            'ipv4 address 11.11.11.59 255.255.255.0',
            '!',
            'interface TenGigE0/0/0/0/24',
            'shutdown',
            '!',
            'interface TenGigE0/0/0/0/25',
            'shutdown',
            '!',

            'router static',
            'address-family ipv4 unicast',
            '0.0.0.0/0 11.11.11.2',
            '!',
            '!',
            'end'],
 'status': 'success'}

###### Apply valid configuration using a file ######

Building configuration...
{'status': 'success', 'output': ['!! IOS XR Configuration version = 6.2.1.21I', 'hostname
customer', 'cdp', 'end']}

###### Apply valid configuration using a string ######

Building configuration...
{'output': ['!! IOS XR Configuration version = 6.2.1.21I',
            'hostname customer2',
            'end'],
 'status': 'success'}

###### Apply invalid configuration using a string ######

{'output': ['!! SYNTAX/AUTHORIZATION ERRORS: This configuration failed due to',
            '!! one or more of the following reasons:',
            '!!  - the entered commands do not exist,',
            '!!  - the entered commands have errors in their syntax,',
            '!!  - the software packages containing the commands are not active,',
```

For information on helper APIs, see https://github.com/ios-xr/iosxr-ztp-python#iosxr-ztp-python.

Set Up DHCP Server for ZTP

For ZTP to operate a valid IPv4 or IPv6 address is required and the DHCP server must send a pointer to the configuration script.

The DHCP request from the router has the following DHCP options to identify itself:

- **Option 60**: “vendor-class-identifier” : Used to Identify the following four elements:
  - The type of client: For example, PXEClient
  - The architecture of The system (Arch): For example: 00009 Identify an EFI system using a x86-64 CPU
  - The Universal Network Driver Interface (UNDI):

For example 003010 (first 3 octets identify the major version and last 3 octets identify the minor version)

- The Product Identifier (PID):

- **Option 61**: “dhcp-client-identifier” : Used to identify the Serial Number of the device.
- **Option 66** : Used to request the TFTP server name.
- **Option 67**: Used request the TFTP filename.
- **Option 97**: “uuid” : Used to identify the Universally Unique Identifier a 128-bit value (not usable at this time)

Example

The following DHCP request sample provides a fixed IP address and a configuration file with the mac address of the management interface.

```
host cisco-rp0 {
   hardware ethernet e4:c7:22:be:10:ba;
   fixed-address 172.30.12.54;
   filename "http://172.30.0.22/configs/cisco-1.config";
}
```

The following DHCP request sample provides a fixed IP address and a configuration file with the mac address of the management interface along with capability to re-image the system using iPXE (xr-config option):

```
host cisco-rp0 {
   hardware ethernet e4:c7:22:be:10:ba;
   fixed-address 172.30.12.54;
   if exists user-class and option user-class = "iPXE" {
      filename = "http://172.30.0.22/boot.ipxe";
   } elsif exists user-class and option user-class =  "xr-config" {
      filename = "http://172.30.0.22/scripts/cisco-rp0_ztp.sh";
   }
}
```

DHCP server identifies the device and responds with either an IOS-XR configuration file or a ZTP script as the filename option.

The DHCP server responds with the following DHCP options:

- DHCPv4 using BOOTP filename to supply script/config location.
- DHCPv4 using Option 67 (bootfile-name) to supply script/config location.
- DHCPv6 using Option 59 (OPT_BOOTFILE_URL) to supply script/config location

The following sample shows the DHCP response with bootfile-name (option 67):

```
option space cisco-vendor-id-vendor-class code width 1 length width 1;
option vendor-class.cisco-vendor-id-vendor-class code 9 = {string};

######### Network 11.11.11.0/24 ################
shared-network 11-11-11-0 {

####### Pools ##############
  subnet 11.11.11.0 netmask 255.255.255.0 {
    option subnet-mask 255.255.255.0;
 option broadcast-address 11.11.11.255;
 option routers 11.11.11.2;
```

```
 option domain-name-servers 11.11.11.2;
 option domain-name "cisco.local";
 # DDNS statements
   ddns-domainname "cisco.local.";
 # use this domain name to update A RR (forward map)
   ddns-rev-domainname "in-addr.arpa.";
   # use this domain name to update PTR RR (reverse map)

    }

######## Matching Classes ##########

  class "cisco" {
       match if (substring(option dhcp-client-identifier,0,11) = "FGE194714QS");
  }


  pool {
      allow members of "cisco";
      range 11.11.11.47 11.11.11.50;
      next-server 11.11.11.2;

      if exists user-class and option user-class = "iPXE" {
         filename="http://11.11.11.2:9090/cisco-mini-x-6.2.25.10I.iso";
      }


      if exists user-class and option user-class =  "xr-config"
       {
           if (substring(option vendor-class.cisco-vendor-id-vendor-class,19,99)="cisco")
           {
            option bootfile-name "http://11.11.11.2:9090/scripts/exhaustive_ztp_script.py";

           }
        }


      ddns-hostname "cisco-local";
      option routers 11.11.11.2;
  }
}
```

Important In Cisco IOS XR Release 7.3.1 and earlier, the system accepts the device sending **user-class = "exr-config"**; however starting Cisco IOS XR Release 7.3.2 and later, you must use only **user-class = "xr-config"**.

In Cisco IOS XR Release 7.3.2 and later, use:

```
host cisco-rp0 {
   hardware ethernet e4:c7:22:be:10:ba;
   fixed-address 172.30.12.54;
   if exists user-class and option user-class = "iPXE" {
      filename = "http://172.30.0.22/boot.ipxe";
   } elsif exists user-class and option user-class = "xr-config" {
      filename = "http://172.30.0.22/scripts/cisco-rp0_ztp.sh";
   }
}
```

Also, when upgrading from any release that is Cisco IOS XR Release 7.3.1 or earlier to Cisco IOS XR Release 7.3.2 or later release, use the following:

```
host cisco-rp0 {
   hardware ethernet e4:c7:22:be:10:ba;
   fixed-address 172.30.12.54;
   if exists user-class and option user-class = "iPXE" {
      filename = "http://172.30.0.22/boot.ipxe";
   } elsif exists user-class and option user-class = "exr-config" {
      filename = "http://172.30.0.22/scripts/cisco-rp0_ztp.sh";
   }
}
```

Authentication on Data Ports

On fresh boot, ZTP process is initiated from management ports and may switch to data ports. To validate the connection with DHCP server, authentication is performed on data ports through DHCP option 43 for IPv4 and option 17 for IPv6. These DHCP options are defined in option space and are included within **dhcpd.conf** and **dhcpd6.conf** configuration files. You must provide following parameters for authentication while defining option space:

- Authentication code—The authentication code is either 0 or 1; where 0 indicates that authentication is not required, and 1 indicates that MD5 checksum is required.
- Client identifier—The client identifier must be 'xr-config'.
- MD5 checksum—This is chassis serial number. It can be obtained using **echo -n $SERIALNUMBER | md5sum | awk '{print $1}'** .

Here is the sample **dhcpd.conf** configuration. In the example below, the option space called **VendorInfo** is defined with three parameters for authentication:

```
class "vendor-classes" {
   match option vendor-class-identifier;
}

option space VendorInfo;
option VendorInfo.clientId code 1 = string;
option VendorInfo.authCode code 2 = unsigned integer 8;
option VendorInfo.md5sum code 3 = string
option vendor-specific code 43 = encapsulate VendorInfo;
subnet 10.65.2.0 netmask 255.255.255.0 {
```

```
  option subnet-mask 255.255.255.0;
  option routers 10.65.2.1;
  range 10.65.2.1 10.65.2.200;
}
host cisco-mgmt {
   hardware ethernet 00:50:60:45:67:01;
   fixed-address 10.65.2.39;
   vendor-option-space VendorInfo;
   option VendorInfo.clientId  "xr-config";
   option VendorInfo.authCode 1;
   option VendorInfo.md5sum "aedf5c457c36390c664f5942ac1ae3829";
   option bootfile-name "http://10.65.2.1:8800/admin-cmd.sh";
}
```

Here is the sample **dhcpd6.conf** configuration file. In the example below, the option space called **VendorInfo** is defined that has code width 2 and length width 2 (as per dhcp standard for IPv6) with three parameters for authentication:

```
log-facility local7;
option dhcp6.name-servers 2001:1451:c632:1::1;
option dhcp6.domain-search "cisco.com";
dhcpv6-lease-file-name "/var/lib/dhcpd/dhcpd6.leases";
option dhcp6.info-refresh-time 21600;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.user-class code 15 = string;
option space CISCO-XR-CONFIG code width 2 length width 2;
option CISCO-XR-CONFIG.client-identifier code 1 = string;
option CISCO-XR-CONFIG.authCode code 2 = integer 8;
option CISCO-XR-CONFIG.md5sum code 3 = string;
option vsio.CISCO-XR-CONFIG code 9 = encapsulate CISCO-XR-CONFIG;
subnet6 2001:1451:c632:1::/64{
 range6 2001:1451:c632:1::2 2001:1451:c632:1::9;
 option CISCO-XR-CONFIG.client-identifier "xr-config";
 option CISCO-XR-CONFIG.authCode 1;
 #valid md5
 option CISCO-XR-CONFIG.md5sum "90fd845ac82c77f834d57a034658d0f0";
 if option dhcp6.user-class = 00:04:69:50:58:45 {
  option dhcp6.bootfile-url "http://[2001:1851:c632:1::1]/cisco-2/image.iso";
 }
 else {
   #option dhcp6.bootfile-url "http://[2001:1851:c632:1::1]/cisco-2/cisco-mini-x.iso.sh";
   option dhcp6.bootfile-url "http://[2001:1851:c632:1::1]/cisco-2/ztp.cfg";
  }
}
```

Manual ZTP Invocation

You can ZTP manually through Command Line Interface. This method is Ideal for verifying the ZTP configuration without a reboot. This manual way helps you to provision the router in stages. If you would like to invoke a ZTP on an interfaces (data ports or management port), you don't have to bring up and configure the interface first.

You can execute the ztp initiate command, even if the interface is down, ZTP script will bring it up and invoke dhclient. So ZTP could run over all interfaces no matter it is up or down.

Use the following commands to manually execute the ZTP commands to force ZTP to run over more interfaces:

- **ztp initiate** — Invokes a new ZTP DHCP session. Logs can be found in **/disk0:/ztp/ztp.log**.

  Configuration Example:

```
Router#ztp initiate debug verbose interface HundredGigE 0/0/0/24
Invoke ZTP? (this may change your configuration) [confirm] [y/n] :
```

- **ztp terminate** —Terminates any ZTP session in progress.

  Configuration Example:

  ```
  Router #ztp terminate verbose
  Mon Oct 10 16:52:38.507 UTC
  Terminate ZTP? (this may leave your system in a partially configured state) [confirm]
  [y/n] :y
  ZTP terminated
  ```

- **ztp enable** —Enables the ZTP at boot.

  Configuration Example:

  ```
  Router#ztp enable
  Fri Jul 12 16:09:02.154 UTC
  Enable ZTP? [confirm] [y/n] :y
  ZTP Enabled.
  ```

- **ztp disable** —Disables the ZTP at boot.

  Configuration Example:

  ```
  Router#ztp disable
  Fri Jul 12 16:07:18.491 UTC
  Disable ZTP? [confirm] [y/n] :y
  ZTP Disabled.
  Run ZTP enable to run ZTP again.
  ```

- **ztp clean** —Removes only the ZTP state files.

  Configuration Example:

  ```
  Router#ztp clean verbose
  Mon Oct 10 17:03:43.581 UTC
  Remove all ZTP temporary files and logs? [confirm] [y/n] :y
  All ZTP files have been removed.
  If you now wish ZTP to run again from boot, do 'conf t/commit replace' followed by
  reload.
  ```

  The log file ztp.log is saved in **/var/log** folder, and a copy of log file is available at **/disk0:/ztp/ztp.log** location using a soft link. However, executing **ztp clean** clears files saved on disk and not on **/var/log** folder where current ZTP logs are saved. In order to have a log from current ZTP run, you must manually clear the ZTP log file from **/var/log/** folder.

Configuration

This task shows the most common use case of manual ZTP invocation: invoke ZTP.

1. Invoke DHCP sessions on all data ports which are up or could be brought up. ZTP runs in the background. Use show logging or look at /disk0:/ztp/ztp.log to check progress.

Configuration Example:

```
Router# ztp initiate dataport
```

Configure ZTP BootScript

If you want to hard code a script to be executed every boot, configure the following.

```
Router#configure
Router(config)#ztp bootscript /disk0:/myscript
Router(config)#commit
```

The above configuration will wait for the first data-plane interface to be configured and then wait an additional minute for the management interface to be configured with an IP address, to ensure that we have connectivity in the third party namespace for applications to use. If the delay is not desired, use:

```
Router#configure
Router(config)#ztp bootscript preip /disk0:/myscript
Router(config)#commit
```

Note When the above command is first configured, you will be prompted if you wish to invoke it now. The prompt helps with testing.

This is the example content of **/disk0:/myscript**:

```
#!/bin/bash
exec &> /dev/console # send logs to console
source /pkg/bin/ztp_helper.sh

# If we want to only run one time:
xrcmd "show running" | grep -q myhostname
if [[ $? -eq 0 ]]; then
    echo Already configured
fi

# Set the hostname
cat >/tmp/config <<%%
!! XR config example
hostname myhostname
%%
xrapply /tmp/config

#
# Force an invoke of ZTP again. If there was a username normally it would not run. This
forces it.
# Kill off ztp if it is running already and suppress errors to the console when ztp runs
below and
# cleans up xrcmd that invokes it. ztp will continue to run however.
#
xrcmd "ztp terminate noprompt" 2>/dev/null
xrcmd "ztp initiate noprompt" 2>/dev/null
```

Customize the ZTP Configurable Options

You can customize the following ZTP configurable options in the *ztp.ini* file:

- `ZTP`: You can enable or disable ZTP at boot using CLI or by editing the *ztp.ini* file.

- `Retry`: Set the ZTP DHCP retry mechanism: The available values are infinite and once.
- `Fetcher Priority`: Fetcher defines which port ZTP should use to get the provisioning details. By default, each port has a fetcher priority defined in the *ztp.ini* file. You can modify the default priority of the fetcher. Allowed range is from 0 to 9.

Note Lower the number higher the priority. The value 0 has the highest priority and 9 has the lowest priority.

By default, the USB port has the higher priority.

In the following example, the Mgmt4 port has the highest priority:

```
[Fetcher Priority]
Mgmt4: 0
Mgmt6: 1
DPort4: 2
DPort6: 3
```

- `progress_bar`: Enable progress bar on the console. By default, the progress bar is disabled. To enable the progress bar, add the following entry in the `ztp.ini` file.

```
[Options]
progress_bar: True
```

By default, the `ztp.ini` file is located in the `/pkg/etc/` location. To modify the ZTP configurable options, make a copy of the file in the `/disk0:/ztp/` directory and then edit the `ztp.ini` file.

To reset to the default options, delete the ztp.ini file in the `/disk0:/ztp/` directory.

Note Do not edit or delete the `ztp.ini` file in the `/pkg/etc/` location to avoid issues during installation.

The following example shows the sample of the `ztp.ini` file:

```
[Startup]
start: True
retry_forever: True

[Fetcher Priority]
USB: 0

Mgmt4:  1
Mgmt6:  2
DPort4: 3
DPort6: 4
```

Enable ZTP Using CLI

If you want to enable ZTP using CLI, use the **ztp enable** command.

Configuration example

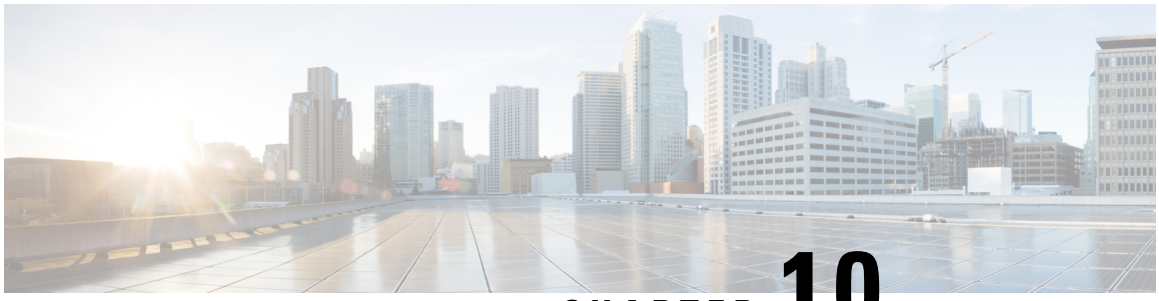
```
Router#ztp enable
Fri Jul 12 16:09:02.154 UTC
Enable ZTP? [confirm] [y/n] :y
ZTP Enabled.
```

Disable ZTP Using CLI

If you want to disable ZTP using CLI, use the **ztp disable** command.

Configuration example

```
Router#ztp disable
Fri Jul 12 16:07:18.491 UTC
Disable ZTP? [confirm] [y/n] :y
ZTP Disabled.
Run ZTP enable to run ZTP again.
```



CHAPTER 10

Securely Provision Your Network Devices

With Secure Zero Touch Provisioning, you can securely and seamlessly provision thousands of network devices accurately within minutes and without any manual intervention.

Table 4: Feature History Table

Feature	Release Information	Feature Description
Secure Zero Touch Provisioning with Removable Storage Device	Release 7.3.2	This feature allows you to securely sign onboarding data in a removable storage device so that you can use the device for secure ZTP operations. This support gives you the plug-and-play flexibility for ZTP without any additional infrastructure requirements.
Secure Zero Touch Provisioning	Release 7.3.1	This feature allows devices in the network to establish a secure connection with the ZTP server and authenticate information using a three-step validation process involving validation of the network device, the ZTP server, and onboarding information. This eliminates security risks or malicious actions during remote provisioning. The **ztp secure-mode enable** command is introduced.

In a secured network such as datacenter, the zero-touch provisioning mechanism helps you provision hundreds of remote devices without your intervention. But, the access devices are typically in an insecure network. There is a high risk of malicious actions on the device, such as adding an unauthorized or infected device. Security is a critical aspect while remotely provisioning the network devices.

Secure ZTP combines seamless automation with security. Network devices can securely establish a connection with the ZTP server and authenticate the onboarding information that it receives. The process eliminates any security risks or malicious actions during the provisioning of remote devices.

- ZTP helps you remotely provision a router securely anywhere in the network. Thus, eliminate the risk of malicious attacks or unauthorized ownership claims.
- Secure ZTP authenticates not only the onboarding network device but also validates the server authenticity and provisioning information that it is receiving from the ZTP server.

The following are the topics covered in this chapter:

Onboarding Devices Using Three-Step Validation

The Cisco IOS XR software implements the secure zero touch provisioning capabilities as described in RFC 8572. Secure ZTP uses a three-step validation process to onboard the remote devices securely:

1. **Router Validation**: The ZTP server authenticates the router before providing bootstrapping data using the Trust Anchor Certificate (also called SUDI certificate).
2. **Server Validation**: The router device in turn validates the ZTP server to make sure that the onboarding happens to the correct network. Upon completion, the ZTP server sends the bootstrapping data (for example, a YANG data model) or artifact to the router. See Secure ZTP Components , on page 92.
3. **Artifact Validation**: The configuration validates the bootstrapping data or artifact received from the ZTP server.

Secure ZTP Components

Let's first understand the components required for secure ZTP.

Table 5: Components used in Secure ZTP

Components	Description
Onboarding Device (Router)	The router is a Cisco device that you want to provision and connect to your network. Secure ZTP is supported only on platforms that have Hardware TAM support. Routers with HW TAM have the SUDI embedded in TAM.
DHCP Server	The secure ZTP process relies on the DHCP server to provide the URL to access the bootstrapping information.

Components	Description

ZTP Server	A ZTP server is any server used as a source of secure ZTP bootstrapping data and can be a RESTCONF or HTTPs server.
	Note Currently, ZTP only supports single name-server. When the DHCP server has more than one server address configured, ZTP fails to apply the server configuration.
	The ZTP server contains the following artifacts:
	• Cisco IOS XR software images: You can download Cisco images, SMU, and patches using the Cisco Support & Downloads page.
	• ZTP scripts: Contains the following libraries and you can build a script to initiate the ZTP process. See Build your Configuration File, on page 75.
	  • Python library: Includes IOS XR CLI (show commands and configuration commands) and YANG-XML (ncclient, native Netconf client).
	  • BASH library: Includes IOS XR CLI show commands, configuration commands
	• Bootstrapping Data

Components	Description
Bootstrapping Data	

Components	Description

	Bootstrapping data is the collection of data that the router obtains from the ZTP server during the secure ZTP process. You must create and upload the bootstrapping data in the ZTP server. For more information, refer RFC 8572.
	• The bootstrapping data mainly has three artifacts:
	• **Conveyed Information**: Conveyed Information contains the required bootstrapping data for the device. It contains either the redirect information or onboarding information to provision the device.
	For example:
	`module: ietf-sztp-conveyed-info`
	`yang-data conveyed-information: +-- (information-type)`
	`+--:(redirect-information) | +-- redirect-information | +-- bootstrap-server* [address] | +-- address inet:host | +-- port? inet:port-number | +-- trust-anchor? cms`
	`+--:(onboarding-information) +-- onboarding-information +-- boot-image | +-- os-name? string | +-- os-version? string | +-- download-uri* inet:uri | +-- image-verification* [hash-algorithm] | +-- hash-algorithm identityref | +-- hash-value yang:hex-string +-- configuration-handling? enumeration +-- pre-configuration-script? script +-- configuration? binary +-- post-configuration-script? script`

Components	Description

	• **Redirect Information**: Redirect information is used to redirect a device to another bootstrap server. The redirect information contains a list of bootstrap servers along with a hostname, an optional port, and an optional trust anchor certificate that the device uses to authenticate the bootstrap server.
	For Example:
	`{`
	`"ietf-sztp-conveyed-info:redirect-information" : {`
	`"bootstrap-server" : [`
	`{`
	`"address" : "sztp1.example.com",`
	`"port" : 8443,`
	`"trust-anchor" : "base64encodedvalue=="`
	`},`
	`{`
	`"address" : "sztp2.example.com",`
	`"port" : 8443,`
	`"trust-anchor" : "base64encodedvalue=="`
	`},`
	`{`
	`"address" : "sztp3.example.com",`
	`"port" : 8443,`
	`"trust-anchor" : "base64encodedvalue=="`
	`}`
	`]`
	`}`
	`}`

Components	Description
	• **Onboarding Information:** Onboarding information provides data necessary for a device to bootstrap itself and establish secure connections with other systems. It specifies details about the boot image, an initial configuration the device must commit, and scripts that the device must execute. For Example: `{ "ietf-sztp-conveyed-info:onboarding-information" : { "boot-image" : { "os-name" : "VendorOS", "os-version" : "17.2R1.6", "download-uri" : ["https://example.com/path/to/image/file"], "image-verification" : [{ "hash-algorithm" : "ietf-sztp-conveyed-info:sha-256", "hash-value" : "ba:ec:cf:a5:67:82:b4:10:77:c6:67:a6:22:ab:\ 7d:50:04:a7:8b:8f:0e:db:02:8b:f4:75:55:fb:c1:13:b2:33" }] }, "configuration-handling" : "merge", "pre-configuration-script" : "base64encodedvalue==", "configuration" : "base64encodedvalue==", "post-configuration-script" : "base64encodedvalue==" } }`

Components	Description
	• **Owner Certificate**: The owner certificate is installed on the router with the public key of your organization. The router uses the owner certificate to verify the signature in the conveyed information artifact using the public key that is available in the owner certificate. • **Ownership Voucher**: Ownership Voucher is used to identify the owner of the device by verifying the owner certificate that is stored in the device. Cisco supplies Ownership Voucher in response to your request. You must submit the Pinned Domain Certificate and device serial numbers with the request. Cisco generates and provides the Ownership Voucher to you.

Components	Description

Report Progress	When the device obtains the onboarding information from a ZTP server, the router reports the bootstrapping progress to the ZTP server using the API calls.
	See RFC 8572 for the detailed report-progress messages that can be sent to the ZTP server.
	The following is the structure of the `report-progress` sent the progress message to a ZTP server.
	`+---x report-progress {onboarding-server}?`
	`+---w input`
	`+---w progress-type enumeration`
	`+---w message? string`
	`+---w ssh-host-keys`
	`+---w ssh-host-key* []`
	`+---w algorithm string`
	`+---w key-data binary`
	`+---w trust-anchor-certs`
	`+---w trust-anchor-cert* cms`
	The following example illustrates a device using the Yang module to post a progress report to a ZTP server with a `bootstrap complete` message:
	`{`
	`'progress-type': 'bootstrap-complete',`
	`'message': 'example message',`
	`'trust-anchor-certs': [{`
	`'trust-anchor-cert': 'base64encodedvalue=='`
	`'ssh-host-keys': [{`
	`'key-data': 'base64encodedvalue==',`
	`'algorithm': 'ssh-rsa'`
	`}, {`
	`'key-data': 'base64encodedvalue==',`
	`'algorithm': 'rsa-sha2-256'`
	`}]`
	`}`
	`RESPONSE from the ZTP server`
	`HTTP/1.1 204 No Content`
	`Date: Sat, 31 Oct 2015 17:02:40 GMT`
	`Server: example-server`

Secure Zero Touch Provisioning

When you boot the device, the secure ZTP process initiates automatically if the device does not have a prior configuration.

During the process, the router verifies the list of sources and receives the information of the configuration file accordingly. The following are the sources that can provide the configuration file information.

- Removable storage: A directly attached removable storage device, for example, USB flash drive.
- DHCP server

The section covers the following topics:

Secure ZTP with Removable Storage Device

A Removable storage device such as a USB drive is an untrusted source of bootstrapping data. So, the onboarding information present in the removable storage device must always be signed.

Whenever the data is signed, it's mandatory that the Owner Certificate and Ownership Voucher must also be available. The removable storage device must contain the following three artifacts. For more information on the three artifacts, see Secure ZTP Components , on page 92.

- Conveyed Information
- Owner Certificate
- Ownership Voucher

This section covers the following topics:

Prepare Removable Storage Device to Provision Secure ZTP

The network administrator performs the following tasks as part of the initial setup for secure ZTP:

Before performing the following tasks, ensure to enable secure ZTP on the router using the **ztp secure-mode enable** command and then reload the router.

1. Contact Cisco Support to obtain a voucher. Provide the following details to request for ownership voucher certificate:
   - Pinned Domain certificate (PDC): PDC is an X.509 v3 certificate structure that uses Distinguished Encoding Rules (DER). This certificate is used by the router to trust a public key infrastructure in order to verify a domain certificate supplied to the router separately in the bootstrapping data. This certificate could be an end-entity certificate, including a self signed entity.
   - Order details with the Serial numbers of the routers

   For example,

   ```
   {
          "expires-on": "2016-10-21T19:31:42Z",
          "assertion": "verified",
          "serial-number": "JADA123456789",
          "idevid-issuer": "base64encodedvalue==",
          "pinned-domain-cert": "base64endvalue==",
          "last-renewal-date": "2017-10-07T19:31:42Z"
      }
   ```

2. Copy the following data to the removable storage device in the **EN9** directory in its root:
   - Conveyed information: Conveyed information must be named as `conveyed-information.cms` and must contain only the onboarding information and not the redirect information.

- Onboarding Information: The conveyed information consists of the following onboarding information:
  - Cisco IOS XR software images: You can download Cisco images, SMU, and patches using the Cisco Support & Downloads page.
    a. Click **Routers** and select the product that you want to download the image for.
    b. On the product home page, select the required Product model from the **Downloads** tab.
    c. From the **Software Available For This Product** page, download the required Cisco image, SMU, and patches.
  - ZTP scripts that include IOS XR configurations, pre, and post configuration scripts.

    During the secure ZTP process, secure ZTP executes the scripts to provision the router. You can build your script using one of the following methods:
    a. Python library: Includes IOS XR CLI (show commands and configuration commands) and YANG-XML (`ncclient`, `native Netconf client`).
    b. BASH library: Includes IOS XR CLI show commands, configuration commands.

    See Build your Configuration File, on page 75.

- Owner certificate: The owner certificate must be named as `owner-certificate.cms`.
- Ownership vouchers: The ownership vouchers must be named as `ownership-voucher.vcj`.

The artifacts must be stored inside the subdirectory named after the RP serial number of the router.The following example shows a directory structure for the router with RP serial number `FOC2202R293` containing all three artifacts:

```
EN9
└── FOC2202R293
    └── bootstrapping-data
        ├── conveyed-information.cms
        ├── owner-certificate.cms
        └── ownership-voucher.vcj
```

3. Plug in the removable storage device into the router.
4. Power on the router.

How Does Secure ZTP Work with Removable Storage Device?

Before you begin, complete the task to prepare the removable storage device. See Prepare Removable Storage Device to Provision Secure ZTP, on page 100.

Here is the high-level workflow of the Secure ZTP process using a removable storage device:

1. When you boot the device with an IOS-XR image, the secure ZTP process verifies if the secure ZTP mode (`secure-ztp mode`) is enabled. If not enabled, the device boots normally.
2. The device verifies if the USB is enabled in the `ztp.ini` file. By default, the USB is enabled and assigned the highest priority in the fetcher priority in the `ztp.ini` file.

Fetcher priority defines how secure ZTP can get the provisioning details. By default, each port has a fetcher priority defined in the `ztp.ini` file. The fetcher priority range is from 0 to 9. The lower the number higher is the priority. The value 0 has the highest priority and 9 has the lowest priority. For more information, see Customize the ZTP Configurable Options, on page 87.

The following example shows the sample of the `ztp.ini` file:

```
[Startup]
start: True
retry_forever: True

[Fetcher Priority]
USB: 0

Mgmt4:  1
Mgmt6:  2
DPort4: 3
DPort6: 4
```

3. Secure ZTP checks for a removable storage device on the router. If the removable storage device isn't available, the secure ZTP process moves to the next fetcher as defined in the fetcher priority of the `ztp.ini`file.
4. If a removable storage device is available, the router scans for the `EN9` directory in the root of the removable storage device.

   If the `EN9` directory isn't available, the secure ZTP process moves to the next fetcher as defined in the fetcher priority of the `ztp.ini`file.
5. **Artifact Validation**:

   The router validates the artifacts received from the removable storage device.

   a. The router validates the ownership voucher and extracts the `pinned-domain-cert` node, an X.509 certificate from the ownership voucher to verify the owner certificate.

   b. The router authenticates the owner certificate by performing the X.509 certificate path verification process on the trusted certificate.

   c. Finally, the router verifies whether the conveyed information artifact is signed by the validated owner certificate.
6. **Provision the router**:

   a. The device first processes the boot image information.

   b. Executes the preconfiguration script and then commits the initial configuration.

   c. Execute the post configuration script.
7. After the onboarding process is completed, router is operational.

Note If there is a failure in any of the steps, the secure ZTP process moves to the next fetcher as defined in the fetcher priority of the `ztp.ini` file.

Secure ZTP with DHCP

When you boot the device, the ZTP process initiates automatically if the device does not have a prior configuration. During the process, the router receives the details of the configuration file from the DHCP server.

This section covers the following topics:

Initial Set Up for Secure ZTP

The network administrator performs the following tasks as part of the initial setup for secure ZTP:

1. Contact Cisco Support to obtain a voucher. Provide the following details to request for ownership voucher certificate:
   - Pinned Domain Certificate: A trusted digital certificate issued by the Certificate Authority (CA) and pinned by the operator.
   - Order details with the Serial numbers of the routers
   - For example,

```
{
        "expires-on": "2016-10-21T19:31:42Z",
        "assertion": "verified",
        "serial-number": "JADA123456789",
        "idevid-issuer": "base64encodedvalue==",
        "pinned-domain-cert": "base64endvalue==",
        "last-renewal-date": "2017-10-07T19:31:42Z"
    }
```

2. Upload the following bootstrapping data to the ZTP server. Steps to upload may vary depending on the server that you're using, refer to the documentation provided by your vendor.
   - Cisco IOS XR software images: You can download Cisco images, SMU, and patches using the Cisco Support & Downloads page.
   - ZTP scripts that include IOS XR configurations, pre, and post configuration scripts. Build a script to initiate the ZTP process. See Build your Configuration File, on page 75.
     - Python library: Includes IOS XR CLI (show commands and configuration commands) and YANG-XML (`ncclient`, `native Netconf client`).
     - BASH library: Includes IOS XR CLI show commands, configuration commands
   - Serial numbers of the routers you plan to onboard using ZTP
   - Owner certificates
   - Pinned Domain Certificate (PDC)
   - Ownership vouchers
3. Set up the DHCP server to provide the redirect URL to the router:

   Before triggering the secure ZTP process, configure the DHCP server to provide the location of the IOS-XR image to the router. For information on how to configure the DHCP server, see your DHCP server documentation.

Configure the following parameters in the DHCP server:

- `option-code`: The DHCP SZTP redirect Option has the following parameters:
  - OPTION_V4_SZTP_REDIRECT (143): Use this DHCP v4 code for IPV4.
  - OPTION_V6_SZTP_REDIRECT (136): Use this DHCP v4 code for IPV6.

  For example, `option dhcp6.bootstrap-servers code 136 = text;`
- `option-length`: The option length in octets
- `bootstrap-servers`: A list of servers for the onboarding device to contact the servers for the bootstrapping data.
- `bootfile-url` : The URI of the SZTP bootstrap server should use the HTTPS URI scheme and it should be in the following format:

  `"https://<ip-address-or-hostname>[:<port>]".`

4. Power on the router.
5. Enable the secure ZTP option on the onboarding device. Execute the following command on your router to enable secure ZTP:

```
Router# ztp secure-mode enable
```

How Does Secure ZTP Work?

Before you begin, ensure that you configure the network with the DHCP and ZTP server. See Initial Set Up for Secure ZTP, on page 103.

1. When you boot the device with an IOS-XR image, the secure ZTP process verifies if the secure ZTP mode (`secure-ztp mode`) is enabled. If not enabled, the device boots normally.

   Note When `secure-ztp mode` is enabled, the ZTP process accepts only the `secure-redirect-URL` and ignores t presence of boot file name option from the DHCP response.

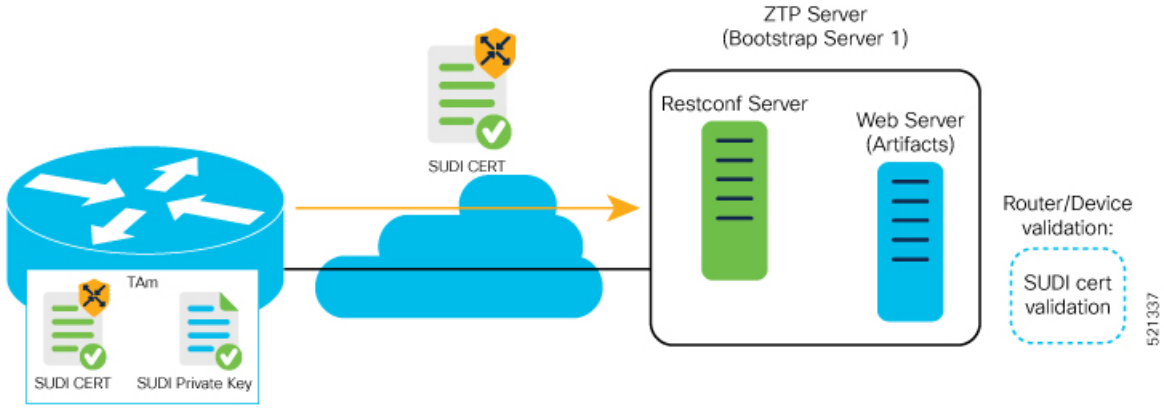
2. **DHCP discovery**:
   a. The router initiates a DHCP request to the DHCP server.
   b. The DHCP server responds with a DHCPv4 143 address option (for IPv4 addressing) or a DHCPv6 136 option (for IPv6 addressing). In addition, URLs to access bootstrap servers for further configuration is also listed.

Figure 5: DHCP discovery

3. **Router validation**:

   a. After receiving the URL from the DHCP server, the router sends an HTTPs request to the RESTCONF or HTTPs server using the specified URL. Along with the HTTPs request, the device sends the client certificate that is provided by the manufacturer (also called SUDI certificate). This certificate identifies and authenticates itself to the ZTP server.

   Figure 6: Router Validation



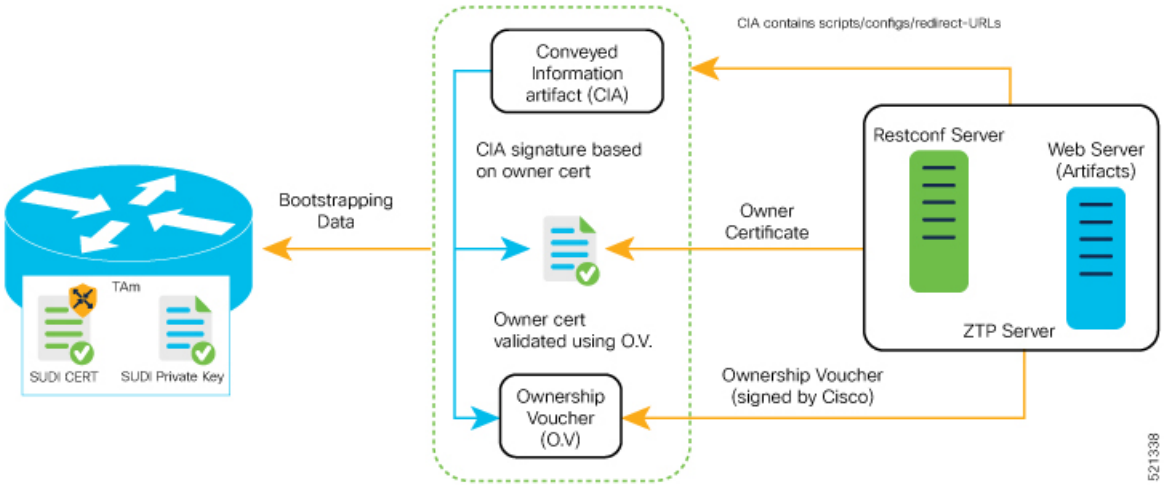
   b. The RESTCONF or HTTPs server verifies the received SUDI certificate with the public certificate that it contains. Cisco issues the public certificate to ensure that the onboarding device is an authorized Cisco device.

   c. After the onboarding device is authenticated, the web server sends the required artifacts along with the secure ZTP yang model to the onboarding device.

4. **Server validation** :

   The router receives the yang model that contains Owner Certificate, Ownership Voucher, and Conveyed Information artifact. The router verifies the ownership voucher by validating its signature to one of its preconfigured trusts anchors and downloads the image. When the router obtains the onboarding information, it reports the bootstrapping progress to the ZTP server. See RFC 8572 for the progress information.

Figure 7: Server Validation



5. **Artifact Validation**:

   The router validates the artifact received from the ZTP server.

   a. The device extracts the `pinned-domain-cert` node, an X.509 certificate from the ownership voucher to verify the owner certificate.

   b. The device authenticates the owner certificate by performing the X.509 certificate path verification process on the trusted certificate.

   c. Finally, the device verifies whether the conveyed information artifact is signed by the validated owner certificate.

6. **Provision the device**:

   a. The device first processes the boot image information.

   b. Executes the pre-configuration script and then commits the initial configuration

   c. Execute the post configuration script.

7. After the onboarding process is completed, the network device is operational.

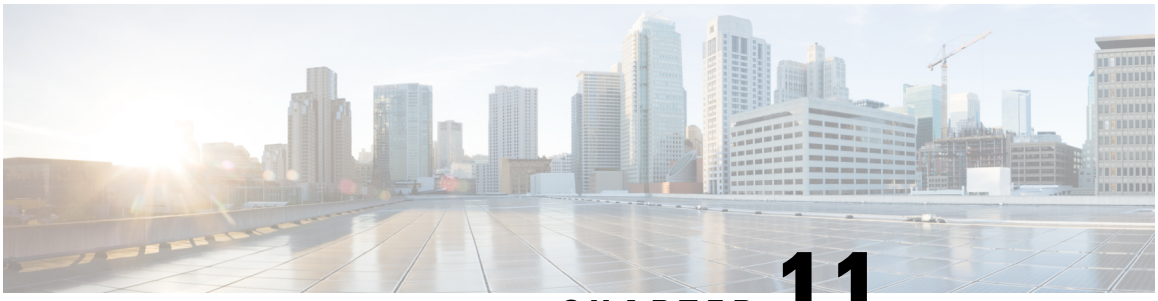
The following figure illustrates the end-to-end sequence of the Secure ZTP process:

Figure 8: End-to-end sequence of the Secure ZTP process

Disable Secure ZTP

Execute the following commands to disable the secure ZTP:

```
Router# request consent-token generate-challenge secure-ztp auth-timeout 15
Router# request consent-token accept-challenge secure-ztp
```



CHAPTER 11

Disaster Recovery

The topics covered in this chapter are:

Boot using USB Drive

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

Create a Bootable USB Drive Using Compressed Boot File

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

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

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

Before you begin

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

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

- Copy the compressed boot file from the software download page at cisco.com to your local machine. The file name for the compressed boot file is in the format *ncs5500-usb-boot-<release_number>.zip*.

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

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

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

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

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

Step 5 Eject the USB drive from your local machine.

What to do next

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

Boot the Router Using USB

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

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

Before you begin

Create a bootable USB drive. See Create a Bootable USB Drive Using Compressed Boot File, on page 109.

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

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

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

a. Insert the USB drive.

b. Connect to the console.

c. Power the router.

d. Press **Esc** or **Del** to pause the boot process and get the RP to BIOS menu.

e. Select the USB from the boot menu on the RP to which the USB is connected to. The RP boot the image from USB and installs the image onto the hard disk. The router boots from the hard disk after installation.

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

What to do next

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

Boot the Router Using iPXE

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

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

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

Zero Touch Provisioning

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

ZTP auto provisioning involves:

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

Setup DHCP Server

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

Before you begin

- Consult your network administrator or system planner to procure IP addresses and a subnet mask for the management interface.
- Physical port Ethernet 0 on RP is the management port. Ensure that the port is connected to management network.
- Enable firewall to allow the server to process DHCP packets.
- For DHCPv6, a Routing advertisement (RA) message must be sent to all nodes in the network that indicates which method to use to obtain the IPv6 address. Configure Router-advertise-daemon (radvd, install using yum install radvd) to allow the client to send DHCP request. For example:

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

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

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

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

- Use MAC address of the router:

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

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

Ensure that the above configuration is successful.

- Use serial number of the router:

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

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

Step 3 Restart DHCP.

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

Example

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

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

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

```
option dhcp6.name-servers <ip-address-server>;
option dhcp6.domain-search "cisco.com";
dhcpv6-lease-file-name "/var/db/dhcpd6.leases";
option dhcp6.info-refresh-time 21600;
option dhcp6.bootfile-url code 59 = string;
subnet6 <subnet> netmask <netmask> {
```

```
range6 2001:1851:c622:1::2 2001:1851:c622:1::9;
 option dhcp6.bootfile-url "http://<address>/<path>/<image.bin>";
```

What to do next

Invoke ZTP.

Invoke ZTP

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

Before you begin

Ensure that a DHCP server is setup. For more information, see Setup DHCP Server, on page 112.

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

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

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

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

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

Invoke ZTP Manually

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

Before you begin

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

```
#
# List all the interfaces that ZTP will consider running on. ZTP will attempt
# to bring these interfaces. At which point dhclient will be able to use them.
```

```
#
# Platforms may add dynamically to this list.
#
#ZTP_DHCLIENT_INTERFACES=" \
#    Gi0_0_0_0 \
#"
...
```

Step 1 Boot the router.

Step 2 Login manually.

Step 3 Enable interfaces.

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

```
Router#ztp initiate
```

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

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

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

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

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

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

To override the prompt:

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

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

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

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

What to do next

Boot the router using iPXE.

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

Boot the Router Using iPXE

Before you use the iPXE boot, ensure that:

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

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

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

Example:

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

The following example shows the output of the command:

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


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

Disaster Recovery Using Manual iPXE Boot

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

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

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

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

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

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

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

Example:

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

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

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

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

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

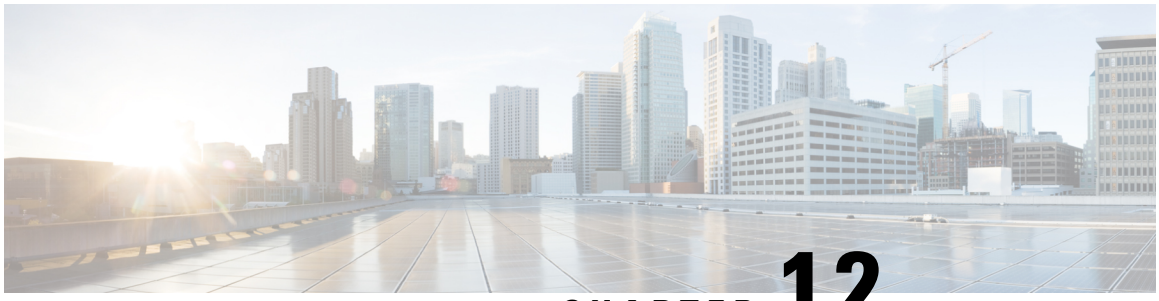
iPXE also supports HTTP, TFTP and FTP. For more information, see https://ipxe.org/cmd.

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

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

PART II

Setup System and Install IOS XR7 Software



CHAPTER 12

Setup Cisco NCS 5700 Series Routers with XR7 OS

The Cisco Network Convergence System 5700 Series builds on the Cisco NCS 5500 fixed systems by combining the forwarding ASIC design with the Cisco IOS XR7 OS. The Cisco NCS 5700 series chassis is a standalone 1RU router that offers aggregation, distributed core and peering fabric, and 100G Top of Rack (ToR).

The following variants of Cisco NCS 5700 series router run on XR7 OS:

- NCS-57B1-6D24-SYS
- NCS-57B1-5DSE-SYS

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

This document helps you set up the Cisco NCS 5700 series router with XR7 OS. You will bring-up the router, run a health check of the system, create user profiles, and assign privileges.

- Bring-up the Cisco Series Router, on page 121
- Perform Preliminary Checks with Cisco Router, on page 127
- Create Users and Assign Privileges on Cisco NCS 5700 Series Router, on page 132

Bring-up the Cisco Series Router

Connect to the console port 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 6: 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.

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 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 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>5700-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]
```

Boot the Cisco 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 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.

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:

- **Boot menu**

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 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 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
```

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.

Configure the Management Port on the Cisco 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 Place the interface in `UP` state.

Example:

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

Step 7 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 8 Commit the configuration.

Example:

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

Step 9 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 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 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 7.3.1 LNT
Copyright (c) 2013-2021 by Cisco Systems, Inc.
Build Information:
Built By :   xyz
Built On :   Tue Feb 09 19:43:44 UTC 2021
Build Host : iox-lnx-064
Workspace :  ../ncs5700/ws
Version :    7.3.1
Label :      7.3.1
cisco NCS5700 (D-1563N @ 2.00GHz)
cisco NCS-57B1-5DSE-SYS (D-1563N @ 2.00GHz) processor with 32GB of memory
NCS5700 uptime is 3 weeks, 1 day, 10 hours, 11 minutes
NCS55B1 Fixed Scale HW Flexible Consumption Need Smart Lic
```

Verify Status of Hardware Modules on Cisco NCS 5700 Series Router

Hardware modules such as 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         NCS-57B1-5DSE-SYS(Active) IOS XR RUN               NSHUT

0/PM0              PSU2KW-ACPI               OPERATIONAL              NSHUT

0/PM1              PSU2KW-ACPI               OPERATIONAL              NSHUT

0/FT0              N5700-FAN                 OPERATIONAL              NSHUT

0/FT1              N5700-FAN                 OPERATIONAL              NSHUT

0/FT2              N5700-FAN                 OPERATIONAL              NSHUT

0/FT3              N5700-FAN                 OPERATIONAL              NSHUT

0/FT4              N5700-FAN                 OPERATIONAL              NSHUT

0/FT5              N5700-FAN                 OPERATIONAL              NSHUT
```

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

Example:

```
Router#show hw-module fpd
Auto-upgrade:Enabled
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 NCS-57B1-5DSE-SYS     0.1   IoFpga               CURRENT    0.08    0.08         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFPgaGolden     B   CURRENT            0.02         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   Primary-BIOS      S  CURRENT    1.10    1.10         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpga         S  CURRENT    0.24    0.24         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpgaGolden  BS  NEED UPGD          0.00         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFw             S  CURRENT    6.05    6.05         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFwGolden      BS  NEED UPGD          0.00         0/RP0
0/PM0      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT    1.08    1.08        NOT REQ
0/PM1      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT   17.56   17.56        NOT REQ
```

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.
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
Auto-upgrade:Enabled
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 NCS-57B1-5DSE-SYS     0.1   IoFpga               CURRENT    0.08    0.08         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFPgaGolden     B   CURRENT    0.02                 0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   Primary-BIOS      S  CURRENT    1.10    1.10         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpga         S  CURRENT    0.24    0.24         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpgaGolden  BS  CURRENT            0.00         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFw             S  CURRENT    6.05    6.05         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFwGolden      BS  RLOAD REQ  0.00    0.01         0/RP0
0/PM0      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT    1.08    1.08       NOT REQ
0/PM1      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT   17.56   17.56       NOT REQ
```

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
Auto-upgrade:Enabled
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 NCS-57B1-5DSE-SYS     0.1   IoFpga               CURRENT    0.08    0.08         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   IoFPgaGolden     B   CURRENT    0.02                 0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   Primary-BIOS      S  CURRENT    1.10    1.10         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpga         S  CURRENT    0.24    0.24         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   StdbyFpgaGolden  BS  CURRENT    0.00    0.01         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFw             S  CURRENT    6.05    6.05         0/RP0
0/RP0/CPU0 NCS-57B1-5DSE-SYS     0.1   TamFwGolden      BS  CURRENT    0.00    0.01         0/RP0
0/PM0      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT    1.08    1.08       NOT REQ
0/PM1      PSU2KW-ACPI           0.0   PO-PrimMCU           CURRENT   17.56   17.56       NOT REQ
```

Verify Interface Status on Cisco NCS 5700 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.

Verify Node Status on Cisco NCS 5700 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        NCS-57B1-5DSE-SYS(Active) IOS XR RUN               NSHUT

0/PM0             PSU2KW-ACPI               OPERATIONAL              NSHUT

0/PM1             PSU2KW-ACPI               OPERATIONAL              NSHUT

0/FT0             N5700-FAN                 OPERATIONAL              NSHUT

0/FT1             N5700-FAN                 OPERATIONAL              NSHUT

0/FT2             N5700-FAN                 OPERATIONAL              NSHUT

0/FT3             N5700-FAN                 OPERATIONAL              NSHUT

0/FT4             N5700-FAN                 OPERATIONAL              NSHUT

0/FT5             N5700-FAN                 OPERATIONAL              NSHUT
```

Displays the status of nodes present in the chassis.

Verify that the software state and the hardware state of 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

Card Type	State	Description
All	IDLE	Error – Card state is not initialized
All	DISCOVERED	Card is detected
All	POWERED_ON	Card is powered on
FC, FT, PT, PM	OPERATIONAL	Card is operating normally and is functional

Create Users and Assign Privileges on Cisco NCS 5700 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 NCS5500 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 132.

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 ...*".

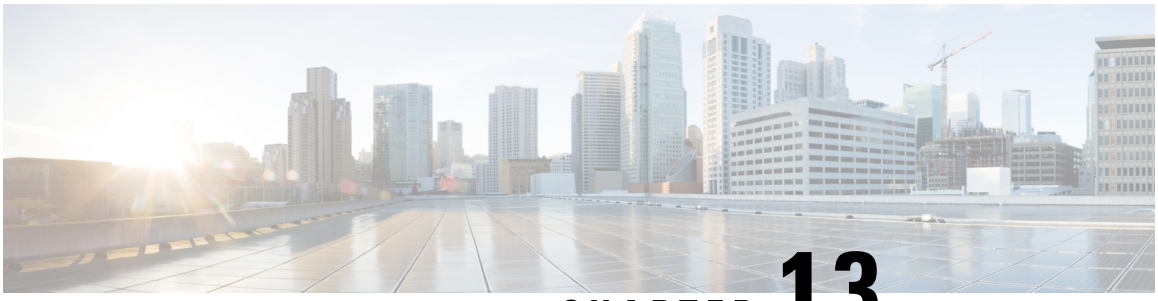
Step 4 Commit the configuration.

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 13

Install XR7 OS on NCS 5700 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 5700 series routers.

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

The router variants that support XR7 in Cisco IOS XR Release 7.3.1 are:

- NCS57B1-6D24
- NCS57B1-5DSE

Cisco NCS 5700 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.

Supported Packages

The base ISO image is contained within a `.iso` 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 can be downloaded from Cisco Software Download center.

Optional Package	Included in ISO by Default
ncs5500-netflow	Yes
ncs5500-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
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. Contact Cisco Support to build a GISO.
- **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 A manual or automatic system reload without the transaction being completed by the `install commit` command successfully executed, reverts the system to the point before the install transaction commenced, including any configuration changes. Only the log is preserved for debugging.

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 `ncs5700-x64-<version>.docs.tar` file for the release.

Obtain Data Models for Install Operation

XR7 can be installed using one of these two methods:

- CLI
- Cisco Software Manager Server
- YANG data models

To install using data models, you must first obtain the data models.

Step 1 Access the supported data models to install Cisco IOS XR software from the Github repository.

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 2 Explore 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-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.

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-ncs5700-core       x86_67        7.3.1v1.0.1-1      local-repo


xr-core               x86_64        7.3.1v1.0.1-1      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 7.3.1, 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-ncs5700-core       x86_67        7.3.1v1.0.1-1      remote-repo



xr-core               x86_64        7.3.1v1.0.1-1      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

You can upgrade the system when a newer version is available. A system upgrade replaces the existing version of the software with a newer version. By keeping the software up to date, you can ensure that the device works with the latest features and bug fixes.

You can replace the currently active software on your system with the software from a specified ISO image or GISO image. Only a minimal set of changes is performed to upgrade to the new software. Packages are not removed and reinstalled if they have the same name and version. For example, an upgrade that differs by only one package, removes and install only that one modified package.

Note The instructions in this section also apply to system downgrade.

This section shows replacing the current software version with `.iso` image. To understand the phases of install operation, see Software Deliverables and Terminologies, on page 137. For information about repositories, see Create Repository to Access Files for Installing IOS XR Software, on page 139.

Upgrade the System

In this scenario, you replace the current software with `.iso` 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.

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:/ncs5700-x64.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:/8000-x64.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:/ncs5700-x64.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 139.

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:/ncs5700_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
Thu Nov 25 15:13:17.395 UTC

User request: install package add xr-procmgr
Operation ID: 1.1.1
State:        Success since 2021-11-25 15:12:56 UTC

Current activity:    Await user input
Time started:        2021-11-25 15:13:02 UTC

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 reload

Least impactful apply method: install apply reload
```

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

On Cisco 8000 routers, you can upgrade the Field-Programmable Device (FPD) for QDD optical modules through CLI from IOS XR 7.5.x.

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

Before you begin

Get the QDD firmware file from Cisco Support.

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-7.3.1v1.0.1-1.x86_64.rpm`.

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-
7.3.1v1.0.1-1.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 153.

- **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 139.

- **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-7.3.1v1.0.1-1.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-7.3.1v1.0.0-1.x86_64.rpm
xr-mcast-v1.0.0-1.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:

```
Router# show install history last package
Tue Jul 14 11:09:19.748 UTC
2020-07-14 11:08:12 UTC        Packaging operation 1.1.1 started
2020-07-14 11:08:12 UTC        Add
2020-07-14 11:08:12 UTC         xr-telnet
2020-07-14 11:09:10 UTC        Packaging operation 1.1.1 success

Location 0/RP0/CPU0
   Add xr-telnet-7.3.1v1.0.0-1.x86_64
   Add xr-telnet-36cad6c174d48ffe-7.3.1v1.0.0-1.x86_64
   Add xr-telnet-ncs5700
-7.3.1v1.0.0-1.x86_64
   Add xr-telnet-a1f05ad3091205a8-7.3.1v1.0.0-1.x86_64
```

Note To display the list of incomplete installation requests, running and queued, use the **show install request** command.

When there is insufficient disk space in the root file system, the **show install request** command displays an error message.

```
Router#show install request
User request: install package add xr-telnet
Operation ID: 3.2
State:        Failure since 2020-01-08 13:28:26 UTC

Disk space check failed on nodes:
                                    0/RP0/CPU0.
Automatically recovered after failure, ready
for next user request.

Current activity:     Await user input
Time started:         2020-01-08 13:29:25

The following actions are available:
    install package add
    install package remove
    install package upgrade
    install package downgrade
    install package replace
    install package rollback
    install commit
```

Use the **show install history last package** command to obtain complete details of the failure.

```
Router#show install history last package
Wed Jan  8 13:29:51.586 UTC
2020-01-08 13:25:32 UTC   Packaging operation 3.2.1 started
2020-01-08 13:25:32 UTC   Add
2020-01-08 13:25:32 UTC   xr-telnet
2020-01-08 13:28:26 UTC   Error on 0/1/CPU0: Insufficient disk space to install packages
2020-01-08 13:28:26 UTC   Packaging operation 3.2.1 failed: Disk space check failed on nodes:
 0/1/CPU0
2020-01-08 13:28:26 UTC   Packaging operation 3.2.1 aborted: Automatically recovered after
failure

Location 0/1/CPU0
  Last event: Error (Insufficient disk space to install packages)
  Disk space pre-check failure:
     Phase: Download
     Required space: 140944B
     Available space: 110623B
```

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 7.3.1 LNT
Copyright (c) 2013-2021 by Cisco Systems, Inc.
Build Information:
Built By     : xyz
Built On     : Tue Feb 09 19:43:44 UTC 2021
Build Host   : iox-lnx-064
Workspace    : ../ncs5700/ws
Version      : 7.3.1
Label        : 7.3.1

cisco NCS5700 (D-1563N @ 2.00GHz)
cisco NCS-57B1-5DSE-SYS (D-1563N @ 2.00GHz) processor with 32GB of memory
NCS5700 uptime is 3 weeks, 1 day, 10 hours, 11 minutes
NCS55B1 Fixed Scale HW Flexible Consumption Need Smart Lic
```

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 7.3.1 LNT
Copyright (c) 2013-2021 by Cisco Systems, Inc.
Build Information:
Built By     : xyz
Built On     : Tue Feb 09 19:43:44 UTC 2021
Build Host   : iox-lnx-064
Workspace    : ../ncs5700/ws
Version      : 7.3.1
Label        : 7.3.1-Customer_Label

cisco NCS5700 (D-1563N @ 2.00GHz)
cisco NCS-57B1-5DSE-SYS (D-1563N @ 2.00GHz) processor with 32GB of memory
NCS5700 uptime is 3 weeks, 1 day, 10 hours, 11 minutes
NCS55B1 Fixed Scale HW Flexible Consumption Need Smart Lic
```

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
Fri Mar  5 17:37:23.205 UTC
Active Packages:    XR: 156    All: 1214
Label:              7.4.1-LABEL
Software Hash:      28dd70ef227aeca3d3fd3ecf8d1792a4f51fabb299ec7d38725869575fd9cfaf
Optional Packages                                                          Version
-------------------------------------------------------------------------------------
xr-bgp                                                                  7.3.1v1.0.0-1
xr-cdp                                                                  7.3.1v1.0.0-1
xr-eigrp                                                                7.3.1v1.0.0-1
xr-ipsla                                                                7.3.1v1.0.0-1
xr-is-is                                                                7.3.1v1.0.0-1
xr-lldp                                                                 7.3.1v1.0.0-1
xr-mcast                                                                7.3.1v1.0.0-1
xr-mpls-oam                                                             7.3.1v1.0.0-1
xr-ncs5700-mcast                                                        7.3.1v1.0.0-1
xr-ncs5700-netflow                                                      7.3.1v1.0.0-1
xr-netflow                                                              7.3.1v1.0.0-1
xr-ospf                                                                 7.3.1v1.0.0-1
xr-perf-meas                                                            7.3.1v1.0.0-1
xr-perfmgmt                                                             7.3.1v1.0.0-1
xr-telnet                                                               7.3.1v1.0.0-1
```

```
xr-track                                                    7.3.1v1.0.0-1
xr-xcare                                                    7.3.1v1.0.0-1
```

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 Obtain Data Models for Install Operation, on page 138.

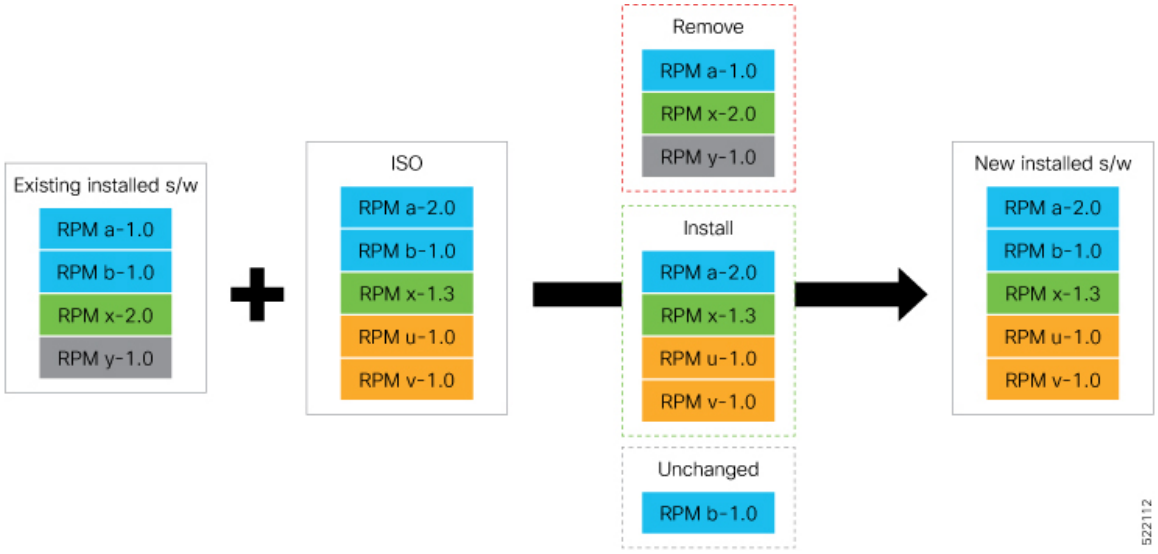
Build a Golden ISO

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 .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:

Upgrade the System to Obtain Bug Fixes

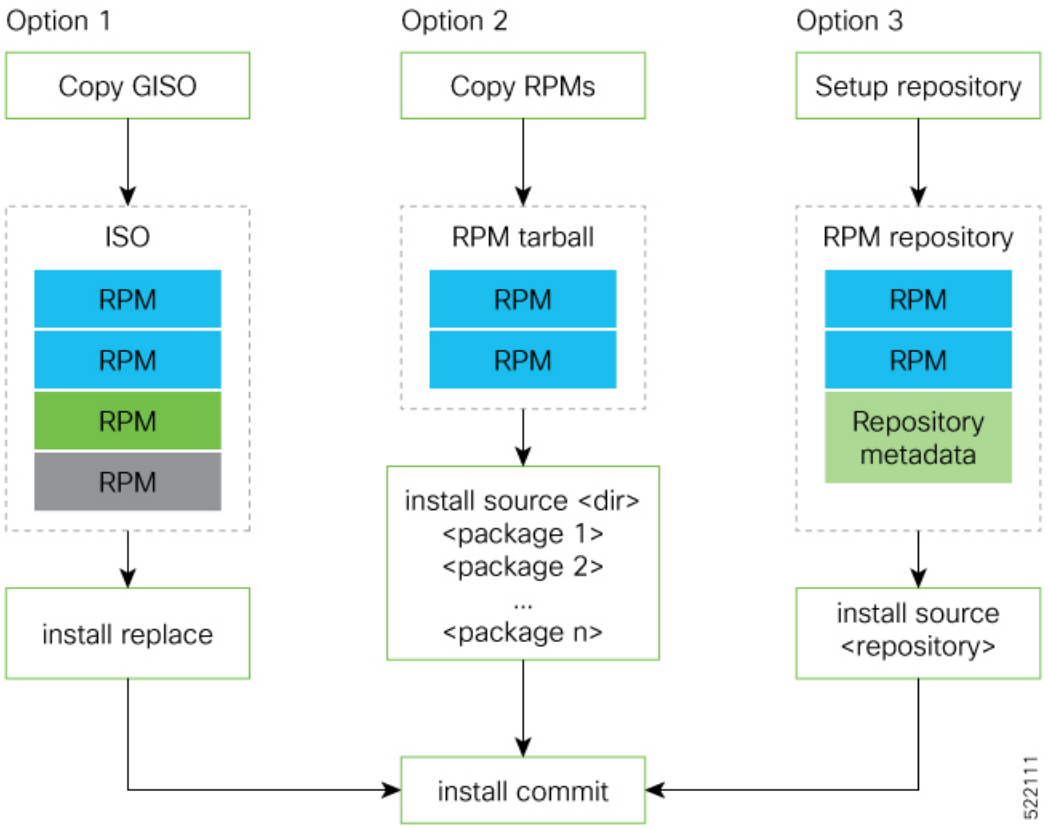
You can upgrade the system to obtain all available bug fixes or choose specific bug fix using bug ID.

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 .

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 139.

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-5700-core-7.3.1v1.0.1-1      <repository-name>

               xr-core-7.3.1v1.0.1-1           <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-5700-core-7.3.1v1.0.1-1 xr-core-7.0.1v1.0.1-1
Packaging operation 1.1.1 started - xr-5700-core-7.3.1v1.0.1-1 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 startedtion cleanup in progress
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

```
Router#show install request
User request: install package upgrade  xr-5700-core-7.3.1v1.0.1-1
Operation ID: 2.1.1
State: Success

Current activity: Await user input
Time started:

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

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-5700-core-7.3.1v1.0.1-1.x86_64.rpm
```

Note Packages can also be installed using the package name.

```
Router#install source /harddisk:/files  xr-5700-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-5700-core-7.3.1v1.0.1-1 xr-core-7.0.1v1.0.1-1
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-5700-core-7.3.1v1.0.1-1
2019-06-25 07:45:08 UTC    xr-5700-core-7.3.1v1.0.1-1
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-5700-core-7.3.1v1.0.1-1` and `xr-core-7.3.1v1.0.1-1` are installed and active.

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 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.

If a system fails to boot successfully, or reboots unexpectedly when the package is undergoing a version change, it is automatically recovered to its old software state.

This example shows the package `xr-telnet-7.3.1v1.0.1` is downgraded to `xr-telnet-7.3.1v1.0.0`. The path to source can be a local location or a configured repository.

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 or restart the system after applying the changes, 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>
      </packagename>
   </packages>
     <source>file://<path-to-source>/</source>
  </install>
  ```

  The package version `xr-telnet-7.3.1v1.0.1` is downgraded to `xr-telnet-7.3.1v1.0.0`.

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

- You can only roll back to the last commit (transaction ID).
- 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 Obtain Data Models for Install Operation, on page 138.

Step 5 Commit the operation.

Example:

```
Router#install commit
```