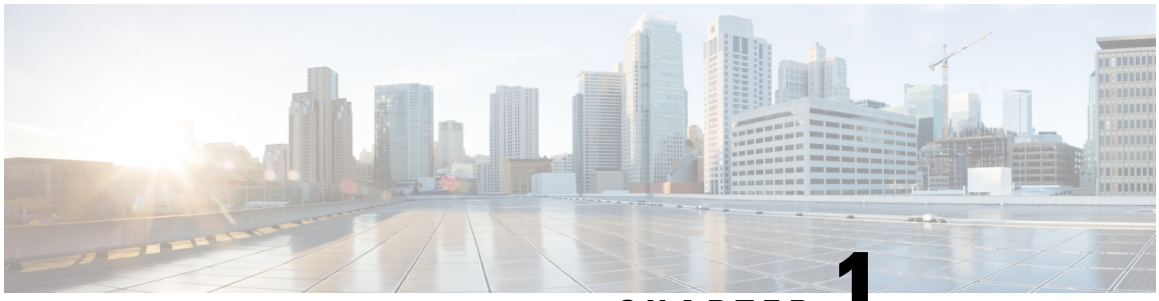
System Setup and Software Installation Guide for Cisco NCS 1004

First Published: 2019-08-30

Last Modified: 2024-09-04

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



CHAPTER 1

Bring-up Cisco NCS 1004

After installing the hardware, boot the Cisco NCS 1004 system. You can connect to the XR console port and power on the system. NCS 1004 completes the boot process using the pre-installed operating system (OS) image. If no image is available, NCS 1004 can be booted using the iPXE boot, an external bootable USB drive, or Golden ISO.

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

Note The output of the examples in the procedures is not from the latest software release. The output will change for any explicit references to the current release.

Boot NCS 1004

The various boot options in NCS 1004 are as follows:

1. Boot using SSD (hard disk)

2. Boot using USB drive
3. Boot using iPXE
4. Boot using ZTP
5. Boot using Golden ISO

If there is no bootable image in all of the above boot options, reboot the system.

Boot NCS 1004

Use the console port to connect to NCS 1004. By default, the console port connects to the XR mode. If necessary, you can establish subsequent connections through the management port, after it is configured.

Procedure

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 115,200 bps, 8 data bits, 1 stop bit and no parity.

Step 3 Power on NCS 1004.

To turn on the power shelves, press the power switch up. As NCS 1004 boots up, you can view the boot process details at the console of the terminal emulation program.

Step 4 Press **Enter**.

The boot process is complete when the system prompts you to enter the root-system username. If the prompt does not appear, wait for a while to give NCS 1004 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 NCS 1004 is corrupt. In this case, you can boot NCS 1004 using an external bootable USB drive.

Boot NCS 1004 Using USB Drive

The bootable USB drive is used to reimage NCS 1004 for system upgrade or to boot the NCS 1004 in case of boot failure. 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.

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

Before you begin

- You need a USB drive with a storage capacity of at least 4 GB.

- The USB drive should have a single partition.
- NCS 1004 software image can be downloaded from Software Download page on Cisco.com.
- Copy the compressed boot file from the software download page at Cisco.com to your local machine. The filename for the compressed boot file is in the format *ncs1004-usb-boot-<release_number>.zip*. For example, *ncs1004-usb-boot-7.0.1.zip*.

Procedure

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

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

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

Step 4 Extract the content of the compressed boot file by unzipping it in the USB drive. This makes the USB drive a bootable drive.

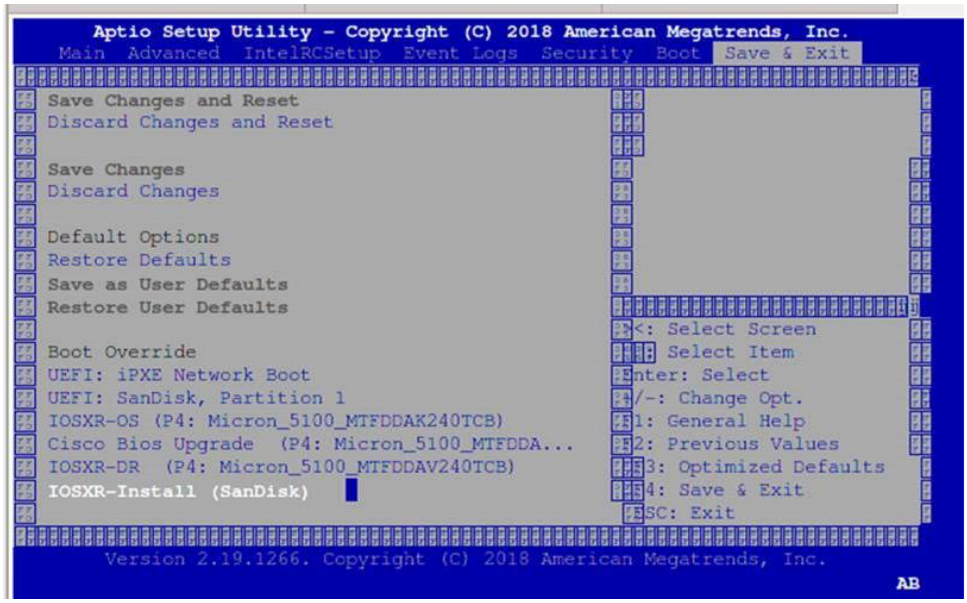
Note You must extract the contents of the zipped file ("EFI" and "boot" directories) directly in the root folder of the USB drive. If the unzipping application places the extracted files in a new folder, move the "EFI" and "boot" directories to the root folder of the USB drive.

Step 5 Insert the USB drive in one of the USB ports of NCS 1004.

Step 6 Reboot NCS 1004 using power cycle or console.

Step 7 Press Esc to enter BIOS.

Step 8 Select the **Save & Exit** tab of BIOS.



Step 9 Choose **IOS -XR Install**.

The system detects USB and boots the image from USB.

```
Admin Console:
```

```
GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from USB..
Loading Kernel..

Validating End Entity Certificate...

Validating SubCA Certificate...

Validating Root Certificate...
Loading initrd..

Validating End Entity Certificate...

Validating SubCA Certificate...

Validating Root Certificate...
CiscoSec: Image signature verification completed.
XR Console:
CiscoSec: Image signature verified.
[    9.957281] i8042: No controller found
Starting udev
udevd[972]: failed to execute '/etc/udev/scripts/network.sh' '/etc/udev/scripts/network.sh':
 No such file or directory
Populating dev cache
Running postinst /etc/rpm-postinsts/100-dnsmasq...
update-rc.d: /etc/init.d/run-postinsts exists during rc.d purge (continuing)
 Removing any system startup links for run-postinsts ...
  /etc/rcS.d/S99run-postinsts
Configuring network interfaces... done.
```

Step 10 Remove the USB drive. The NCS 1004 reboots automatically.

```
Setting maximal mount count to -1
Setting interval between checks to 0 seconds
Fri Dec 11 20:35:56 UTC 2015: Install EFI on /dev/mb_disk4
Fri Dec 11 20:35:57 UTC 2015: Install finished on mb_disk
Rebooting system after installation ...
[  116.973666] reboot: Restarting system
Version 2.17.1245. Copyright (C) 2015 American Megatrends, Inc.
BIOS Date: 11/29/2015 12:02:45 Ver: 0ACBZ1110
Press <DEL> or <ESC> to enter setup.
CiscoSec: Image signature verified.


GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from Disk..
Loading Kernel..

Validating End Entity Certificate...

Validating SubCA Certificate...

Validating Root Certificate...
Loading initrd..

Validating End Entity Certificate...

Validating SubCA Certificate...

Validating Root Certificate...
CiscoSec: Image signature verification completed.
```

```
Initrd, addr=0xff69a000, size=0x955cb0
[    1.745686] i8042: No controller found
```

Boot Using iPXE

iPXE is a pre-boot execution environment that is included in the network card of the management interfaces and works at the system firmware (UEFI) level of the chassis. iPXE is used to reimage the system, and boot the chassis 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.

Note The time taken for iPXE to download the ISO image depends on the network speed. Ensure that the network speed is sufficient to complete the image download in less than 10 minutes. The chassis reloads if the image is not downloaded by 10 minutes.

iPXE acts as a bootloader 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. You must define iPXE in the DHCP server configuration file.

Setup DHCP Server

A DHCP server must be configured for IPv4, IPv6, or both communication protocols.

Note For DHCPv6, a routing advertisement (RA) message must be sent to all nodes in the network that indicates which method is to be used to obtain the IPv6 address. Configure Router-advertise-daemon (radvd, install using yum install radvd) to allow the client to send the 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;
        };
};
```

To setup a DHCP server:

1. Create the `dhcpd.conf` file (for IPv4, IPv6 or both communication protocols), `dhcpv6.conf` file (for IPv6) or both in the `/etc/` 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 chassis.

2. Test the server once the DHCP server is running:

   For example, for ipv4:

   a. Use MAC address of the chassis:

   ```
   host ncs1004
   {
   hardware ethernet ab:cd:ef:01:23:45;
   fixed-address <ip address>;
   filename "http://<httpserver-address>/<path-to-image>/ncs1004-mini-x.iso";
   }
   ```

   Ensure that the above configuration is successful.

   b. Use serial number of the chassis:

   ```
   host demo {
   option dhcp-client-identifier "<chassis-serial-number>";
     filename "http://<IP-address>/<hardware-platform>-mini-x.iso";
     fixed-address <IP-address>;
   }
   ```

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

   Example

   ```
   host 10.89.205.202 {
          hardware ethernet 40:55:39:56:0c:e8;
             if exists user-class and option user-class = "iPXE" {
             filename "http://10.89.205.127/box1/ncs1004-mini-x-7.0.1.iso";
          } else {
              filename "http://10.89.205.127/box1/StartupConfig.cfg";
          }
          fixed-address 10.89.205.202;
       }
   ```

Boot 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 chassis:

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

Example:

```
sysadmin-vm:0_RP0# hw-module location all bootmedia network reload
Tue Feb 12 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/ncs1004/ncs1004-mini-x.iso
http://10.37.1.235/ncs1004/ncs1004-mini-x.iso ncs1004/ncs1004-mini-x.iso... 58% << Downloading
 file as indicated by DHCP/PXE server to boot install image
```

Boot Using Zero Touch Provisioning (ZTP)

Zero Touch Provisioning (ZTP) is used to deploy minimal configurations on several chassis. You can use ZTP to boot, set up, and configure the system. Configurations such as configuring the management Ethernet interface, installing SMUs, applications, and optional packages can be automated using ZTP. ZTP does not execute if a username is already configured in the system.

ZTP auto provisioning involves:

- **Configuration:** Downloads and executes the configuration files. 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. These 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 script.

You can either use the ZTP bash script or the ZTP configuration file.

```
host ncs1004 {
  #hardware ethernet 00:a0:c9:00:00:00;
  option dhcp-client-identifier "<chassis-serial-number>";
     filename "http://<IP-address>/<folder>/ncs1004-ztp.script";
     #filename "http://<IP-address>/<folder>/ncs1004-ztp.cfg";
  }
```

The following is the sample content of the ZTP bash script.

```
#! /bin/bash
#
# NCS1004 Demo Sample
# ZTP installation of config and day-0 SMU's
#
source ztp_helper

wget http://downloads.sourceforge.net/project/yourcode/application.tgz
#install the downloaded application.tgz

#Run XR CLI's from the script
`xrcmd "show version"`
```

The following is the sample content of the ZTP configuration file. You can automate all the configurations.

```
!! IOS XR Configuration version = 7.0.1
!
telnet vrf default ipv4 server max-servers 20
!
vty-pool default 0 20 line-template default
```

```
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address dhcp
 no shutdown
!
router static
 address-family ipv4 unicast
  0.0.0.0/0 10.77.132.1
!
end
```

Boot NCS 1004 Using Golden ISO

Golden ISO is a feature that is provided to the user to build the customized ISO using mini ISO, required SMUs, and IOS XR configuration.

Before the introduction of Golden ISO feature, you must perform the following three steps, to install a new image.

1. Boot the system with mini ISO. You can do this task using iPXE or USB boot.
2. Install, add, and activate all the relevant SMUs and optional packages on to NCS 1004. NCS 1004 reloads on reload of any SMUs.
3. Apply IOS XR configuration.

Benefits of Golden ISO

- Saves installation effort and time.
- The system is available in a single command and boot.

You can build the Golden ISO using ‘gisobuild.py’script available at /pkg/bin/gisobuild.py location.

Limitations

- install operation over IPv6 is not supported.

Build Golden ISO

You can use the following command to build the Golden ISO.

```
gisobuild.py -i./ncs1004-mini-x.iso -r ./rpm-directory -c ./xr-config -l label
```

rpm-directory - Directory where SMUs (xr, calvados, and host) are copied.

xr-config - IOS XR configuration to be applied to the system after booting.

label - Label of the Golden ISO.

Note You must copy /pkg/bin/gisobuild.py from NCS 1004 to the Linux environment and use the following command to build the Golden ISO image.

```
python gisobuild.py -i ./ncs1004-mini-x-7.0.1.04I.iso -r. -c startup_new.cfg -l v2
System requirements check [PASS]
Golden ISO build process starting...
```

```
Platform: ncs1004 Version: 7.0.1.04I

XR-Config file (/bh/bosshogg_images/r701/701_04I_DT_IMAGE/giso/startup_new.cfg) will be
encapsulated in Golden ISO.

Scanning repository [/bh/bosshogg_images/r701/701_04I_DT_IMAGE/giso]...

Building RPM Database...
Total 1 RPM(s) present in the repository path provided in CLI

Following XR x86_64 rpm(s) will be used for building Golden ISO:

(+) ncs1004-k9sec-2.1.0.0-r70104I.x86_64.rpm

...RPM compatibility check [PASS]

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

XR rpms:
ncs1004-k9sec-2.1.0.0-r70104I.x86_64.rpm

XR Config file:
router.cfg

...Golden ISO creation SUCCESS.

Golden ISO Image Location:
/bh/bosshogg_images/r701/701_04I_DT_IMAGE/giso/ncs1004-goldenk9-x-7.0.1.04I-v2.iso

Detail logs:
/bh/bosshogg_images/r701/701_04I_DT_IMAGE/giso/Giso_build.log-2019-03-20:15:47:19.516203
```

Golden ISO file is created in the following format:

platform-name-golden-x.iso-*version.label* (does not contain security(*k9sec*.rpm) rpm)

Example: ncs1004-golden-x-7.0.1.014I-V1.iso

platform-name-goldenk9-x.iso-*version.label* (contains security(*k9sec*.rpm) rpm)

Example: ncs1004-goldenk9-x-7.0.1.014I-V1.iso

Verify Boot Operation

Procedure

show version

Example:

```
RP/0/RP0/CPU0:ios# show version
Thu Apr 30 21:57:48.371 IST
Cisco IOS XR Software, Version 7.2.1 Copyright (c) 2013-2020 by Cisco Systems, Inc.

Build Information:
 Built By     : ahoang
 Built On     : Wed Apr 29 19:22:26 PDT 2020
 Built Host   : iox-lnx-023
```

```
 Workspace    : /auto/srcarchive14/prod/7.2.1/ncs1004/ws
 Version      : 7.2.1
 Location     : /opt/cisco/XR/packages/
 Label        : 7.2.1

cisco NCS-1004 () processor
System uptime is 5 hours 25 minutes
```

Compare the displayed version with the boot image version. The versions must be the same.

Boot NCS 1004 Using Golden ISO for Open ROADM

The following topics describe on how to boot NCS 1004 using golden ISO for Open ROADM:

- GISO for Open ROADM
- Build GISO Image for Open ROADM
- Create USB File for Open ROADM
- Boot NCS 1004 using USB File for Open ROADM
- Verify Boot Operation for Open ROADM

GISO for Open ROADM

From Release 7.3.1 onwards, NCS 1004 supports GISO images for new Open ROADM deployments. The GISO image is bundled with the following files:

- Mini ISO image
- Open ROADM RPM
- OTN-XP RPM
- Startup configuration file

The new Open ROADM deployment mandatorily requires a startup configuration file to enable open ROADM. The start up configuration file contains the following information:

- DHCP client configuration for IPv4 and IPv6 addresses
- SSH sever configuration
- XR Netconf configuration
- Telnet configuration for IPv4 and IPv6 addresses

Build GISO Image for Open ROADM

The mini ISO file, RPM directory, and the startup configuration file should be placed in the same path.

To build the new Golden ISO for open ROADM, use the following command:

```
gisobuild.py -i ./ncs1004-mini-x.iso -r ./rpm-directory -c ./xr-config -l label
```

Example

```
gisobuild.py -i ./ncs1004-mini-xr-7.3.1.iso -r ./RPMS -c ./giso.startup.txt -1 V1
```

- *gisobuild.py* – Python script to run the GISO image. You can download the script from the Github site.
- *ncs1004-mini-x.iso* – Mini ISO NCS 1004 file, for example ncs1004-mini-xr-7.3.1.iso.
- *rpm-directory* - RPM directory where the RPM files such as OPEN ROADM RPM and OTN-XP RPM files are stored.

  Sample RPM files:

  - *OPEN ROADM RPM* - ncs1004-tp-sw-1.0.0.0-r731.rpm
  - *OTN-XP RPM* - ncs1004-sysadmin-otn-xp-dp-7.3.1-r731.rpm

- *xr-config* - IOS XR start up configuration file, for example, *giso.startup.txt*. This file has Open ROADM specific configurations that are to be applied to the system after booting.
- *label* - Label of the Golden ISO image.

Sample

```
python gisobuild.py -i ./ncs1004-mini-x-7.3.1.iso -r./RPMS-c giso.startup.txt -l v1
System requirements check [PASS]
Golden ISO build process starting...

Platform: ncs1004 Version: 7.3.1

XR-Config file (/bh/bosshogg_images/r731/731_image/giso/giso.startup.txt) will be encapsulated
 in Golden ISO.

Scanning repository [/bh/bosshogg_images/r731/731_image/giso]...

Building RPM Database...
Total 1 RPM(s) present in the repository path provided in CLI

Following XR x86_64 rpm(s) will be used for building Golden ISO:

(+) ncs1004-k9sec-2.1.0.0-r731.x86_64.rpm

...RPM compatibility check [PASS]

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

XR rpms:
ncs1004-k9sec-2.1.0.0-r731.x86_64.rpm

XR Config file:
giso.startup.txt

...Golden ISO creation SUCCESS.

Golden ISO Image Location:
/bh/bosshogg_images/r731/731_image/giso/ncs1004-goldenk9-x-7.3.1-v1.iso

Detail logs: /bh/bosshogg_images/r731/731_image/giso/Giso_build.log-2021-03-10:15:47:19.516203
```

Create USB File for Open ROADM

Once the Golden ISO image is available, you need to create a bootable compressed USB file. Use this USB file to boot NCS 1004.

To create the USB file using the GISO image, use the following command:

```
./create_usb_zip ncs1004 ncs1004-golden-x-7.3.1-V1.iso
```

The bootable compressed USB file is created. You must copy the boot file from the system to the USB drive. Use the following procedure to copy the compressed USB file, extract the content, and reboot NCS 1004.

Boot NCS 1004 using USB File for Open ROADM

The bootable USB drive is used to reimage NCS 1004 for system upgrade or to boot the NCS 1004 in case of boot failure. 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.

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

Before you begin

- You need a USB drive with a storage capacity of at least 8 GB.
- The USB drive should have a single partition.
- NCS 1004 software image can be downloaded from Software Download page on Cisco.com.
- Copy the compressed boot file from the software download page at Cisco.com to your local machine. The filename for the compressed boot file is in the format *ncs1004-usb-boot-<release_number>.zip*. For example, *ncs1004-usb-boot-7.1.3.zip*.
- Plugin the USB drive into the USB 0 port of NCS 1004.

Procedure

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

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

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

Step 4 Extract the content of the compressed boot file by unzipping it in the USB drive. This makes the USB drive a bootable drive.

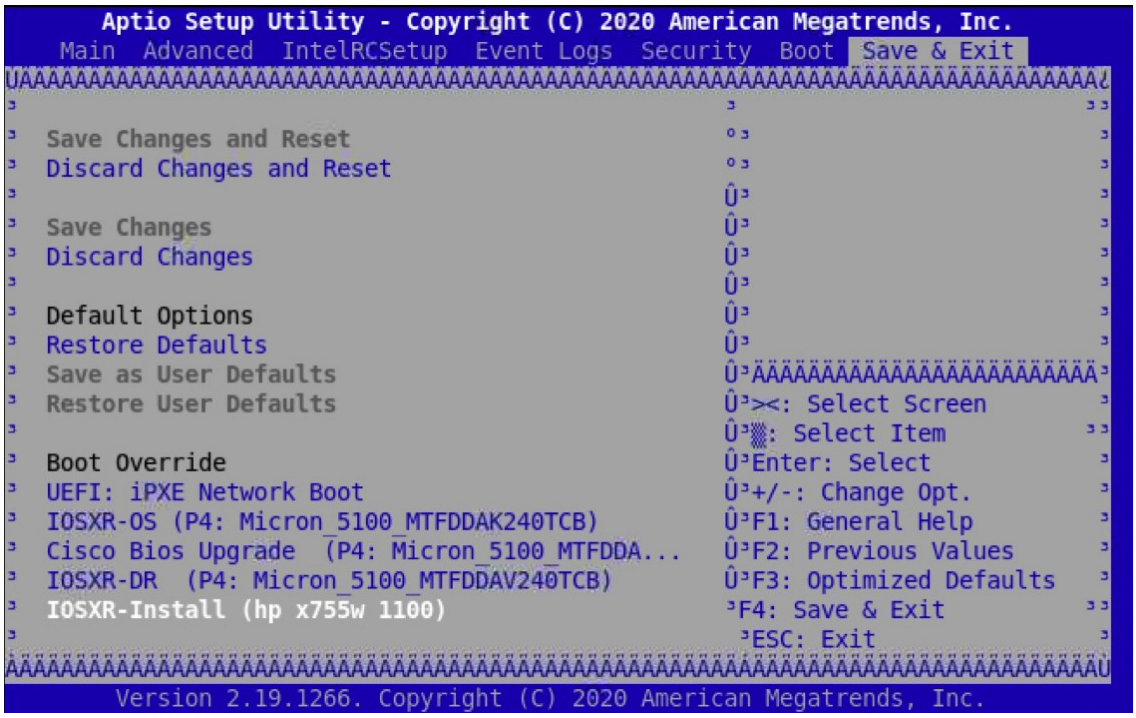
Note You must extract the contents of the zipped file ("EFI" and "boot" directories) directly in the root folder of the USB drive. If the unzipping application places the extracted files in a new folder, move the "EFI" and "boot" directories to the root folder of the USB drive.

Step 5 Insert the USB drive in one of the USB ports of NCS 1004.

Step 6 Reboot NCS 1004 using power cycle or console.

Step 7 Press Esc to enter BIOS.

Step 8 Select the **Save & Exit** tab of BIOS.



521541

Step 9 Choose **IOS -XR Install**.

The system detects USB and boots the image from USB.

```
TAM: Chip DB Verified
CiscoSec: Image Signature Verified
GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from USB..
Loading Kernel..
Kernel Secure Boot Validation Result: PASSED
Loading initrd….
Initrd Secure Boot Validation Result: PASSED
Starting udev…..
Running postinst /etc/rpm-postinsts/100-dnsmasq...
Sun Mar  7 19:22:30 UTC 2021: pd_download_giso
Write at Address 0x7bbe000098 (mmap addr 0x7fe08ec87000(0x98)) value 0x1 len 4 width 4 byte

Write at Address 0x7bbe000098 (mmap addr 0x7f54fc88b000(0x98)) value 0x2 len 4 width 4 byte

 Watchdog timer reset done, next reset needed within 10 minutes
Golden ISO type = 1.1 and PKG_VER = 1.0
Current Boot: IOSXR-Install
Current Boot: USB…
 * First booting, filesystem will be relabeled...
Finished Calvados patch for lxc
Starting to prepare calvados logical volume---
 Create sub partition on /dev/panini_vol_grp/calvados_lv0
 Create data sub partition on /dev/panini_vol_grp/calvados_data_lv0
 File system creation on /dev/panini_vol_grp/calvados_lv0 took 6 seconds
 Install sysadmin-vm image on /dev/panini_vol_grp/calvados_lv0
 RP based installation
 Starting Calvados patch for lxc for sysadmin-vm
```

```
 Uninstalling rpm task-nxos-core
 Uninstalling rpm gdb
 Uninstalling rpm smartmontools
NCS1004: Complete Patch Calvados
Enable selinux to relabel filesystem from initramfs
Checking SELinux security contexts:
 * First booting, filesystem will be relabeled...
 Finished Calvados patch for lxc
 Installing sysadmin-vm image size of 1.9G took 53 seconds
---Starting to prepare repository---
 File system creation on /dev/cpu_disk2 took 3 seconds
 Check for unwanted iso and remove if required.
 Copying /iso/host.iso to repository /iso directory
 Copying /iso/ncs1004-sysadmin.iso to repository /iso directory
 Copy Sysadmin rpms to repository
 Copy XR rpms to repository
 Copy giso_info.txt to repository
 Copying /iso/ncs1004-xr.iso to repository /iso directory
 Copying all ISOs to repository took 12 seconds
 Install EFI on /dev/cpu_disk4
pd_notify_img_install_done
Checking disk error for: sdb
 Chassis disk smartctl -a output
 Chassis disk smartctl output done
 Disk model: Micron_5100_MTFDDAV240TCB
 No failures found in dmesg
 Checking Chassis disk mount failures.
 No mount failures found in Chassis disk /dev/sdb2
 No mount failures found in Chassis disk /dev/BHDisasterRecovery/golden_image
 Chassis disk partitions exist
 Install finished on cpu_disk
```

Step 10 Remove the USB drive. The NCS 1004 reboots automatically.

```
Rebooting system after installation ...
[201.715171] reboot: Restarting system
ERROR: Class:0; Subclass:10000; Operation: 1004
NCS1004: Initilizing Devices
Version 2.19.1266. Copyright (C) 2020 American Megatrends, Inc.
BIOS Date: 10/23/2020 09:03:42 Ver: 0ACHI470
Press <DEL> or <ESC> to enter setup
TAM: Chip DB
CiscoSec: Image Signature Verified
GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from Disk..
Loading Kernel..
Kernel Secure Boot Validation Result: PASSED
Loading initrd..
Initrd Secure Boot Validation Result: PASSED
[3.836637] i8042: No controller found
Enable selinux to relabel filesystem from initramfs


Load IMA appraise policy: OK


Switching to new root and running init.


Sourcing /etc/sysconfig/udev
```

```
Starting udev: [  OK  ]


Starting udev


Running postinst /etc/rpm-postinsts/100-dnsmasq...


update-rc.d: /etc/init.d/run-postinsts exists during rc.d purge (continuing)


 Removing any system startup links for run-postinsts
  /etc/rcS.d/S99run-postinsts
Configuring network interfaces... done.
Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
  generating ssh RSA key...
  generating ssh ECDSA key...
  generating ssh DSA key...
  generating ssh ED25519 key...
sshd start/running, process 3559
Starting rpcbind daemon...done.
Starting kdump:[  OK  ]
Starting random number generator daemon.
Starting system log daemon...0
Starting kernel log daemon...0
tftpd-hpa disabled in /etc/default/tftpd-hpa
Starting internet superserver: xinetd.
Starting S.M.A.R.T. daemon: smartd.
Starting Lighttpd Web Server: lighttpd.
Starting libvirtd daemon: [  OK  ]
Starting crond: OK
Starting cgroup-init
Network ieobc_br defined from /etc/init/ieobc_br_network.xml
Network local_br defined from /etc/init/local_br_network.xml
Network xr_local_br defined from /etc/init/xr_local_br_network.xml
Network ieobc_br started
Network local_br started
Network xr_local_br started
mcelog start/running, process 4647
diskmon start/running, process 4653
Creating default host password file
Start serial incoming on , Clearing ..
initctl: Unknown instance: /dev/ttyS0
Connecting to 'default-sdr--1' console
bootlogd: ioctl(/dev/pts/2, TIOCCONS): Device or resource busy
Running postinst /etc/rpm-postinsts/100-dnsmasq...
update-rc.d: /etc/init.d/run-postinsts exists during rc.d purge (continuing)
Removing any system startup links for run-postinsts ...
  /etc/rcS.d/S99run-postinsts
Configuring network interfaces... done.
Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
  generating ssh RSA key...
  generating ssh ECDSA key...
  generating ssh DSA key...
  generating ssh ED25519 key...
sshd start/running, process 2197
Starting rpcbind daemon...done.
Starting random number generator daemon.
Starting system log daemon...0
Starting kernel log daemon...0
```

```
tftpd-hpa disabled in /etc/default/tftpd-hpa
Starting internet superserver: xinetd.
net.ipv4.ip_forward = 1
Libvirt not initialized for container instance
Starting crond: OK
SIOCADDRT: File exists
Start serial incoming on , Clearing ..
ios con0/RP0/CPU0 is now available
Press RETURN to get started.
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply third-party
authority to import, export, distribute or use encryption. Importers,
exporters, distributors and users are responsible for compliance with
U.S. and local country laws. By using this product you agree to comply
with applicable laws and regulations. If you are unable to comply with
U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```

Verify Boot Operation for Open ROADM

Procedure

show version

Example:

```
RP/0/RP0/CPU0:ios#show version
Sun Mar  7 19:31:38.139 UTC
Cisco IOS XR Software, Version 7.3.1
Copyright (c) 2013-2021 by Cisco Systems, Inc.

Build Information:
Built By     : ingunawa
Built On     : Thu Feb 25 19:10:10 PST 2021
Built Host   : iox-lnx-070
Workspace    : /auto/srcarchive17/prod/7.3.1/ncs1004/ws
Version      : 7.3.1
Location     : /opt/cisco/XR/packages/
Label        : 7.3.1-0

cisco NCS-1004 () processor
System uptime is 1 minute
```

Compare the displayed version with the boot image version. The versions must be the same.

Bring-Up Line Card

Procedure

Step 1 Insert the line card into slot.

Step 2 Wait until the LED on the line card turns Green.

Step 3 Configure OTN-XP card with LC MODE.

See LC Mode on OTN-XP Card.

Step 4 Upgrade the FPDs of the line card depending on the output of **show hw-module location 0**/*line-card-slot* **fpd** command.

Disaster Recovery

When you replace the CPU or NCS 1004 chassis, the Disaster Recovery feature allows you to restore the node configuration with minimum downtime. The feature works without console access. Before replacing CPU, use the **graceful-recovery backup initiate** command to back up the XR configuration. The node will also back up the running XR configuration after 20 mins. After reboot, the node backs up the XR configuration immediately.

CPU Replacement

You must consider the following points for CPU replacement.

- The node runs in headless mode.
- You can insert the CPU with SSD and the node starts to boot the OS from CPU SSD.
- The version of the images in CPU or chassis SSD are compared.
- If the version is different, configuration is taken from chassis SSD as the chassis golden image has priority.
- If the version is same, the node boots up. This version comparison happens upon each reboot including power cycle.
- The configuration is always taken from the chassis. If the chassis SSD is not functional, the node boots with only the CPU.

Chassis Replacement

You must consider the following points for chassis replacement.

- Chassis replacement involves minimum downtime.
- When the chassis is obtained, you can connect the CPU and boot. After receiving the empty chassis through RMA, you can insert the CPU and same configuration is restored.

- CPU swap from other units is also supported; however, the chassis image and configuration will be replaced in the CPU.

Health Check for Proper Backup ISO Image

Table 1: Feature History

Feature Name	Release Information	Feature Description
Health Check for Proper Backup ISO Image	Cisco IOS XR Release 7.5.2	This feature primitively validates the backup ISO image to be used during Disaster Recovery. The validation happens before copying the image to the CPU disk and motherboard disks, and thereafter the copied image is audited every 12 hours. Image corruption triggers the **Disaster recovery is disabled due to corrupted ISO** alarm. This Health Check feature ensures error-free booting of NCS 1004 chassis during disaster recovery operations.

Note To clear "Clear the DISASTER-RECOVERY-DISABLED Alarm", log in to the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note Verify that there is no **Disaster recovery is disabled due to corrupted ISO** alarm using the **show alarms** command before sending the CPU for RMA.

Access the System Admin Console

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

Procedure

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

Step 2 Type **Ctrl + O** to access the console logs.

Example:

```
RP/0/RP0/CPU0:ios# Ctrl + O


RP/0/RP0/CPU0:ios#
Disconnecting from 'default-sdr--1' console. Continue(Y/N)?


Y
Connecting to 'sysadmin' console

System Admin Username: root
Password:
root connected from 127.0.0.1 using console on sysadmin-vm:0_RP0
sysadmin-vm:0_RP0#
```

After you enter the System Admin console, the prompt changes to:

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

Configure Management Interface

To use the management interface for system management and remote communication, you must configure an IP address and subnet mask for the management Ethernet interface. To communicate with devices on other networks (such as remote management stations or TFTP servers), you must configure a default (static) route for NCS 1004.

Before you begin

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

Procedure

Step 1 **configure**

Example:

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

Enters XR configuration mode.

Step 2 **interface mgmtEth** *rack/slot/instance/port*

Example:

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

Enters interface configuration mode for the management interface.

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

Example:

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

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

Step 4 **no shutdown**

Example:

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

Places the interface in an "up" state.

Step 5 **exit**

Example:

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

Exits the management interface configuration mode.

Step 6 **router static address-family ipv4 unicast** *0.0.0.0/0default-gateway*

Example:

```
RP/0/RP0/CPU0:ios(config)# router static address-family ipv4 unicast 0.0.0.0/0 192.0.2.1
```

Specifies the IP address of the default gateway to configure a static route. This IP address must be used for communication with devices on other networks.

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.

What to do next

Configure Telnet and Configure SSH.

Configure Telnet

This procedure allows you to establish a telnet session to the management interface port using its IP address.

Procedure

Step 1 **configure**

Example:

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

Enters the configuration mode.

Step 2 **telnet {ipv4 | ipv6} server max-servers** *limit*

Example:

```
RP/0/RP0/CPU0:ios(config)# telnet ipv4 server max-servers 10
```

Specifies the number of allowable telnet servers (up to 100). By default, no telnet servers are allowed. You must configure this command to enable the use of telnet servers.

Step 3 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

Configure SSH

Configure SSH

This procedure allows you to establish an SSH connection to the management interface port using its IP address.

Before you begin

- Install the ncs1004-k9sec package on NCS 1004. For details about package installation, see Install Packages.
- Generate the crypto key for SSH using the **crypto key generate dsa** command.

Procedure

Step 1 **configure**

Example:

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

Enters the configuration mode.

Step 2 **ssh server v2**

Example:

```
RP/0/RP0/CPU0:ios(config)# ssh server v2
```

Enables the SSH server to accept only SSHv2 client connections.

Step 3 Use the **commit** or **end** command.

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

end-Prompts the 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.

Step 4 **show ssh session details**

Example:

```
RP/0/RP0/CPU0:ios# show ssh session details
```

Displays a detailed report of the SSHv2 connections to and from NCS 1004.

```
Tue Feb 12 16:03:51.455 UTC
SSH version : Cisco-2.0

id      key-exchange           pubkey               incipher    outcipher   inmac
outmac
-----------------------------------------------------------------------------------------------
Incoming Sessions
1       ecdh-sha2-nistp256     ecdsa-sha2-nistp256  aes128-ctr  aes128-ctr  hmac-sha2-256
hmac-sha2-256

Outgoing sessions
```

What to do next

Perform Clock Synchronization with NTP Server

Perform Clock Synchronization with NTP Server

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

Before you begin

Configure Management Interface.

Procedure

Step 1 **configure**

Example:

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

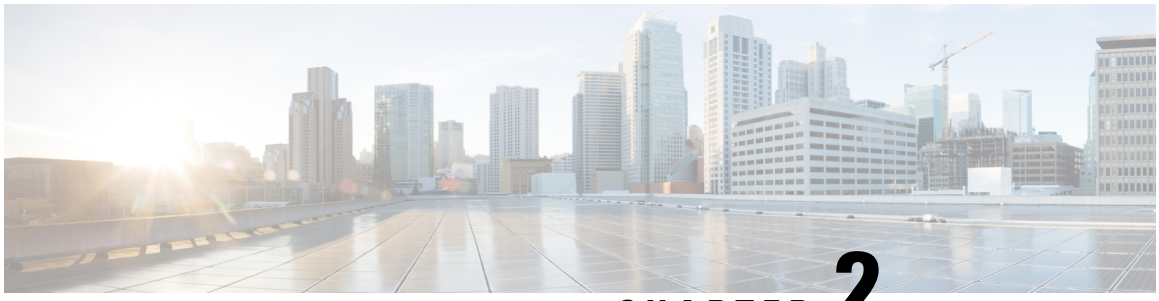
Enters XR configuration mode.

Step 2 **ntp server** *server_address*

Example:

```
RP/0/RP0/CPU0:ios# ntp server 192.0.2.55
```

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



CHAPTER 2

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, take corrective action before making further configurations.

Note The output of the examples in the procedures is not from the latest software release. The output will change for any explicit references to the current release.

Verify Status of Hardware Components

To verify the status of all the hardware components installed on NCS 1004, perform the following procedure.

Before you begin

Ensure that all the required hardware components are installed on NCS 1004. For installation details, see *Cisco Network Convergence System 1004 Hardware Installation Guide*.

Procedure

Step 1 **show platform**

When you execute this command from the Cisco IOS XR EXEC mode, the status of Cisco IOS XR is displayed.

Example:

```
RP/0/RP0/CPU0:ios# show platform
Wed Mar  4 06:21:26.929 UTC
Node              Type                        State             Config state
--------------------------------------------------------------------------------
0/0               NCS1K4-LC-FILLER            PRESENT           NSHUT
0/1               NCS1K4-1.2T-K9              OPERATIONAL       NSHUT
0/2               NCS1K4-1.2TL-K9             OPERATIONAL       NSHUT
0/3               NCS1K4-LC-FILLER            PRESENT           NSHUT
0/RP0/CPU0        NCS1K4-CNTLR-K9(Active)     IOS XR RUN        NSHUT
0/FT0             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/FT1             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/FT2             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/PM0             NCS1K4-AC-PSU               OPERATIONAL       NSHUT
0/PM1             NCS1K4-AC-PSU               OPERATIONAL       NSHUT
0/SC0             NCS1004                     OPERATIONAL       NSHUT
```

```
RP/0/RP0/CPU0:ios# show platform
Thu May  7 10:03:03.394 UTC
Node              Type                        State             Config state
--------------------------------------------------------------------------------
0/0               NCS1K4-1.2T-K9              OPERATIONAL       NSHUT
0/1               NCS1K4-OTN-XP               OPERATIONAL       NSHUT
0/2               NCS1K4-OTN-XP               OPERATIONAL       NSHUT
0/3               NCS1K4-OTN-XP               OPERATIONAL       NSHUT
0/RP0/CPU0        NCS1K4-CNTLR-K9(Active)     IOS XR RUN        NSHUT
0/FT0             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/FT1             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/FT2             NCS1K4-FAN                  OPERATIONAL       NSHUT
0/PM0             NCS1K4-DC-PSU               OPERATIONAL       NSHUT
0/PM1             NCS1K4-DC-PSU               OPERATIONAL       NSHUT
0/SC0             NCS1004                     OPERATIONAL       NSHUT
```

a) If Cisco IOS XR is not operational, no output is shown in the result. In this case, verify the state of service domain router (SDR) on the node using the **show sdr** command in Cisco IOS XR mode.

   The following example shows sample output of the **show sdr** command in Cisco IOS XR mode.

```
RP/0/RP0/CPU0:ios# show sdr
Wed Mar  4 06:23:16.143 UTC
Type                 NodeName       NodeState      RedState       PartnerName
--------------------------------------------------------------------------------
NCS1K4-LC-FILLER     0/0            PRESENT                       N/A
NCS1K4-1.2T-K9       0/1            OPERATIONAL                   N/A
NCS1K4-1.2TL-K9      0/2            OPERATIONAL                   N/A
NCS1K4-LC-FILLER     0/3            PRESENT                       N/A
RP                   0/RP0/CPU0     IOS XR RUN     ACTIVE         NONE
NCS1K4-CNTLR-K9      0/RP0          OPERATIONAL                   N/A
NCS1K4-FAN           0/FT0          OPERATIONAL                   N/A
NCS1K4-FAN           0/FT1          OPERATIONAL                   N/A
NCS1K4-FAN           0/FT2          OPERATIONAL                   N/A
NCS1K4-AC-PSU        0/PM0          OPERATIONAL                   N/A
NCS1K4-AC-PSU        0/PM1          OPERATIONAL                   N/A
NCS1004              0/SC0          OPERATIONAL                   N/A
```

```
RP/0/RP0/CPU0:ios# show sdr
Thu May  7 10:50:08.651 UTC
Type                 NodeName       NodeState      RedState       PartnerName
--------------------------------------------------------------------------------
NCS1K4-1.2T-K9       0/0            OPERATIONAL                   N/A
NCS1K4-OTN-XP        0/1            OPERATIONAL                   N/A
NCS1K4-OTN-XP        0/2            OPERATIONAL                   N/A
NCS1K4-OTN-XP        0/3            OPERATIONAL                   N/A
RP                   0/RP0/CPU0     IOS XR RUN     ACTIVE         NONE
NCS1K4-CNTLR-K9      0/RP0          OPERATIONAL                   N/A
NCS1K4-FAN           0/FT0          OPERATIONAL                   N/A
```

```
NCS1K4-FAN            0/FT1          OPERATIONAL                N/A
NCS1K4-FAN            0/FT2          OPERATIONAL                N/A
NCS1K4-DC-PSU         0/PM0          OPERATIONAL                N/A
NCS1K4-DC-PSU         0/PM1          OPERATIONAL                N/A
NCS1004               0/SC0          OPERATIONAL                N/A
```

Step 2 **admin**

Enters System Admin EXEC mode.

Example:

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

Step 3 **show platform**

Displays information and status of each node in the system.

Example:

```
sysadmin-vm:0_RP0# show platform
Wed Mar  4  06:24:46.700 UTC+00:00
Location  Card Type               HW State      SW State      Config State
------------------------------------------------------------------------------
0/0       NCS1K4-LC-FILLER        PRESENT       N/A           NSHUT
0/1       NCS1K4-1.2T-K9          OPERATIONAL   N/A           NSHUT
0/2       NCS1K4-1.2TL-K9         OPERATIONAL   N/A           NSHUT
0/3       NCS1K4-LC-FILLER        PRESENT       N/A           NSHUT
0/RP0     NCS1K4-CNTLR-K9         OPERATIONAL   OPERATIONAL   NSHUT
0/FT0     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/FT1     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/FT2     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/PM0     NCS1K4-AC-PSU           OPERATIONAL   N/A           NSHUT
0/PM1     NCS1K4-AC-PSU           OPERATIONAL   N/A           NSHUT
0/SC0     NCS1004                 OPERATIONAL   N/A           NSHUT

sysadmin-vm:0_RP0# show platform
Thu May  7  10:58:09.331 UTC+00:00
Location  Card Type               HW State      SW State      Config State
------------------------------------------------------------------------------
0/0       NCS1K4-1.2T-K9          OPERATIONAL   N/A           NSHUT
0/1       NCS1K4-OTN-XP           OPERATIONAL   N/A           NSHUT
0/2       NCS1K4-OTN-XP           OPERATIONAL   N/A           NSHUT
0/3       NCS1K4-OTN-XP           OPERATIONAL   N/A           NSHUT
0/RP0     NCS1K4-CNTLR-K9         OPERATIONAL   OPERATIONAL   NSHUT
0/FT0     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/FT1     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/FT2     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/PM0     NCS1K4-DC-PSU           OPERATIONAL   N/A           NSHUT
0/PM1     NCS1K4-DC-PSU           OPERATIONAL   N/A           NSHUT
0/SC0     NCS1004                 OPERATIONAL   N/A           NSHUT
```

Verify that all the components of NCS 1004 are displayed in output. The software state and the hardware state must be in the OPERATIONAL state. The various hardware and software states are:

Hardware states:

- OPERATIONAL—Node is operating normally and is fully functional.
- POWERED_ON—Power is on and the node is booting up.
- FAILED—Node is powered on but has encountered an internal failure.
- PRESENT—Node is in intermediate state in the boot sequence.

- POWERED_OFF—Power is off and the node cannot be accessed.

Software states:

- OPERATIONAL—Software is operating normally and is fully functional.
- SW_INACTIVE—Software is not completely operational.

Step 4 **show inventory**

Displays details of the physical entities of NCS 1004 along with the details of QSFPs when you execute this command in Cisco IOS XR EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# show inventory
Wed Mar  4 05:10:17.107 UTC
NAME: "0/0", DESCR: "Network Convergence System 1004 Filler"
PID: NCS1K4-LC-FILLER, VID: V01, SN: N/A

NAME: "0/1", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9, VID: V00, SN: CAT2250B0AE

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics Module"
PID: QSFP-100G-AOC3M   , VID: V03, SN: INL22262339-A

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S, VID: V03, SN: AVF2219S16U

NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: JFQ2145701U

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S, VID: ES1, SN: AVF1925G012

NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: JFQ2145706N

NAME: "0/1-Optics0/1/0/8", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4, VID: V01, SN: JFQ19026014

NAME: "0/1-Optics0/1/0/9", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: OPM220518HS

NAME: "0/1-Optics0/1/0/10", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: INL21490043

NAME: "0/1-Optics0/1/0/11", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V01, SN: JFQ211930JL

NAME: "0/1-Optics0/1/0/12", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S, VID: V02, SN: JFQ2210801H

NAME: "0/2", DESCR: "NCS1K4 12x QSFP28 2 Trunk L-Band DWDM card"
PID: NCS1K4-1.2TL-K9   , VID: V00, SN: CAT2337B0S4

NAME: "0/2-Optics0/2/0/2", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL22262332-A

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: FNS22070HWF

NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
```

```
PID: QSFP-100G-SM-SR, VID: V02, SN: SPT2225302D

NAME: "0/2-Optics0/2/0/6", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: FNS22310Z1X

NAME: "0/2-Optics0/2/0/8", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4, VID: V01, SN: FNS20520R8Z

NAME: "0/2-Optics0/2/0/9", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL23312282-A

NAME: "0/2-Optics0/2/0/10", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL23312282-B

NAME: "0/2-Optics0/2/0/11", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: FNS23080LKF

NAME: "0/3", DESCR: "Network Convergence System 1004 Filler"
PID: NCS1K4-LC-FILLER, VID: V01, SN: N/A

:
:
:

RP/0/RP0/CPU0:ios# show inventory
Thu May  7 11:05:13.211 UTC
NAME: "0/0", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9    , VID: V00, SN: CAT2237B25A

NAME: "0/0-Optics0/0/0/2", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS2333080E

NAME: "0/0-Optics0/0/0/3", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23330801

NAME: "0/0-Optics0/0/0/4", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS21140GZK

NAME: "0/0-Optics0/0/0/6", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS233209CN

NAME: "0/0-Optics0/0/0/10", DESCR: "Cisco 40GE QSFP+ LR4 Pluggable Optics Module"
PID: QSFP-40G-LR4      , VID: V02, SN: FNS23110TYD

NAME: "0/1", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B007

NAME: "0/1-Optics0/1/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS2333080J

NAME: "0/1-Optics0/1/0/1", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23330806

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010391

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ20332007

NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ20332088

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010471
```

```
NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010376

NAME: "0/2", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B015

NAME: "0/2-Optics0/2/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS20360V1R

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ21502017

NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ202120DY

NAME: "0/3", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B00A

NAME: "0/3-Optics0/3/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23320BS3

NAME: "0/3-Optics0/3/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: AVP2217S09L

NAME: "0/3-Optics0/3/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: AVP2107S0RZ

NAME: "0/RP0", DESCR: "Network Convergence System 1004 Controller"
PID: NCS1K4-CNTLR-K9   , VID: V01, SN: CAT2323B0SG
:
:
:
:
NAME: "0/PM1", DESCR: "Network Convergence System 1004 DC Power Supply Unit"
PID: NCS1K4-DC-PSU     , VID: V01, SN: POG2308CT4W
```

Verify Software Version

NCS 1004 is shipped with the Cisco IOS XR Software preinstalled. Verify that the latest version of the software is installed. If a newer version is available, perform a Perform System Upgrade and Install Feature Packages. This system upgrade installs the newer version of the software and provide the latest feature set on NCS 1004.

To verify the version of Cisco IOS XR Software running on NCS 1004, perform the following procedure.

Procedure

show version

Displays the software version and details such as system uptime.

Example:

```
RP/0/RP0/CPU0:ios# show version
Wed Feb 10 19:35:38.274 IST
Cisco IOS XR Software, Version 7.3.2
Copyright (c) 2013-2021 by Cisco Systems, Inc.
```

```
Build Information:
 Built By     : ingunawa
 Built On     : Tue Feb  9 11:45:12 PST 2021
 Built Host   : iox-lnx-068
 Workspace    : /auto/iox-lnx-068-san1/prod/7.3.2/ncs1k/ws
 Version      : 7.3.2
 Location     : /opt/cisco/XR/packages/
 Label        : 7.3.2

cisco NCS-1002 () processor
System uptime is 3 hours 37 minutes
```

What to do next

Verify the software version to determine whether system upgrade is required. If the upgrade is required, see the Perform System Upgrade and Install Feature Packages chapter.

Verify Firmware Version

The firmware on various hardware components of NCS 1004 must be compatible with the installed Cisco IOS XR image. Incompatibility may cause the NCS 1004 to malfunction.

To verify the firmware version, perform the following procedure.

Procedure

Step 1 **show hw-module fpd**

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Fri Nov 26 14:53:27.188 UTC

Auto-upgrade:Disabled
                                                                                FPD Versions
                                                                                ==============
Location   Card type              HWver FPD device       ATR Status    Running   Programd
-------------------------------------------------------------------------------------------
0/0        NCS1K4-OTN-XPL         3.0   LC_CPU_MOD_FW        CURRENT    75.10     75.10
0/0        NCS1K4-OTN-XPL         7.0   LC_DP_MOD_FW         CURRENT     3.10      3.10
0/0        NCS1K4-OTN-XPL         2.0   LC_QSFPDD_PORT_11    CURRENT    61.2013   61.2013
0/0        NCS1K4-OTN-XPL         2.0   LC_QSFPDD_PORT_9     CURRENT    61.2013   61.2013
0/1        NCS1K4-OTN-XP          2.0   LC_CPU_MOD_FW        CURRENT    75.10     75.10
0/1        NCS1K4-OTN-XP          7.0   LC_DP_MOD_FW         CURRENT     3.10      3.10
0/1        NCS1K4-OTN-XP          2.0   LC_QSFPDD_PORT_11    CURRENT    61.2013   61.2013
0/1        NCS1K4-OTN-XP          2.0   LC_QSFPDD_PORT_9     CURRENT    61.2013   61.2013
0/RP0      NCS1K4-CNTLR-K9        5.0   CSB_IMG           S  CURRENT     0.200     0.200
0/RP0      NCS1K4-CNTLR-K9        5.0   TAM_FW               CURRENT    36.08     36.08
0/RP0      NCS1K4-CNTLR-K9        1.14  BIOS              S  CURRENT     5.30      5.30
0/RP0      NCS1K4-CNTLR-K9        5.0   CPU_FPGA             CURRENT     1.14      1.14
0/PM1      NCS1K4-AC-PSU          0.1   PO-PriMCU            CURRENT     2.70      2.70
0/SC0      NCS1004                2.0   BP_FPGA              CURRENT     1.25      1.25
0/SC0      NCS1004                2.0   XGE_FLASH            CURRENT    18.04     18.04
```

Displays firmware information of various hardware components of NCS 1004 in the Cisco IOS XR EXEC mode.

In the previous 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.
  - NOT READY—The firmware of the FPD is not ready for upgrade.
  - NEED UPGD—A newer firmware version is available in the installed image. We recommended that upgrade be performed.
  - UPGD PREP—The firmware of the FPD is preparing for upgrade.
  - RLOAD REQ—The upgrade is completed, and the card requires a reload.
  - UPGD DONE—The firmware upgrade is successful.
  - UPGD FAIL—The firmware upgrade has failed.
  - UPGD SKIP—The upgrade is skipped because the installed firmware version is higher than the version available in the image.
  - Running—Current version of the firmware running on the FPD.

Step 2 **show fpd package**

Use the **show fpd package** command to display the FPD image version available with this software release for each hardware component.

```
RP/0/RP0/CPU0:ios# show fpd package
Fri May  8 05:11:47.819 UTC

================================ ================================================
                                        Field Programmable Device Package
                                 ================================================
                                              Req     SW      Min Req   Min Req
Card Type            FPD Description          Reload  Ver     SW Ver  Board Ver
================== ========================== ====== ======= ======== =========
--------------------------------------------------------------------------------
NCS1004-K9           BP_FPGA(A)                NO      1.25    1.25    0.0
                     XGE_FLASH(A)              YES    18.04   18.04    0.0
--------------------------------------------------------------------------------
NCS1K4-1.2T-K9       LC_CPU_MOD_FW(A)          YES    75.10   75.10    0.0
                     LC_OPT_MOD_FW(A)          YES     1.25    1.25    0.0
--------------------------------------------------------------------------------
NCS1K4-1.2T-L-K9     LC_CPU_MOD_FW(A)          YES    75.10   75.10    0.0
                     LC_OPT_MOD_FW(A)          YES     1.25    1.25    0.0
--------------------------------------------------------------------------------
NCS1K4-1.2TL-K9      LC_CPU_MOD_FW(A)          YES    75.10   75.10    0.0
                     LC_OPT_MOD_FW(A)          YES     1.25    1.25    0.0
--------------------------------------------------------------------------------
NCS1K4-2-QDD-C-K9    LC_CPU_MOD_FW(A)          YES    75.10   75.10    0.0
```

```
                     LC_OPT_MOD_FW(A)           YES     1.26    1.26    0.0
--------------------------------------------------------------------------------
NCS1K4-2KW-AC        PO-PriMCU(A)               NO      2.70    2.70    0.0
                     PO-PriMCU(A)               NO      2.70    2.70    0.1
--------------------------------------------------------------------------------
NCS1K4-AC-PSU        PO-PriMCU(A)               NO      2.70    2.70    0.0
                     PO-PriMCU(A)               NO      2.70    2.70    0.1
--------------------------------------------------------------------------------
NCS1K4-CNTLR         BIOS(A)                    YES     5.30    5.30    1.5
                     CSB_IMG                    YES     0.200   0.200   0.0
--------------------------------------------------------------------------------
NCS1K4-CNTLR-B-K9    BIOS(A)                    YES     5.30    5.30    1.0
                     CSB_IMG                    YES     0.200   0.200   0.0
--------------------------------------------------------------------------------
NCS1K4-DC-PSU        PO-PriMCU(A)               NO      1.12    1.12    0.0
                     PO-PriMCU(A)               NO      1.12    1.12    0.1
--------------------------------------------------------------------------------
NCS1K4-OTN-XP        LC_CFP2_PORT_0(A)          NO      0.00    0.00    0.0
   LC_CFP2_PORT_0(A)           NO      1.00    1.00    1.0
                     LC_CFP2_PORT_0(A)          NO      1.52    1.52    2.0
                     LC_CFP2_PORT_1(A)          NO      0.00    0.00    0.0
                     LC_CFP2_PORT_1(A)          NO      1.00    1.00    1.0
                     LC_CFP2_PORT_1(A)          NO      1.52    1.52    2.0
                     LC_CPU_MOD_FW(A)           YES     75.10   75.10   0.0
                     LC_DP_MOD_FW(A)            YES     3.10    3.10    1.0
                     LC_DP_MOD_FW(A)            YES     11.10   11.10   2.0
                     LC_DP_MOD_FW(A)            YES     11.10   11.10   3.0
                     LC_DP_MOD_FW(A)            YES     1.10    1.10    4.0
                     LC_DP_MOD_FW(A)            YES     3.10    3.10    7.0
                     LC_DP_MOD_FW(A)            YES     1.10    1.10    8.0
                     LC_QSFPDD_PORT_11(A)        NO     0.00    0.00    0.0
                     LC_QSFPDD_PORT_11(A)        NO     61.2013 61.2013 1.0
                     LC_QSFPDD_PORT_11(A)        NO     61.2013 61.2013 2.0
                     LC_QSFPDD_PORT_9(A)         NO     0.00    0.00    0.0
                     LC_QSFPDD_PORT_9(A)         NO     61.2013 61.2013 1.0
                     LC_QSFPDD_PORT_9(A)         NO     61.2013 61.2013 2.0
--------------------------------------------------------------------------------
NCS1K4-OTN-XPL       LC_CFP2_PORT_0(A)          NO      0.00    0.00    0.0
   LC_CFP2_PORT_0(A)           NO      1.00    1.00    1.0
                     LC_CFP2_PORT_0(A)          NO      1.52    1.52    2.0
                     LC_CFP2_PORT_1(A)          NO      0.00    0.00    0.0
                     LC_CFP2_PORT_1(A)          NO      1.00    1.00    1.0
                     LC_CFP2_PORT_1(A)          NO      1.52    1.52    2.0
                     LC_CPU_MOD_FW(A)           YES     75.10   75.10   0.0
                     LC_DP_MOD_FW(A)            YES     3.10    3.10    1.0
                     LC_DP_MOD_FW(A)            YES     11.10   11.10   2.0
                     LC_DP_MOD_FW(A)            YES     11.10   11.10   3.0
                     LC_DP_MOD_FW(A)            YES     1.10    1.10    4.0
                     LC_DP_MOD_FW(A)            YES     3.10    3.10    7.0
                     LC_DP_MOD_FW(A)            YES     1.10    1.10    8.0
                     LC_QSFPDD_PORT_11(A)        NO     0.00    0.00    0.0
                     LC_QSFPDD_PORT_11(A)        NO     61.2013 61.2013 1.0
                     LC_QSFPDD_PORT_11(A)        NO     61.2013 61.2013 2.0
                     LC_QSFPDD_PORT_9(A)         NO     0.00    0.00    0.0
                     LC_QSFPDD_PORT_9(A)         NO     61.2013 61.2013 1.0
                     LC_QSFPDD_PORT_9(A)         NO     61.2013 61.2013 2.0
--------------------------------------------------------------------------------
NCS1K4-TESTUNIT      LC_CPU_MOD_FW(A)           YES     0.01    0.01    0.0
```

What to do next

Upgrade all the FPDs using the **upgrade hw-module location all fpd all** command in the Cisco IOS XR EXEC mode. After upgrade is completed, the Status column shows RLOAD REQ if the software requires reload.

If Reload is required

If the FPGA location is 0/RP0, use the **admin hw-module location 0/RP0 reload** command. This command reboots only the CPU. As a result, traffic is not impacted. If the FPGA location is 0/0, use the **admin hw-module location all reload** command. This command reboots the chassis. As a result, traffic is impacted. After the reload is completed, the new FPGA runs the current version.

Caution The upgrade of OTNXP LC_DP_MOD_FW and LC_OPT_MOD_FW FPDs affect traffic. Hence, you must perform this upgrade during a maintenance window.

If Firmware Upgrade Fails

If firmware upgrade fails, use the **show logging** command to view the details and upgrade the firmware again using the above commands.

Note You can upgrade the firmware version of power modules, only when both the power modules are present and powered on.

Verify Management Interface Status

To verify the management interface status, perform the following procedure.

Procedure

show interfaces mgmtEth *instance*

Displays the management interface configuration.

Example:

```
RP/0/RP0/CPU0:ios# show interfaces MgmtEth 0/RP0/CPU0/0
Wed Mar  4 06:13:12.381 UTC
MgmtEth0/RP0/CPU0/0 is up, line protocol is up
  Interface state transitions: 1
  Hardware is Management Ethernet, address is b026.80ff.d870 (bia b026.80ff.d870)
  Internet address is 10.127.60.184/24
  MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 1000Mb/s, CX, link type is autonegotiation
  loopback not set,
  Last link flapped 1d23h
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
```

```
  5 minute input rate 1368000 bits/sec, 193 packets/sec
  5 minute output rate 95000 bits/sec, 194 packets/sec
     6447256 packets input, 3947875102 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 661276 broadcast packets, 271649 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7190033 packets output, 3906991430 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
```

```
RP/0/RP0/CPU0:ios# show interfaces MgmtEth 0/RP0/CPU0/0
Fri May  8 04:40:41.519 UTC
MgmtEth0/RP0/CPU0/0 is up, line protocol is up
  Interface state transitions: 1
  Hardware is Management Ethernet, address is dc8c.37c3.e1a8 (bia dc8c.37c3.e1a8)
  Internet address is 10.105.57.103/25
  MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 1000Mb/s, CX, link type is autonegotiation
  loopback not set,
  Last link flapped 1d04h
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 106000 bits/sec, 140 packets/sec
  5 minute output rate 108000 bits/sec, 139 packets/sec
     7303357 packets input, 696872907 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 40679 broadcast packets, 41523 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7231570 packets output, 740818886 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
          MgmtEth0/RP0/CPU0/0 is up, line protocol is up
```

In the previous output, the management interface is administratively down.

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

The following example shows sample output from the **show interfaces summary** command.

```
RP/0/RP0/CPU0:ios# show interfaces summary
Wed Mar  4 06:14:52.995 UTC
Interface Type          Total    UP       Down     Admin Down
--------------          -----    --       ----     ----------
ALL TYPES               4        2        0        2
--------------
IFT_ETHERNET            3        1        0        2
IFT_NULL                1        1        0        0
```

```
RP/0/RP0/CPU0:ios# show interfaces summary
Fri May  8 04:43:57.355 UTC
Interface Type          Total    UP       Down     Admin Down
--------------          -----    --       ----     ----------
ALL TYPES               6        5        0        1
--------------
IFT_LOOPBACK            2        2        0        0
```

```
IFT_ETHERNET            3        2        0        1
IFT_NULL                1        1        0        0
```

The following example shows sample output from the **show interfaces brief** command.

```
RP/0/RP0/CPU0:ios# show interfaces brief
Wed Mar  4 06:15:51.689 UTC

               Intf       Intf        LineP              Encap  MTU        BW
               Name       State       State               Type (byte)    (Kbps)
--------------------------------------------------------------------------------
                Nu0          up          up               Null  1500           0
     Mg0/RP0/CPU0/0          up          up               ARPA  1514     1000000
     Mg0/RP0/CPU0/1  admin-down  admin-down               ARPA  1514     1000000
     Mg0/RP0/CPU0/2  admin-down  admin-down               ARPA  1514     1000000

RP/0/RP0/CPU0:ios# show interfaces brief
Fri May  8 04:44:41.558 UTC

               Intf       Intf        LineP              Encap  MTU        BW
               Name       State       State               Type (byte)    (Kbps)
--------------------------------------------------------------------------------
                Lo0          up          up           Loopback  1500           0
                Lo1          up          up           Loopback  1500           0
                Nu0          up          up               Null  1500           0
     Mg0/RP0/CPU0/0          up          up               ARPA  1514     1000000
     Mg0/RP0/CPU0/1  admin-down  admin-down               ARPA  1514     1000000
     Mg0/RP0/CPU0/2          up          up               ARPA  1514     1000000
```

What to do next

If the management interface is administratively down, perform the following steps:

- Check the Ethernet cable connection.
- Verify the IP configuration of the management interface. For details on configuring the management interface, see Configure Management Interface.
- Verify whether the management interface is in the no shut state using the **show running-config interface mgmtEth** command.

  The following example shows sample output from the **show running-config interface mgmtEth** command.

  ```
  RP/0/RP0/CPU0:ios#show running-config interface mgmtEth 0/RP0/CPU0/0
  Wed Mar  4 06:17:33.833 UTC
  interface MgmtEth0/RP0/CPU0/0
   ipv4 address dhcp
  !

  RP/0/RP0/CPU0:ios#show running-config interface mgmtEth 0/RP0/CPU0/0
  Fri May  8 04:46:29.582 UTC
  interface MgmtEth0/RP0/CPU0/0
   ipv4 address 10.105.57.103 255.255.255.128
  !
  ```

  In the previous output, the management interface is in the no shut state.

Verify Alarms

You can view the alarm information using the **show alarms** command.

Procedure

show alarms [**brief** [**card | rack | system**] [**location** *location*] [**active | history**] | **detail** [**card | rack | system**] [**location** *location*] [**active | clients | history | stats**]]

Displays alarms in brief or detail.

Example:

```
RP/0/RP0/CPU0:ios# show alarms brief card location 0/RP0/CPU0 active

Wed Mar  4 06:10:55.959 UTC

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

------------------------------------------------------------------------------------
0/1             Major        FPD_Infra        03/02/2020 07:09:04 UTC    One Or More FPDs
Need Upgrade Or Not In Current State

0/2             Major        FPD_Infra        03/03/2020 14:27:33 UTC    One Or More FPDs
Need Upgrade Or Not In Current State

0/2             Major        Ethernet         03/03/2020 20:33:33 UTC
HundredGigECtrlr0/2/0/9 - Carrier Loss On The LAN

0/2             Critical     Controller       03/03/2020 20:34:05 UTC    Optics0/2/0/3 -
Improper Removal

0/2             NotAlarmed   OTN              03/03/2020 20:34:08 UTC    ODU40/2/0/0/2 -
OPUK Client Signal Failure

0/2             NotAlarmed   OTN              03/03/2020 20:34:05 UTC    ODU40/2/0/1/2 -
OPUK Client Signal Failure
```

```
RP/0/RP0/CPU0:ios# show alarms brief card location 0/RP0/CPU0 active

Fri May  8 04:46:29.582 UTC

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

------------------------------------------------------------------------------------
0/2             NotReported  OTN              05/07/2020 14:25:05 UTC    ODU20/2/0/0/2/3 -
 Path Monitoring Alarm Indication Signal

0/2             NotReported  OTN              05/07/2020 14:25:05 UTC    ODU2E0/2/0/0/2/4
- Path Monitoring Alarm Indication Signal

0/1             NotReported  OTN              05/07/2020 14:24:41 UTC    ODU20/1/0/0/2/3 -
 Path Monitoring Alarm Indication Signal
```

```
0/1             NotReported  OTN              05/07/2020 14:25:03 UTC    ODU20/1/0/1/11/3
- Path Monitoring Alarm Indication Signal

0/1             NotReported  OTN              05/07/2020 14:25:03 UTC    ODU2E0/1/0/1/11/4
 - Path Monitoring Alarm Indication Signal

0/3             NotReported  OTN              05/07/2020 14:24:41 UTC    ODU20/3/0/0/2/3 -
 Path Monitoring Alarm Indication Signal

0/3             NotReported  OTN              05/07/2020 14:24:41 UTC    ODU2E0/3/0/0/2/4
- Path Monitoring Alarm Indication Signal

0/1           Major       Ethernet        05/07/2020 14:24:41 UTC    TenGigECtrlr0/1/0/4/1
 - Remote Fault
```

Note In the maintenance mode, all the alarms are suppressed and the **show alarms** command will not show the alarms details. Use the **show controllers** *controllertype R/S/I/P* command to view the client and trunk alarms.

Verify Environmental Parameters

The **show environment** command displays the environmental parameters of NCS 1004.

To verify that the environmental parameters are as expected, perform the following procedure.

Procedure

Step 1 **admin**

Enters System Admin EXEC mode.

Example:

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

Step 2 **show environment** [**all** | **altitude** | **fan** | **power** | **voltages** | **current** | **temperatures**] [**location** | *location*]

Displays the environmental parameters of NCS 1004.

Example:

The following example shows sample output of the **show environment** command with the **fan** keyword.

```
sysadmin-vm:0_RP0# show environment fan
Wed Mar  4  05:36:33.678 UTC+00:00
=============================================
                        Fan speed (rpm)
Location     FRU Type           FAN_0   FAN_1
---------------------------------------------
0/FT0        NCS1K4-FAN          7020    6930
0/FT1        NCS1K4-FAN          6780    6690
0/FT2        NCS1K4-FAN          6810    6720

0/PM0        NCS1K4-AC-PSU      25376   24352
```

```
0/PM1        NCS1K4-AC-PSU      11200   11232

sysadmin-vm:0_RP0# show environment fan
Thu May  7  11:47:11.490 UTC+00:00
=============================================
                       Fan speed (rpm)
Location     FRU Type           FAN_0   FAN_1
---------------------------------------------
0/FT0        NCS1K4-FAN         11070   11070
0/FT1        NCS1K4-FAN         11220   11040
0/FT2        NCS1K4-FAN         11250   11070

0/PM0        NCS1K4-DC-PSU      12624   12576

0/PM1        NCS1K4-DC-PSU      24704   25312
```

The following example shows sample output of the **show environment** command with the **temperatures** keyword.

```
sysadmin-vm:0_RP0# show environment temperatures location 0/RP0
Wed Mar  4  05:44:51.221 UTC+00:00
=================================================================================
Location  TEMPERATURE                Value   Crit Major Minor Minor Major  Crit
          Sensor                   (deg C)   (Lo) (Lo)  (Lo)  (Hi)  (Hi)   (Hi)
---------------------------------------------------------------------------------
0/RP0
          TEMP_LOCAL                  32    -10    -5     0    55    65    70
          TEMP_REMOTE1                32    -10    -5     0    55    65    70
          TEMP_CPU_DIE                31    -10    -5     0    75    80    90

sysadmin-vm:0_RP0# show environment temperatures location 0/RP0
Thu May  7  11:50:23.172 UTC+00:00
=================================================================================
Location  TEMPERATURE                Value   Crit Major Minor Minor Major  Crit
          Sensor                   (deg C)   (Lo) (Lo)  (Lo)  (Hi)  (Hi)   (Hi)
---------------------------------------------------------------------------------
0/RP0
          TEMP_LOCAL                  36    -10    -5     0    55    65    70
          TEMP_REMOTE1                36    -10    -5     0    55    65    70
          TEMP_CPU_DIE                37    -10    -5     0    75    80    90
```

The following example shows sample output of the **show environment** command with the **power** keyword.

```
sysadmin-vm:0_RP0# show environment power
Wed Mar  4  05:45:35.640 UTC+00:00
=================================================================================
CHASSIS LEVEL POWER INFO: 0
=================================================================================
   Total output power capacity (N + 1)             :    2000W +       0W
   Total output power required                     :     910W
   Total power input                               :     456W
   Total power output                              :     407W

Power Group 0:
=================================================================================
   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
=================================================================================
   0/PM0       2kW-AC        0.0      0.0      0.0      0.0    FAILED or NO PWR

Total of Power Group 0:          0W/  0.0A         0W/  0.0A

Power Group 1:
=================================================================================
   Power       Supply     ------Input----   ------Output---      Status
```

```
   Module      Type        Volts     Amps    Volts     Amps
================================================================================
   0/PM1       2kW-AC      227.8      2.0     12.0     33.9    OK

Total of Power Group 1:        456W/  2.0A       407W/ 33.9A

================================================================================
   Location     Card Type            Power       Power       Status
                                     Allocated   Used
                                     Watts       Watts
================================================================================
   0/0          NCS1K4-LC-FILLER       0           -       RESERVED
   0/1          NCS1K4-1.2T-K9       260         101       ON
   0/2          NCS1K4-1.2TL-K9      260         168       ON
   0/3          NCS1K4-LC-FILLER       0           -       RESERVED
   0/RP0        NCS1K4-CNTLR-K9       55           -       ON
   0/FT0        NCS1K4-FAN           100           -       ON
   0/FT1        NCS1K4-FAN           100           -       ON
   0/FT2        NCS1K4-FAN           100           -       ON
   0/SC0        NCS1004               35           -       ON

sysadmin-vm:0_RP0# show environment power
Thu May  7  11:55:13.388 UTC+00:00
================================================================================
CHASSIS LEVEL POWER INFO: 0
================================================================================
   Total output power capacity (N + 1)             :    2000W +       0W
   Total output power required                     :    1670W
   Total power input                               :    1007W
   Total power output                              :     956W

Power Group 0:
================================================================================
   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
================================================================================
   0/PM0       2kW-DC       50.3     20.0     12.1     79.0    OK

Total of Power Group 0:       1006W/ 20.0A       956W/ 79.0A

Power Group 1:
================================================================================
   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
================================================================================
   0/PM1       2kW-DC        1.3      0.6      0.0      0.0    FAILED or NO PWR

Total of Power Group 1:          1W/  0.6A         0W/  0.0A

================================================================================
   Location     Card Type            Power       Power       Status
                                     Allocated   Used
                                     Watts       Watts
================================================================================
   0/0          NCS1K4-1.2T-K9       260         194       ON
   0/1          NCS1K4-OTN-XP        340         182       ON
   0/2          NCS1K4-OTN-XP        340         153       ON
   0/3          NCS1K4-OTN-XP        340         160       ON
   0/RP0        NCS1K4-CNTLR-K9       55           -       ON
   0/FT0        NCS1K4-FAN           100           -       ON
   0/FT1        NCS1K4-FAN           100           -       ON
   0/FT2        NCS1K4-FAN           100           -       ON
   0/SC0        NCS1004               35           -       ON
```

The following example shows sample output of the **show environment** command with the **voltages** keyword.

```
sysadmin-vm:0_RP0# show environment voltages location 0/RP0
Wed Mar  4  05:47:24.668 UTC+00:00
================================================================================
Location  VOLTAGE                      Value   Crit Minor Minor  Crit
          Sensor                       (mV)    (Lo) (Lo)  (Hi)   (Hi)
--------------------------------------------------------------------------------
0/RP0
          ADM1266_VH1_12V             12028  10800 11040 12960 13200
          ADM1266_VH3_3V3              3306   3036  3135  3465  3564
          ADM1266_VH4_2V5              2492   2300  2375  2625  2700
          ADM1266_VP1_1V8              1801   1656  1710  1890  1944
          ADM1266_VP2_1V2              1201   1104  1140  1260  1296
          ADM1266_3V3_STAND_BY         3293   3036  3135  3465  3564
          ADM1266_VP4_3V3_CPU          3301   3036  3135  3465  3564
          ADM1266_VP5_2V5_CPU          2494   2300  2375  2625  2700
          ADM1266_VP6_1V8_CPU          1797   1656  1710  1890  1944
          ADM1266_VP7_1V24_VCCREF      1236   1140  1178  1302  1339
          ADM1266_VP8_1V05_CPU         1045    966   997  1102  1134
          ADM1266_VP9_1V2_DDR_VDDQ     1196   1104  1140  1260  1296
          ADM1266_VP10_1V0_VCCRAM      1074    500   650  1300  1400
          ADM1266_VP11_VNN              882    400   550  1300  1400
          ADM1266_VP12_VCCP            1068    300   450  1300  1400
          ADM1266_VP13_0V6_VTT          599    552   570   630   648
          ADM1293_DB_5V0               5007   4600  4750  5250  5400
          ADM1293_DB_3V3               3305   3036  3135  3465  3564
          ADM1293_DB_5V0_USB_0         5007   4000  4500  5500  6000
          ADM1293_DB_5V0_USB_1         5017   4000  4500  5500  6000
          ADM1293_MB_5V0_PMOD0         5062   4600  4750  5250  5400
          ADM1293_MB_5V0_PMOD1         5032   4600  4750  5250  5400
          ADM1293_MB_2V5_PLL           2483   2300  2375  2625  2700
```

```
sysadmin-vm:0_RP0# show environment voltages location 0/RP0
Thu May  7  11:57:18.650 UTC+00:00
================================================================================
Location  VOLTAGE                      Value   Crit Minor Minor  Crit
          Sensor                       (mV)    (Lo) (Lo)  (Hi)   (Hi)
--------------------------------------------------------------------------------
0/RP0
          ADM1266_VH1_12V             11961  10800 11040 12960 13200
          ADM1266_VH3_3V3              3306   3036  3135  3465  3564
          ADM1266_VH4_2V5              2487   2300  2375  2625  2700
          ADM1266_VP1_1V8              1795   1656  1710  1890  1944
          ADM1266_VP2_1V2              1198   1104  1140  1260  1296
          ADM1266_3V3_STAND_BY         3301   3036  3135  3465  3564
          ADM1266_VP4_3V3_CPU          3299   3036  3135  3465  3564
          ADM1266_VP5_2V5_CPU          2489   2300  2375  2625  2700
          ADM1266_VP6_1V8_CPU          1788   1656  1710  1890  1944
          ADM1266_VP7_1V24_VCCREF      1233   1140  1178  1302  1339
          ADM1266_VP8_1V05_CPU         1046    966   997  1102  1134
          ADM1266_VP9_1V2_DDR_VDDQ     1200   1104  1140  1260  1296
          ADM1266_VP10_1V0_VCCRAM      1039    500   650  1300  1400
          ADM1266_VP11_VNN              850    400   550  1300  1400
          ADM1266_VP12_VCCP            1056    300   450  1300  1400
          ADM1266_VP13_0V6_VTT          600    552   570   630   648
          ADM1293_DB_5V0               4998   4600  4750  5250  5400
          ADM1293_DB_3V3               3315   3036  3135  3465  3564
          ADM1293_DB_5V0_USB_0         4998   4000  4500  5500  6000
          ADM1293_DB_5V0_USB_1         5047   4000  4500  5500  6000
          ADM1293_MB_5V0_PMOD0         5044   4600  4750  5250  5400
          ADM1293_MB_5V0_PMOD1         5026   4600  4750  5250  5400
          ADM1293_MB_2V5_PLL           2515   2300  2375  2625  2700
```

What to do next

Environment parameter anomalies are logged in the syslog. As a result, if an environment parameter displayed in the **show environment** command output is not as expected, check the syslog using the **show logging** command. The syslog provides details on any logged problems.

Verify Inventory

The **show inventory** command displays details of the hardware inventory of NCS 1004.

To verify the inventory information for all the physical entities, perform the following procedure.

Procedure

Step 1 **show inventory**

Displays the details of NCS 1004 when you execute this command in the Cisco IOS XR EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# show inventory
Wed Mar  4 05:10:17.107 UTC
NAME: "0/0", DESCR: "Network Convergence System 1004 Filler"
PID: NCS1K4-LC-FILLER, VID: V01, SN: N/A

NAME: "0/1", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9, VID: V00, SN: CAT2250B0AE

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics Module"
PID: QSFP-100G-AOC3M   , VID: V03, SN: INL22262339-A

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S, VID: V03, SN: AVF2219S16U

NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: JFQ2145701U

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S, VID: ES1, SN: AVF1925G012

NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: JFQ2145706N

NAME: "0/1-Optics0/1/0/8", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4, VID: V01, SN: JFQ19026014

NAME: "0/1-Optics0/1/0/9", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: OPM220518HS

NAME: "0/1-Optics0/1/0/10", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: INL21490043

NAME: "0/1-Optics0/1/0/11", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S , VID: V01, SN: JFQ211930JL

NAME: "0/1-Optics0/1/0/12", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics Module"
PID: QSFP-100G-CWDM4-S, VID: V02, SN: JFQ2210801H

NAME: "0/2", DESCR: "NCS1K4 12x QSFP28 2 Trunk L-Band DWDM card"
```

```
PID: NCS1K4-1.2TL-K9   , VID: V00, SN: CAT2337B0S4

NAME: "0/2-Optics0/2/0/2", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL22262332-A

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: FNS22070HWF

NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: SPT2225302D

NAME: "0/2-Optics0/2/0/6", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: FNS22310Z1X

NAME: "0/2-Optics0/2/0/8", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4, VID: V01, SN: FNS20520R8Z

NAME: "0/2-Optics0/2/0/9", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL23312282-A

NAME: "0/2-Optics0/2/0/10", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL23312282-B

NAME: "0/2-Optics0/2/0/11", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: FNS23080LKF

NAME: "0/3", DESCR: "Network Convergence System 1004 Filler"
PID: NCS1K4-LC-FILLER, VID: V01, SN: N/A

NAME: "0/RP0", DESCR: "Network Convergence System 1004 Controller"
PID: NCS1K4-CNTLR-K9, VID: V00, SN: CAT2231B069

NAME: "0/SC0", DESCR: "Network Convergence System 1004 Chassis"
PID: NCS1004, VID: V00, SN: CAT2231B192

NAME: "Rack 0", DESCR: "Network Convergence System 1004 Chassis"
PID: NCS1004, VID: V00, SN: CAT2231B192

NAME: "0/FT0", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN, VID: V00, SN: CAT2231B2GL

NAME: "0/FT1", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN, VID: V00, SN: CAT2231B2H4

NAME: "0/FT2", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN, VID: V00, SN: CAT2231B2GW

NAME: "0/PM0", DESCR: "Network Convergence System 1004 AC Power Supply Unit"
PID: NCS1K4-AC-PSU, VID: V00, SN: POG2221CL1V

NAME: "0/PM1", DESCR: "Network Convergence System 1004 AC Power Supply Unit"
PID: NCS1K4-AC-PSU, VID: V00, SN: POG2221CL04

RP/0/RP0/CPU0:ios# show inventory
Thu May  7 11:37:33.960 UTC
NAME: "0/0", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9    , VID: V00, SN: CAT2237B25A

NAME: "0/0-Optics0/0/0/2", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS2333080E

NAME: "0/0-Optics0/0/0/3", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23330801

NAME: "0/0-Optics0/0/0/4", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
```

```
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS21140GZK

NAME: "0/0-Optics0/0/0/6", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS233209CN

NAME: "0/0-Optics0/0/0/10", DESCR: "Cisco 40GE QSFP+ LR4 Pluggable Optics Module"
PID: QSFP-40G-LR4      , VID: V02, SN: FNS23110TYD

NAME: "0/1", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B007

NAME: "0/1-Optics0/1/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS2333080J

NAME: "0/1-Optics0/1/0/1", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23330806

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010391

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ20332007

NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ20332088

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010471

NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010376

NAME: "0/2", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B015

NAME: "0/2-Optics0/2/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS20360V1R

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ21502017

NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ202120DY

NAME: "0/3", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B00A

NAME: "0/3-Optics0/3/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23320BS3

NAME: "0/3-Optics0/3/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: AVP2217S09L

NAME: "0/3-Optics0/3/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics Module"
PID: QSFP-40G-SR4      , VID: V03, SN: AVP2107S0RZ

NAME: "0/RP0", DESCR: "Network Convergence System 1004 Controller"
PID: NCS1K4-CNTLR-K9   , VID: V01, SN: CAT2323B0SG

NAME: "0/RP0-SFP-Port", DESCR: "Cisco SFP Pluggable Optics Module"
PID: SFP-GE-S          , VID: V01, SN: FNS15512KVG

NAME: "0/SC0", DESCR: "Network Convergence System 1004 4 line card slots"
PID: NCS1004           , VID: V01, SN: CAT2323B0DC
```

```
NAME: "Rack 0", DESCR: "Network Convergence System 1004 4 line card slots"
PID: NCS1004           , VID: V01, SN: CAT2323B0DC

NAME: "0/FT0", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V01, SN: CAT2325B1NW

NAME: "0/FT1", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V01, SN: CAT2324B0Z6

NAME: "0/FT2", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V01, SN: CAT2324B0Z8

NAME: "0/PM0", DESCR: "Network Convergence System 1004 DC Power Supply Unit"
PID: NCS1K4-DC-PSU     , VID: V01, SN: POG2310CT00

NAME: "0/PM1", DESCR: "Network Convergence System 1004 DC Power Supply Unit"
PID: NCS1K4-DC-PSU     , VID: V01, SN: POG2308CT4W
```

Step 2 **admin**

Enters System Admin EXEC mode.

Example:

Step 3 **show inventory**

Displays inventory information for all the physical entities of NCS 1004.

Example:

```
sysadmin-vm:0_RP0# show inventory
Wed Mar  4  05:27:26.231 UTC+00:00

 Name: Rack 0               Descr: Network Convergence System 1004 Chassis
 PID: NCS1004               VID: V00                   SN: CAT2231B192

 Name: 0/0                  Descr: Network Convergence System 1004 Filler
 PID: NCS1K4-LC-FILLER      VID: V01                   SN: N/A

 Name: 0/1-Optics0/1/0/2    Descr: Cisco 100G QSFP28 AOC Pluggable Optics Module
 PID: QSFP-100G-AOC3M       VID: V03                   SN: INL22262339-A

 Name: 0/1-Optics0/1/0/4    Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S       VID: V03                   SN: AVF2219S16U

 Name: 0/1-Optics0/1/0/5    Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics Module
 PID: QSFP-100G-LR4-S       VID: V02                   SN: JFQ2145701U

 Name: 0/1-Optics0/1/0/6    Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics Module
 PID: QSFP-100G-SR4-S       VID: ES1                   SN: AVF1925G012

 Name: 0/1-Optics0/1/0/7    Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics Module
 PID: QSFP-100G-LR4-S       VID: V02                   SN: JFQ2145706N

 Name: 0/1-Optics0/1/0/8    Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
 PID: ONS-QSFP28-LR4        VID: V01                   SN: JFQ19026014

 Name: 0/1-Optics0/1/0/9    Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics Module
 PID: QSFP-100G-LR4-S       VID: V02                   SN: OPM220518HS

 Name: 0/1-Optics0/1/0/10   Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics Module
 PID: QSFP-100G-SM-SR       VID: V02                   SN: INL21490043

 Name: 0/1-Optics0/1/0/11   Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
```

```
 PID: QSFP-100G-CWDM4-S      VID: V01                  SN: JFQ211930JL

 Name: 0/1-Optics0/1/0/12    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics Module
 PID: QSFP-100G-CWDM4-S      VID: V02                  SN: JFQ2210801H

 Name: 0/1                   Descr: NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
 PID: NCS1K4-1.2T-K9         VID: V00                  SN: CAT2250B0AE

 Name: 0/2-Optics0/2/0/2     Descr: Cisco 100G QSFP28 AOC Pluggable Optics Module
 PID: QSFP-100G-AOC3M        VID: V03                  SN: INL22262332-A

 Name: 0/2-Optics0/2/0/4     Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics Module
 PID: QSFP-100G-SM-SR        VID: V02                  SN: FNS22070HWF

 Name: 0/2-Optics0/2/0/5     Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics Module
 PID: QSFP-100G-SM-SR        VID: V02                  SN: SPT2225302D

 Name: 0/2-Optics0/2/0/6     Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics Module
 PID: QSFP-100G-LR4-S        VID: V02                  SN: FNS22310Z1X

Name: 0/2-Optics0/2/0/8     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
 PID: ONS-QSFP28-LR4         VID: V01                  SN: FNS20520R8Z

 Name: 0/2-Optics0/2/0/9     Descr: Cisco 100G QSFP28 AOC Pluggable Optics Module
 PID: QSFP-100G-AOC3M        VID: V03                  SN: INL23312282-A

 Name: 0/2-Optics0/2/0/10    Descr: Cisco 100G QSFP28 AOC Pluggable Optics Module
 PID: QSFP-100G-AOC3M        VID: V03                  SN: INL23312282-B

 Name: 0/2-Optics0/2/0/11    Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics Module
 PID: QSFP-100G-LR4-S        VID: V02                  SN: FNS23080LKF

 Name: 0/2                   Descr: NCS1K4 12x QSFP28 2 Trunk L-Band DWDM card
 PID: NCS1K4-1.2TL-K9        VID: V00                  SN: CAT2337B0S4

 Name: 0/3                   Descr: Network Convergence System 1004 Filler
 PID: NCS1K4-LC-FILLER       VID: V01                  SN: N/A

 Name: 0/RP0                 Descr: Network Convergence System 1004 Controller
 PID: NCS1K4-CNTLR-K9        VID: V00                  SN: CAT2231B069

 Name: 0/FT0                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V00                  SN: CAT2231B2GL

 Name: 0/FT1                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V00                  SN: CAT2231B2H4

 Name: 0/FT2                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V00                  SN: CAT2231B2GW

 Name: 0/PM0                 Descr: Network Convergence System 1004 AC Power Supply Unit
 PID: NCS1K4-AC-PSU          VID: V00                  SN: POG2221CL1V

 Name: 0/PM1                 Descr: Network Convergence System 1004 AC Power Supply Unit
 PID: NCS1K4-AC-PSU          VID: V00                  SN: POG2221CL04

 Name: 0/SC0                 Descr: Network Convergence System 1004 Chassis
 PID: NCS1004                VID: V00                  SN: CAT2231B192

sysadmin-vm:0_RP0# show inventory
Thu May  7  11:40:11.150 UTC+00:00

 Name: Rack 0                Descr: Network Convergence System 1004 4 line card slots
 PID: NCS1004                VID: V01                  SN: CAT2323B0DC
```

```
Name: 0/0-Optics0/0/0/2     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS2333080E

Name: 0/0-Optics0/0/0/3     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS23330801

Name: 0/0-Optics0/0/0/4     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS21140GZK

Name: 0/0-Optics0/0/0/6     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS233209CN

Name: 0/0-Optics0/0/0/10    Descr: Cisco 40GE QSFP+ LR4 Pluggable Optics Module
PID: QSFP-40G-LR4           VID: V02                   SN: FNS23110TYD

Name: 0/0                   Descr: NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card
PID: NCS1K4-1.2T-K9         VID: V00                   SN: CAT2237B25A

Name: 0/1-Optics0/1/0/0     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS2333080J

Name: 0/1-Optics0/1/0/1     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS23330806

Name: 0/1-Optics0/1/0/2     Descr: Cisco 4x10GE QSFP+ MLR Pluggable Optics Module
PID: ONS-QSFP-4X10-MLR      VID: V01                   SN: INL21010391

Name: 0/1-Optics0/1/0/4     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics Module
PID: QSFP-40G-SR4           VID: V03                   SN: JFQ20332007

Name: 0/1-Optics0/1/0/5     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics Module
PID: QSFP-40G-SR4           VID: V03                   SN: JFQ20332088

Name: 0/1-Optics0/1/0/6     Descr: Cisco 4x10GE QSFP+ MLR Pluggable Optics Module
PID: ONS-QSFP-4X10-MLR      VID: V01                   SN: INL21010471

Name: 0/1-Optics0/1/0/7     Descr: Cisco 4x10GE QSFP+ MLR Pluggable Optics Module
PID: ONS-QSFP-4X10-MLR      VID: V01                   SN: INL21010376

Name: 0/1                   Descr: NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder
PID: NCS1K4-OTN-XP          VID: V00                   SN: CAT2352B007

Name: 0/2-Optics0/2/0/0     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS20360V1R

Name: 0/2-Optics0/2/0/4     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics Module
PID: QSFP-40G-SR4           VID: V03                   SN: JFQ21502017

Name: 0/2-Optics0/2/0/5     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics Module
PID: QSFP-40G-SR4           VID: V03                   SN: JFQ202120DY

Name: 0/2                   Descr: NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder
PID: NCS1K4-OTN-XP          VID: V00                   SN: CAT2352B015

Name: 0/3-Optics0/3/0/0     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS23320BS3

Name: 0/3-Optics0/3/0/4     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics Module
PID: QSFP-40G-SR4           VID: V03                   SN: AVP2217S09L

Name: 0/3-Optics0/3/0/5     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics Module
PID: QSFP-40G-SR4           VID: V03                   SN: AVP2107S0RZ

Name: 0/3                   Descr: NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder
```

```
PID: NCS1K4-OTN-XP          VID: V00                   SN: CAT2352B00A

Name: 0/RP0-SFP-Port        Descr: Cisco SFP Pluggable Optics Module
PID: SFP-GE-S               VID: V01                   SN: FNS15512KVG

Name: 0/RP0                 Descr: Network Convergence System 1004 Controller
PID: NCS1K4-CNTLR-K9        VID: V01                   SN: CAT2323B0SG

Name: 0/FT0                 Descr: Network Convergence System 1004 Fan
PID: NCS1K4-FAN             VID: V01                   SN: CAT2325B1NW

Name: 0/FT1                 Descr: Network Convergence System 1004 Fan
PID: NCS1K4-FAN             VID: V01                   SN: CAT2324B0Z6

Name: 0/FT2                 Descr: Network Convergence System 1004 Fan
PID: NCS1K4-FAN             VID: V01                   SN: CAT2324B0Z8

Name: 0/PM0                 Descr: Network Convergence System 1004 DC Power Supply Unit
PID: NCS1K4-DC-PSU          VID: V01                   SN: POG2310CT00

Name: 0/PM1                 Descr: Network Convergence System 1004 DC Power Supply Unit
PID: NCS1K4-DC-PSU          VID: V01                   SN: POG2308CT4W

Name: 0/SC0                 Descr: Network Convergence System 1004 4 line card slots
PID: NCS1004                VID: V01                   SN: CAT2323B0DC
```

In the previous output, the significant fields are:

- PID—Physical model name of the chassis or node.
- VID—Physical hardware revision of the chassis or node.
- SN—Physical serial number of the chassis or node.

Verify Context

The **show context** command displays core dump context information of NCS 1004.

Procedure

Step 1 **show context**

Displays the core dump context information of NCS 1004 when you execute this command in the Cisco IOS XR EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# show context
Mon Sep 27 17:21:59.219 UTC

node: node0_RP0_CPU0
------------------------------------------------------------------
No context
```

The command output is empty during system upgrade.

Step 2 **admin**

Enters System Admin EXEC mode.

Step 3 **show context**

Displays the core dump context information of NCS 1004.

Example:

```
sysadmin-vm:0_RP0# show context
Mon Sep  27 17:22:19.351 UTC+00:00
**************************************************************
Location : 0/RP0
**************************************************************
No context
```

Verify Core Files

The **run** command checks for core files of NCS 1004.

Procedure

Step 1 **run**

Example:

```
RP/0/RP0/CPU0:ios# run
Mon Sep 27 17:29:11.163 UTC
[xr-vm_node0_RP0_CPU0:~]$cd /misc/disk1/
[xr-vm_node0_RP0_CPU0:/misc/disk1]$ls -lrt *.tgz
```

Step 2 **admin**

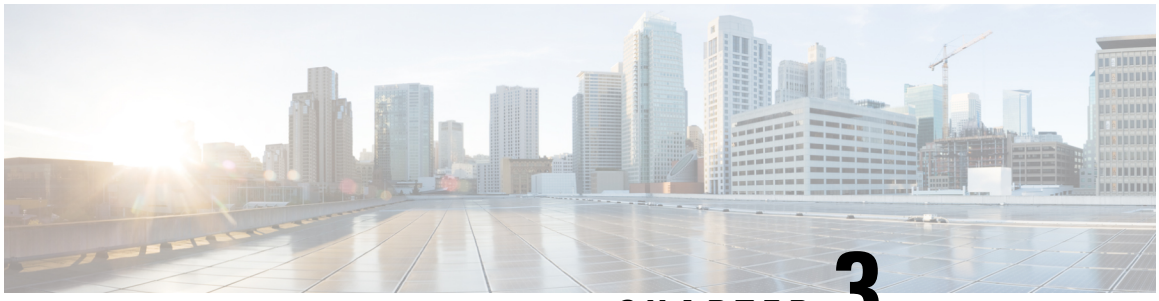
Enters System Admin EXEC mode.

Step 3 **run**

Example:

```
sysadmin-vm:0_RP0# run
Mon Sep  27 17:31:10.365 UTC+00:00

[sysadmin-vm:0_RP0:~]$cd /misc/disk1/
[sysadmin-vm:0_RP0:~]$ls -lrt *.tgz
```



CHAPTER 3

Create User Profiles and Assign Privileges

To provide controlled access to the System Admin configurations on NCS 1004, you must create user profiles and assign privileges. While assigning privileges, you can specify command rules and data rules, and apply these rules to user groups. To create users, groups, command rules, and data rules, use the authentication, authorization, and accounting (`aaa`) commands in the System Admin Config mode. You can also use the `aaa` commands to change the disaster-recovery password.

You can use a username and a password for authentication. On successful authentication, you can execute commands and access data elements that are based on the command rules and data rules. Users, who are part of a user group, have access privileges to the system as defined in the command rules and data rules for that user group.

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

The topics that are covered in this chapter are:

Create a User Profile

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 console, based on assigned privileges.

NCS 1004 supports up to 1024 user profiles.

Note Users who are created in the System Admin are different from users who are created in XR. As a result, the username and password of a System Admin user cannot be used to access the XR, and the other way round.

As a XR user, you can access the System Admin by entering the **admin** command in the XR EXEC mode. NCS 1004 does not prompt you to enter any username and password. As a XR user, you are provided full access to the System Admin console.

Procedure

Step 1 **admin**

Example:

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

Enters System Admin EXEC mode.

Step 2 **config**

Example:

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

Enters System Admin config mode.

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

Example:

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

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

Step 4 **password** *password*

Example:

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

Specifies the password that is used for the user authentication when you log in as System Admin.

Step 5 **uid** *user_id_value*

Example:

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

Specifies 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
```

Specifies 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
```

Specifies any alphanumeric value.

Step 8 **homedir** *homedir*

Example:

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

Specifies 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 a user group that includes the user profile that is created in this task. See Create a User Group, on page 53.
- Create command rules that apply to the user group. See Create Command Rules, on page 54.
- Create data rules that apply to the user group. See Create Data Rules, on page 57.

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.

NCS 1004 supports up to 32 user groups.

Before you begin

Create a user profile. See Create a User Profile, on page 51.

Procedure

Step 1 **admin**

Example:

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

Enters System Admin EXEC mode.

Step 2 **config**

Example:

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

Enters System Admin config mode.

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

Example:

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

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

Note By default, the system creates the user group "root-system" during the root user creation. The root user is part of this user group. Users added to this group get root user permissions.

Step 4 **users** *user_name*

Example:

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

Specifies the name of the user that must be part of the user group.

You can specify multiple usernames that are enclosed within double quotes. For example, **users** "*user1 user2* ...".

Step 5 **gid** *group_id_value*

Example:

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

Specifies 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 54.
- Create data rules. See Create Data Rules, on page 57.

Create Command Rules

Command rules are a set of rules that you can define for users of a user group to permit or deny the use of certain commands. You can associate command rules to a user group and apply the rule to a complete list of users in the user group.

You can create a command rule by specifying whether to permit or deny an operation, on command. The following table lists the possible operation and permission combinations:

Operation	**Accept Permission**	**Reject Permission**
Read (R)	Displays command on the CLI, when you enter "?" from the CLI.	Does not display command on the CLI, when you enter "?" from the CLI.

Execute (X)	Executes command from the CLI.	Could not execute command from the CLI.
Read and execute (RX)	Displays command on the CLI and can execute command.	Command is not visible or executable from the CLI.

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

Each command rule is identified by a number that is associated with it. When you apply multiple command rules to a user group, the command rule with a lower number takes precedence. For example, cmdrule5 permits read access, while cmdrule10 rejects read access. When both these command rules are applied to the same user group, user in this group gets read access because cmdrule 5 takes precedence.

As an example, you can create the command rule to deny read and execute permissions for the "show platform" command.

Before you begin

Create a user group. See Create a User Group, on page 53.

Procedure

Step 1 **admin**

Example:

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

Enters System Admin EXEC mode.

Step 2 **config**

Example:

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

Enters System Admin config mode.

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

Example:

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

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

Important Do no use numbers 1–1000 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, the system creates "cmdrule 1" 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 that are imposed on it, unless "cmdrule 1" is modified.

Step 4 **command** *command_name*

Example:

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

Specifies 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
```

Specifies the operation for which permission has to be set:

- **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
```

Specifies 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
```

Specifies the user group on which the command rule applies.

Step 8 **context** *connection_type*

Example:

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

Specifies 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 57.

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 are applied to all the users who are part of the user group.

Each data rule is identified by a number that is 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 a user group. See Create a User Group, on page 53.

Procedure

Step 1 **admin**

Example:

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

Enters System Admin EXEC mode.

Step 2 **config**

Example:

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

Enters System Admin config mode.

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

Example:

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

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

Important Do no use numbers between 1–1000 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, the system creates "datarule 1", when the root-system user is created. This data rule provides "accept" permission to "read", "write", and "execute" operations for all the configuration data. Therefore, the root user has no restrictions that are imposed on it, unless "datarule 1" is modified.

Step 4 **keypath** *keypath*

Example:

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

Specifies the key path of the data element. The key path 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
```

Specifies the operation for which permission has to be set. Use the following letters to identify various operations:

- 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
```

Specifies whether to permit or deny users to perform the operation.

- **accept**—Permit users to perform the operation
- **accept_log**—Permit users to perform the operation and log every access attempt
- **reject**—Restrict users from performing the operation

Step 7 **group** *user_group_name*

Example:

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

Specifies the user group to which you can apply the data rule. You can also specify multiple group names.

Step 8 **context** *connection type*

Example:

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

Specifies 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). We recommend 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 *
```

Enters asterisk '*' to indicate that the data rule is applicable to 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 NCS 1004, you can use the same username and password for disaster recovery in the System Admin mode. However, you can also change the username and password.

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

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

Note At a time, you can configure only one disaster-recovery username and password.

Before you begin

Create a user profile. For details, see Create a User Profile, on page 51.

Procedure

Step 1 **admin**

Example:

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

Enters System Admin EXEC mode.

Step 2 **config**

Example:

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

Enters System Admin config mode.

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

Example:

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

Specifies the disaster-recovery username and the password. You must 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'. You can enter the password as a plaintext or md5 digest string.

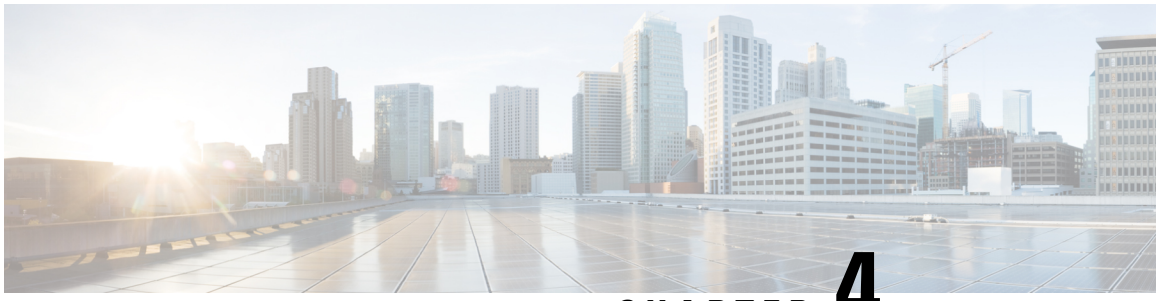
When you must make use of the disaster recovery username, you need to enter it as *username***@localhost**.

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

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

end-Prompts user to take one of these actions:

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



CHAPTER 4

Perform System Upgrade and Install Feature Packages

You can execute the system upgrade and package installation processes using the **install** commands on NCS 1004. The processes involve adding and activating the ISO images (*.iso*) and feature packages (*.rpm*) on NCS 1004. You can accesss these files from a network server and then activate on NCS 1004. If the installed package or SMU causes any issue, you can uninstall it.

Note We recommend that you collect the output of **show tech-support ncs1004** command before performing operations such as a reload or CPU OIR on NCS 1004. The command provides information about the state of the system before reload or before the CPU OIR operation is performed. This information is useful in debugging.

Note The output of the examples in the procedures is not from the latest software release. The output will change for any explicit references to the current release.

The topics covered in this chapter are:

Upgrade the System

Upgrading NCS 1004 involves installing a new Cisco IOS XR operating system image to replace the current one that comes pre-installed. However, you can install a new version to keep features up to date. You can perform the system upgrade operation from the XR mode. However, during the system upgrade, the operating systems that run both on the XR and the System Admin are upgraded.

System upgrade is done by installing the base package, Cisco IOS XR Core Bundle plus Manageability Package. Install the ISO image using **install** commands. For more information about the install process, see Workflow for Install Process.

For more information on upgrading the system and the RPMs, see *Cisco IOS XR Flexible Packaging Configuration Guide for Cisco NCS 1000 Series*.

Note

- Software downgrade from R7.2.1 to R7.1.1 affects traffic.
- Configure minimum and maximum values for chromatic dispersion on the trunk optical controller of the OTN-XP card to maintain the flow of traffic. This is recommended before upgrade from Release 7.3.1 and later or downgrade from Release 7.3.1 and earlier. Use the **controller optics** *R/S/I/P* [**cd-max** *cd-max* | **cd-min** *cd-min*] command to configure minimum and maximum chromatic dispersion values. See Command Reference for Cisco NCS 1004 for the range of cd values.

View Supported Software Upgrade or Downgrade Versions

Table 2: Feature History Table

Feature Name	Release Information	Description
Supported Software Upgrade or Downgrade IOS XR Versions	Cisco IOS XR Release 7.5.1	You can determine whether a software version can be upgraded or downgraded to another version using this functionality. Before an actual upgrade or downgrade process, you can also view the hardware or software limitations that could cause the upgrade or downgrade to fail. This feature helps you plan successful software upgrades or downgrades. This feature introduces the **show install upgrade-matrix** command.

Table 3: Feature History

Feature Name	Release Information	Feature Description
Pre and Post-Upgrade Install Health Checks using Profile	Cisco IOS XR Release 7.8.1	This feature allows you to create profiles that define the actions performed during pre and post-upgrade installation checks. You can configure the default actions for: • Pre-upgrade check failure • Upgrade failure • Revert after post-installation check failure

Your Cisco chassis comes preinstalled with IOS XR software. You either upgrade the software release to use new features and software fixes, or you downgrade the software. To leverage new features that are added or software fixes that are provided, it is important that you upgrade your software to a current version.

To help you select a Cisco IOS XR software release that aligns with Cisco-certified upgrade and downgrade paths, this feature provides answers to the following questions:

- What upgrade or downgrade releases are supported for the current release?
- I plan to upgrade from Release X to Release Y. Does my chassis support upgrade to Release Y?
- Are there any bridging SMUs that must be installed before I upgrade the software?

This feature provides a mechanism to determine whether the current release supports an upgrade to a target release. This task is run at the start of a software upgrade or downgrade through the **install replace** command. If the validation fails, the software upgrade is blocked, and the system notifies the reason for the failure. This feature allows you to proactively examine whether you can upgrade or downgrade to a certain release, saving time and effort involved in planning and upgrading the software.

The feature provides the following information to help you understand the prerequisites or limitations related to the specific software upgrade or downgrade:

- Required bridging SMU RPMs
- Blocking SMU RPMs
- Unsupported hardware
- Caveats or restrictions

You can overwrite the automatic validation using the **force** keyword in the **install replace** command. With this option, the system displays warning messages when the upgrade fails but does not block the software upgrade. Use the **force ?** keyword to understand any other impact to system functionalities apart from the disabling of this process that determines the supported releases for software upgrade or downgrade.

You can view the support information using the following **show** commands or through the operational data.

Command	Description
show install upgrade-matrix running	Displays all supported software upgrades from the current version according to the support data installed on the running system
show install upgrade-matrix iso *path-to-ISO*	Displays details about the software upgrade from the current version to the version of the target ISO according to the support data in both the running system and the ISO image
show install upgrade-matrix iso *path-to-ISO* **all**	Displays all supported software upgrades from any version according to the support data in the target ISO image
show install upgrade-matrix iso *path-to-ISO* **from-running**	Displays details about the software upgrade from the current version to the version of ISO according to the support matrices in both the running system and the target ISO image

View All Supported Software Upgrade from Running Version

The following example shows all supported releases for upgrade from the current version 24.1.1 on the chassis:

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix running
Thu Mar 14 16:44:17.034 IST
This may take a while ...

The current software [24.1.1] can be upgraded from and downgraded to the following releases:

================================================================================
From      To        Bridge SMUs Required        Caveats
================================================================================
7.10.1    24.1.1    None                        None
--------------------------------------------------------------------------------
7.9.1     24.1.1    None                        None
--------------------------------------------------------------------------------
7.8.1     24.1.1    None                        None
--------------------------------------------------------------------------------
24.1.1    7.10.1    None                        None
--------------------------------------------------------------------------------
24.1.1    7.9.1     None                        None
--------------------------------------------------------------------------------
24.1.1    7.8.1     None                        None
--------------------------------------------------------------------------------
```

View Supported Releases to Upgrade Software From Current Version to Target Version

This example shows the supported release to upgrade software from the current version to a target version.

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix iso /harddisk:/ncs1k-goldenk9-x-7.5.2.iso
Fri Jul 29 10:08:04.521 IST
This may take a while ...
Upgrade from the current software [7.5.1] to 7.5.2 is supported
```

```
================================================================================
From      To        Bridge SMUs Required        Caveats
================================================================================
7.5.1     7.5.2     None                        None
--------------------------------------------------------------------------------
```

The current image has the upgrade matrix that specifies only its supported upgrade or downgrade versions up to a certain version. If you want to determine the upgrade path of a newer version of ISO that is higher than the version in the current matrix, the upgrade matrix from the new ISO provides the supported upgrade or downgrade paths.

View Supported Releases from Current Version to an ISO Version

The following example shows the software upgrade paths, downgrade paths, and restrictions to an upgrade from the current version to the target ISO version:

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix iso /harddisk:/ncs1k-goldenk9-x-7.5.2.iso all
Fri Jul 29 10:28:59.837 IST
This may take a while ...

7.5.2 can be upgraded from and downgraded to the following releases:
================================================================================
From      To        Bridge SMUs Required        Caveats
================================================================================
7.5.1     7.5.2     None                        None
--------------------------------------------------------------------------------
7.5.2     7.5.1     None                        None
--------------------------------------------------------------------------------
7.5.2     7.3.1     None                        None
--------------------------------------------------------------------------------
7.5.2     7.3.2     None                        None
--------------------------------------------------------------------------------
7.3.1     7.5.2     None                        None
--------------------------------------------------------------------------------
7.3.2     7.5.2     None                        None
--------------------------------------------------------------------------------
```

View Supported Releases from Running Version to an ISO Version

The following example displays details about the software upgrade from the current version to the version of ISO according to the support matrices in both the running system and the target ISO image:

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix iso /harddisk:/ncs1k-goldenk9-x-7.5.2.iso
from-running
Fri Jul 29 10:09:09.223 IST
This may take a while ...
Upgrade from the current software [7.5.1] to 7.5.2 is supported

================================================================================
From      To        Bridge SMUs Required        Caveats
================================================================================
7.5.1     7.5.2     None                        None
--------------------------------------------------------------------------------
```

Pre and Post-Upgrade Installation Health Checks

Note It is mandatory to Install "ncs1004-healthcheck-1.0.0.0-r781.x86_64.rpm" for Pre and Post-Upgrade Installation Health Checks feature to work.

This section describes about of the pre and postupgrade Installation health check for routers.

Existing client-server framework notifies the subscribed clients to perform the precheck functionality.

The System health check infrastructure that is plugged to the install pre and postchecks phase of the system upgrade. This includes other existing install pre or postchecks.

Upgrade precheck:

- If single command upgrade is triggered either with a force option or is configured to skip checks, then health check is bypassed and a syslog entry added.
- When single command upgrade is triggered, install infra performs install specific prechecks. If the install prechecks pass, the system health check infra plug-in is invoked to check the overall system health.
- The health check infrastructure returns the health status during the installation.
- Single command upgrade continues on if the prechecks completes with no errors.
- If any errors are detected, then single command upgrade continues or terminates depending on the option that is selected for abort-on-precheck-failure.
- Single command upgrade postchecks before autocommit triggers based on the user selected level information.

Upgrade post check:

- Post checks are bypassed if force or config option is selected for single command upgrade.
- If install specific postchecks are completed sucessfully, then the system health check infra plug-in is invoked. If no errors are reported then the autocommit triggers.
- If any errors are detected, the abort-on option that is saved before the upgrade reload is used to either abort the single command upgrade or continue. This depends on the severity of the errors that are detected during post check.
- Summary of the pre and posthealth check is appended to the single command upgrade operation log.

Installation Profile Creation

Installation Profile is created to choose and alternate installation behavior. One default profile is created involving pre and postchecks. You can edit the install behavior to choose cases like terminate installation if precheck fails or revert after post installation check. You can also choose to continue installation despite failure in pre checks.

You can configure “enable or disable” options to run pre or post installation checks or “abort-on-failure” for pre checks, or "warn-on-failure" and “restore-to-v1” on post checks. To configure the Install profile, use the following commands:

config

install profile *profile_name* **pre-check***metric-name* **[enable | disable] [abort-on-failure | continue-on-failure | revert-on-failure]**

end

Following is a sample to display metric settings in the install profile.

```
RP/0/RP0/CPU0:ios#show install profile default
Fri Mar 15 11:29:35.381 IST
Profile Name : default
State : Enabled

Prechecks : Enabled
        communication-timeout   : Enabled       [ warn-on-failure ]
        config-inconsistency    : Enabled       [ error-on-failure ]
        process-resource        : Enabled       [ warn-on-failure ]
        process-status          : Enabled       [ warn-on-failure ]
        system-clock            : Enabled       [ warn-on-failure ]
        hw-monitoring           : Enabled       [ warn-on-failure ]
        lc-monitoring           : Enabled       [ warn-on-failure ]
        pci-monitoring          : Enabled       [ warn-on-failure ]
        wd-monitoring           : Enabled       [ warn-on-failure ]
        disk-space              : Enabled       [ error-on-failure ]
        upgrade_matrix          : Enabled       [ error-on-failure ]
        core-cleanup            : Disabled      [ NA ]
        file-cleanup            : Disabled      [ NA ]

Postchecks : Enabled
        communication-timeout   : Enabled       [ error-on-failure ]
        config-inconsistency    : Enabled       [ error-on-failure ]
        process-resource        : Enabled       [ error-on-failure ]
        process-status          : Enabled       [ error-on-failure ]
        system-clock            : Enabled       [ error-on-failure ]
        hw-monitoring           : Enabled       [ error-on-failure ]
        lc-monitoring           : Enabled       [ error-on-failure ]
        pci-monitoring          : Enabled       [ error-on-failure ]
        wd-monitoring           : Enabled       [ error-on-failure ]
```

Use the following configuration to report health check:

config

grpc local-connection

Netconf-yang agent

commit

The following is a sample to display health check states:

```
RP/0/RP0/CPU0:ios#show healthcheck internal states
Fri Mar 15 11:30:24.177 IST

 Internal Structure INFO

 Current state: Disabled

 Reason: Success

 Netconf Config State: Enabled

 Grpc Config State: Enabled

 Nosi state: Initialized
```

```
 Appmgr conn state: Connected

 Nosi lib state: Not ready

 Nosi client: Valid client
```

Use the following configuration to configure healthcheck cadence interval between 30 and 1800 seconds:

config

healthcheck cadence *healthcheck_cadence_interval*

commit

The following is a sample to display health check report:

```
RP/0/RP0/CPU0:New_NODE#show healthcheck report
Thu Jun  2 07:24:53.182 UTC

Healthcheck report
Last Update Time:
METRICS REPORT

cpu
  State: Normal

free-memory
  State: Normal

filesystem
  State: Normal

shared-memory
  State: Normal

platform
  State: Normal

redundancy
  State: Normal

fpd
  State: Normal

asic-errors
  State: Normal

fabric-stats
  State: Normal

process-status
  State: Normal

process-resource
  State: Normal

communication-timeout
  State: Normal

config-inconsistency
  State: Normal

system-clock
  State: Normal
```

```
pci-monitoring
  State: Normal

hw-monitoring
  State: Normal

wd-monitoring
  State: Normal

lc-monitoring
  State: Normal
```

Software Upgrade and Downgrade Matrix

The following table lists the upgrade and downgrade paths supported for Cisco NCS 1004.

Upgrade Path		Downgrade Path	
Source Release	**Destination Release**	**Source Release**	**Destination Release**
R7.3.2, R7.5.1, R7.5.2, R7.7.1, R7.8.1, R7.9.1	R7.10.1	R7.10.1	R7.9.1, R7.8.1, R7.7.1, R7.5.2, R7.5.1, R7.3.2
R7.8.1, R7.9.1, R7.10.1, R24.1.1	R24.3.1	R24.3.1	R24.1.1, R7.10.1, R7.9.1, R7.8.1

Install Packages

You can install packages and software patches (SMU) on NCS 1004. Installing a package on NCS 1004 installs specific features that are part of that package. Cisco IOS XR Software is divided into various software packages; the availability of the software in individual packages enables you to select the features to run on NCS 1004. Each package contains components that perform a specific set of NCS 1004 functions.

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

Standard packages are:

Feature Set	Filename	Description
Composite Package		
Cisco IOS XR Core Bundle + Manageability Package	ncs1004-mini-x-24.1.1.iso	Contains required core packages, including operating system, Admin, Base, Forwarding, SNMP Agent, FPD, and Alarm Correlation and Netconf-yang, Telemetry, XML Parser, HTTP server packages.
Individually Installable Optional Packages		

Cisco IOS XR Security Package	ncs1004-k9sec-1.0.0.0-r2411.x86_64.rpm	Support for Encryption, Decryption, IP Security (IPsec), Secure Socket Layer (SSL), and Public-key infrastructure (PKI).
OpenROADM	ncs1004-tp-sw-1.0.0.0-r2411.x86_64.rpm	Install the ncs1004-tp-sw-1.0.0.0-r732.rpm package for OpenROADM configuration.
OTN-XP	ncs1004-sysadmin-otn-xp-dp-24.1.1-r2411.x86_64.rpm	Install this package on the OTN-XP card to bring up the system with OTN-XP card.
Pre and Post-Upgrade Installation Health Checks	ncs1004-healthcheck-1.0.0.0-r2411.x86_64.rpm	Install this package for Pre and Post-Upgrade Installation Health Checks configuration.

Workflow for Install Process

To install a package, see Install Packages. To uninstall a package, see Uninstall Packages. The workflows for installation and uninstallation processes are depicted in individual flowcharts in their respective subsections.

Install Packages

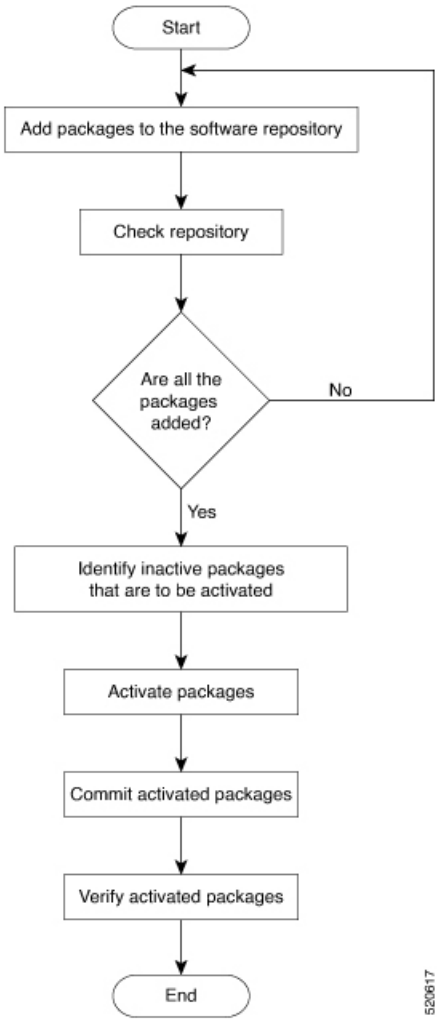
Complete this task to upgrade the system or install a patch. You can perform the system upgrade using an ISO image file and the patch installation using packages and SMUs. This task also enables you to install *.tar* files. The *.tar* file contains multiple packages and SMUs that are merged into a single file. A single *.tar* file can contain up to 64 individual files. The packaging format defines 1 RPM per component, without dependency on the card type.

Note To install a System Admin package or an XR package, execute the **install** commands in System Admin EXEC mode or XR EXEC mode respectively. All **install** commands are applicable in both these modes.

Note Two FPDs are available for the OTN-XP card - LC_CPU_MOD_FW and LC_DP_MOD_FW. LC_CPU_MOD_FW CPU FPD package is available as part of the boot ISO image. You must install the ncs1004-sysadmin-otn-xp-dp-*.rpm data path FPD package on the OTN-XP line card using this procedure to bring up the system with OTN-XP card.

The following flowchart displays workflow for installing a package:

Figure 1: Installing Packages Workflow



Before you begin

- Configure and connect to the management port. You can access the installable file through the management port. For details about configuring the management port, see Configure Management Interface.
- Copy the package to be installed either on NCS 1004 hard disk or on a network server to which NCS 1004 has access.
- When the ncs1004-k9sec package is not installed, use only FTP or TFTP to copy files or during the **install add** operation.

Procedure

Step 1 Execute one of these commands:

- **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:ios#install add source harddisk: ncs1004-mini-x-7.2.1
ncs1004-k9sec-2.1.0.0-r721.x86_64.rpm


Thu Feb  7 11:10:51.867 UTC
Feb 07 11:10:53 Install operation 25 started by root:
 install add source harddisk: ncs1004-mini-x-7.2.1 ncs1004-k9sec-2.1.0.0-r721.x86_64.rpm
Feb 07 11:10:55 Install operation will continue in the background
Thu Feb  7 11:10:51 Install operation 25 finished successfully
```

Ensure to add the respective packages as appropriate. Unpack the software files from the package and add to the software repository. This operation may take time depending on the size of the files that are added. The operation takes place in an asynchronous mode. The **install add** command runs in the background, and the EXEC prompt is returned.

Note install operation over IPv6 is not supported.

Step 2 **show install request**

Example:

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

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

Step 3 **show install repository**

Example:

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


6 package(s) in XR repository:
    ncs1004-mini-x-7.0.1
    ncs1004-mini-x-7.2.1
    ncs1004-mpls-2.0.0.0-r711
    ncs1004-k9sec-2.1.0.0-r721.x86_64
    ncs1004-xr-7.2.1
    ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

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:ios#show install inactive


6 inactive package(s) found:
    ncs1004-mini-x-7.0.1
    ncs1004-mini-x-7.2.1
    ncs1004-mpls-2.0.0.0-r711
    ncs1004-k9sec-2.1.0.0-r721.x86_64
    ncs1004-xr-7.2.1
    ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

Displays inactive packages that are present in the repository. You can activate only inactive packages.

Step 5 **install activate** *package_name*

Example:

```
RP/0/RP0/CPU0:ios#install activate ncs1004-mini-x-7.2.1 ncs1004-k9sec-2.1.0.0-r721.x86_64


Thu Feb  7 11:25:09.229 UTC
Feb 07 11:25:10 Install operation 26 started by root:
  install activate pkg ncs1004-mini-x-7.2.1 ncs1004-k9sec-2.1.0.0-r721.x86_64
Feb 07 11:25:10 Package list:
Feb 07 11:25:10     ncs1004-mini-x-7.2.1 ncs1004-k9sec-2.1.0.0-r721.x86_64
Feb 07 11:25:17 Install operation will continue in the background


RP/0/RP0/CPU0:ios#
RP/0/RP0/CPU0:ios#Feb 07 11:25:10 Install operation 26 finished successfully
```

The package configurations are set to active on NCS 1004. As a result, new features and software fixes take effect. This operation takes place in the asynchronous mode. The **install activate** command runs in the background, and the EXEC prompt is returned.

Note After an RPM of a higher version is activated, and if it is required to activate an RPM of a lower version, use the force option. For example:

Using the traditional method, add the RPM with lower version to the repository and then force the activation:

```
install add source repository ncs1004-xr-7.2.1

install activate ncs1004-xr-7.2.1 force
```

Or

Using the **install update** command:

```
install update source repository ncs1004-xr-7.2.1
```

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

Step 6 **show install active**

Example:

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


Mon Mar 11 07:31:12.302 UTC
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv19
  Active Packages: 5
    ncs1004-mini-x-7.2.1
    ncs1004-mpls-2.0.0.0-r711
    ncs1004-k9sec-2.1.0.0-r721.x86_64
    ncs1004-xr-7.2.1
    ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

Displays packages that are active.

Step 7 **install commit system**

Example:

```
RP/0/RP0/CPU0:ios#install commit system
```

```
Thu Feb  7 11:34:04.207 UTC
Feb 07 11:34:05 Install operation 27 started by root:
  install commit system
Feb 07 11:34:06 Install operation will continue in the background
RP/0/RP0/CPU0:ios#Feb 07 11:34:19 Install operation 27 finished successfully
```

Commits the newly active software.

Note If you perform a manual or automatic system reload without completing the transaction with the install commit command during system update, the action will revert the system to the point before the install transaction commenced, including any configuration changes. Only the log is preserved for debugging. This action clears all configuration rollback points available. You will not be able to rollback to, or view, any commits made until the install rollback event. Any new commits made after the install rollback event will start from commit ID '1000000001'.

Installing Packages: Related Commands

Related Commands	Purpose
show install log	Displays the log information for the install process. This information is used for troubleshooting in case of installation failure.
show install package	Displays the details of the packages that are added to the repository. Use this command to identify individual components of a package.
install prepare	Makes preactivation checks on an inactive package to prepare it for activation.
show install prepare	Displays the list of package that has been prepared and are ready for activation.

What to do next

- After performing system upgrade, upgrade FPD by using the **upgrade hw-module location all fpd all** command from the Cisco IOS XR mode. The progress of FPD upgrade process can be monitored using the **show hw-module fpd** command.
- Reload NCS 1004 if BIOS, BP_SSD, and CPU_SSD are in RLOAD REQ state. Use the **hw-module location 0/RP0 reload** command.
- Verify the installation using the **install verify packages** command.
- Uninstall the packages or SMUs if their installation causes any issues on NCS 1004. See Uninstall Packages.

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

(Optional) Install Prepared Packages

You can perform a system upgrade or feature upgrade by activating the ISO image file, packages, and SMUs. It is possible to prepare these installable files before activation. During the preparation phase, preactivation checks are made, and the components of the installable files are loaded on to the NCS 1004 setup. The preparation process runs in the background, and NCS 1004 is fully usable during this time. When the prepare phase completes, the prepared files are activated instantaneously.

The advantages of preparing before activation are:

- If the installable file is corrupted, then the preparation process fails. This process provides an early warning of the problem. If the corrupted file were to be activated directly, it may cause the NCS 1004 to malfunction.
- Directly activating an ISO image for the system upgrade takes considerable time during which the NCS 1004 is not usable. However, if the image is prepared before activation, the prepare process runs asynchronously. When the prepared image is activated, the activation process takes less time. As a result, the downtime is considerably reduced.

Complete this task to upgrade the system and install packages by using the prepare operation.

Procedure

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

For details, see Install Packages.

Step 2 **show install repository**

Example:

```
RP/0/RP0/CPU0:ios#show install repository
Fri Mar 15 11:31:53.352 IST
12 package(s) in XR repository:
    ncs1004-mpls-1.0.0.0-r241146I.x86_64
    ncs1004-k9sec-1.0.0.0-r2411.x86_64
    ncs1004-xr-24.1.1.46I
    ncs1004-healthcheck-1.0.0.0-r241146I.x86_64
    ncs1004-mpls-te-rsvp-1.0.0.0-r2411.x86_64
    ncs1004-xr-24.1.1
    ncs1004-mini-x-24.1.1.46I
    ncs1004-mpls-1.0.0.0-r2411.x86_64
    ncs1004-mini-x-24.1.1
    ncs1004-healthcheck-1.0.0.0-r2411.x86_64
    ncs1004-k9sec-1.0.0.0-r241146I.x86_64
    ncs1004-mpls-te-rsvp-1.0.0.0-r241146I.x86_64
```

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 commands:

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

Example:

```
RP/0/RP0/CPU0:ios#install prepare ncs1004-mini-x-7.2.1 ncs1004-k9sec-2.1.0.0-r721.x86_64
```

Or

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

The preparation process takes place in an asynchronous mode. The **install prepare** command runs in the background, and the EXEC prompt is returned.

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

Step 4 **show install prepare**

Example:

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

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

Step 5 **install activate** *package_name*

Example:

```
RP/0/RP0/CPU0:ios#install activate ncs1004-mini-x-7.2.1 ncs1004-k9sec-2.1.0.0-r721.x86_64
```

All the packages that have been prepared are activated together to activate the package configurations on NCS 1004.

Step 6 **show install active**

Displays packages that are active.

Step 7 **install commit system**

Example:

```
RP/0/RP0/CPU0:ios#install commit system
```

Commits the recently activated software.

Installing Packages: Related Commands

Related Commands	Purpose
show install log	Displays the log information for the install process. You can use this information for troubleshooting in case of install failure.
show install package	Displays the details of the packages that you have added to the repository. Use this command to identify individual components of a package.
install prepare clean	Clears the prepare operation and removes 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 Cisco IOS XR mode. The progress of FPD upgrade process can be monitored using the **show hw-module fpd** command.

- Reload NCS 1004 if BIOS, BP_SSD, and CPU_SSD are in RLOAD REQ state. Use the **hw-module location 0/RP0 reload** command.
- Verify the installation using the **install verify packages** command.
- Uninstall the packages or SMUs if their installation causes any issues on NCS 1004. See Uninstall Packages.

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

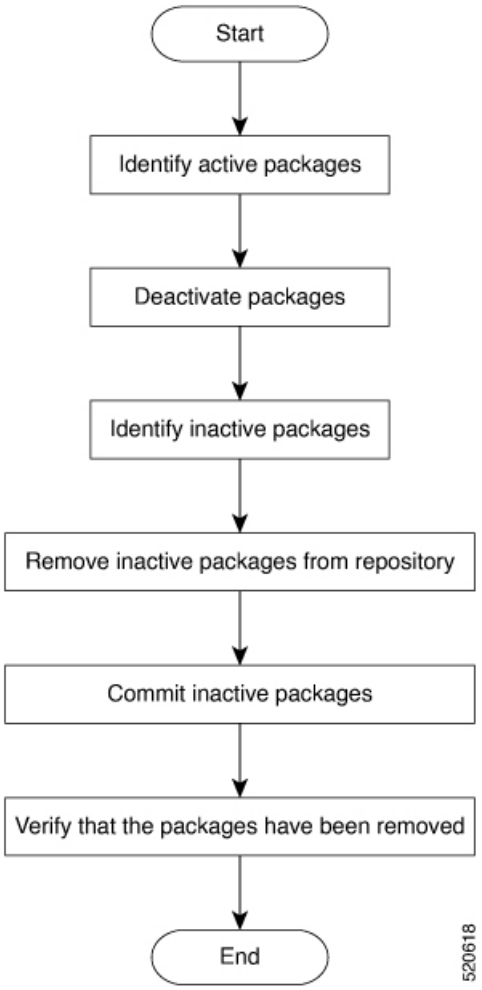
Uninstall Packages

Complete this task to uninstall a package. All the NCS 1004 functionalities that are part of the uninstalled package are deactivated. Packages that are added in the XR mode cannot be uninstalled from the System Admin mode, and the other way round.

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

The following flowchart shows a workflow for uninstalling a package:

Figure 2: Uninstalling Packages Workflow



Procedure

Step 1 **show install active**

Example:

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

Mon Mar 11 07:31:12.302 UTC
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv19
  Active Packages: 5
    ncs1004-mini-x-7.2.1
    ncs1004-mpls-2.0.0.0-r711
    ncs1004-k9sec-2.1.0.0-r721.x86_64
    ncs1004-xr-7.1.1
    ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

Displays active packages. You can deactivate only active packages.

Step 2 Execute one of these commands:

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

Example:

```
RP/0/RP0/CPU0:ios#install deactivate ncs1004-k9sec-2.1.0.0-r721.x86_64
```

Or

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

All features and software patches that are 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 are added in the specified operation are deactivated together. You do not have to deactivate the packages individually.

Step 3 **show install inactive**

Example:

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

Mon Mar 11 08:07:46.504 UTC
1 inactive package(s) found:
    ncs1004-k9sec-2.1.0.0-r721.x86_64
```

The deactivated packages are now listed as inactive packages. You can remove only inactive packages from the repository.

Step 4 **install remove** *package_name*

Example:

```
RP/0/RP0/CPU0:ios#install remove ncs1004-k9sec-2.1.0.0-r721.x86_64
```

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 are added for the specified operation ID.

Step 5 **install commit system**

Example:

```
RP/0/RP0/CPU0:ios#install commit system
```

Commits the newly active software.

Step 6 **show install repository**

Example:

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

Mon Mar 11 08:11:55.780 UTC
4 package(s) in XR repository:
     ncs1004-xr-7.2.1 version=7.2.1 [Boot image]
     ncs1004-mini-x-7.2.1
     ncs1004-mpls-2.0.0.0-r711
     ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

Displays packages available in the repository. The package that is removed is not displayed in the output.

What to do next

Install required packages. See Install Packages.

FPD Automatic Upgrade

Table 4: Feature History

Feature Name	Release Information	Feature Description
Automatic FPD Upgrade	Cisco IOS XR Release 7.9.1	The automatic FPD upgrade functionality is now enabled by default. It upgrades the FPD components' firmware version to the latest version. This enhancement eliminates the need to explicitly enable the functionality using the **fpd auto-upgrade enable** command. As a result, the software upgrade is simplified, and the system always maintains the latest state of the FPD firmware version.

The FPD automatic upgrade feature upgrades the FPD firmware version of all components to the latest version along with software activation. This feature helps to upgrade the firmware automatically without manual intervention. After the software upgrade, all FPD components are in the CURRENT status. You can check the FPD components status with details using the **show hw-module fpd** command.

After the FPD is upgraded, the FPD version is not downgraded to the previous version even if the image is rolled back to the original version.

From R7.9.1, FPD automatic upgrade is enabled by default. The user can manually disable FPD automatic upgrade using the **fpd auto-upgrade disable** command.

Before the user upgrades the software from an older release to R7.9.1, default configurations must be cleared using the **no fpd auto-upgrade** command. This would enable the FPD automatic upgrade in the R7.9.1 software image. When the user upgrades the software from R7.9.1 to later releases, FPD upgrades happen automatically as the FPD automatic upgrade is enabled by default from R7.9.1.

Note FPD automatic upgrade is supported for the BP_SSD and CPU_SSD FPDs only if the SSDs are programmed with the latest firmware. FPD automatic upgrade for the BP_SSD and CPU_SSD from R7.5.2 to a later release will work without manual intervention. During a system upgrade from a previous release to R7.5.2, SSDs are programmed with the old firmware. Hence, manual upgrade of BP_SSD and CPU_SSD FPDs is required even though FPD automatic upgrade is enabled.

Note FPD automatic upgrade is not supported on the LC_DP_MOD_FW FPD of the OTN_XP card as the upgrade is traffic-affecting.

You can enable the FPD automatic upgrade feature using the following commands.

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# fpd auto-upgrade enable
RP/0/RP0/CPU0:ios(config)# commit
RP/0/RP0/CPU0:ios(config)#end
```

To verify whether the FPD automatic upgrade feature is enabled, examine the output of the **show running-config** command.

```
RP/0/RP0/CPU0:ios#
RP/0/RP0/CPU0:ios#show running-config | inc fpd
Thu Feb  7 10:43:44.822 UTC
Building configuration...
fpd auto-upgrade enable
```

Example

The following example shows the output of the **show hw-module fpd** command.

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Fri May 29 11:35:24.492 UTC

                                                                                FPD Versions
                                                                                ==============
Location   Card type              HWver FPD device       ATR Status    Running   Programd
-------------------------------------------------------------------------------------------
0/0        NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW              CURRENT    21.31     21.31

0/0        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW              CURRENT     1.26      1.26

0/1        NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW              CURRENT    21.31     21.31

0/1        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW              CURRENT     1.26      1.26

0/2        NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW              CURRENT    21.31     21.31

0/2        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW              CURRENT     1.26      1.26

0/3        NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW              CURRENT    21.31     21.31

0/3        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW              CURRENT     1.26      1.26

0/RP0      NCS1K4-CNTLR-K9   1.14  BIOS              S        CURRENT     5.30      5.30

0/RP0      NCS1K4-CNTLR-K9   5.4   BP_SSD                     CURRENT    75.00     75.00

0/RP0      NCS1K4-CNTLR-K9   4.0   CPU_FPGA                   CURRENT     1.14      1.14

0/RP0      NCS1K4-CNTLR-K9   5.4   CPU_SSD                    CURRENT    75.00     75.00

0/PM1      NCS1K4-AC-PSU     0.1   PO-PriMCU                  CURRENT     2.70      2.70

0/SC0      NCS1004           2.0   BP_FPGA                    CURRENT     1.25      1.25

0/SC0      NCS1004           2.0   XGE_FLASH                  CURRENT    18.04     18.04
```

Note The "show hw-module fpd" command displays "BP_SSD" and "CPU_SSD" version details in release 7.10.1 and 24.1.1 for Soldigm type SSD.

Note The "show hw-module fpd" command displays "BP_SSD" and "CPU_SSD" version details in release 24.1.1 only for Micron type SSD.

Note FPD automatic upgrade is not supported for POWMAN_CFG. During a system upgrade to R7.5.2 or a higher release, manual upgrade of POWMAN_CFG is required if POWMAN_CFG is not running the latest version. Manual upgrade of POWMAN_CFG does not affect the traffic.

Example

The following example shows the output of the **show hw-module fpd** command after the manual upgrade of the POWMAN_CFG during the automatic FPD upgrade.

```
RP/0/RP0/CPU0:ncs1004-129#show hw-module fpd
Tue Nov 21 15:55:27.689 UTC

Auto-upgrade:Disabled
                                                                                FPD Versions
                                                                                ==============
Location   Card type             HWver FPD device       ATR Status    Running   Programd
-------------------------------------------------------------------------------------------
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_CPU_MOD_FW        NEED UPGD  80.10     80.10
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.38      1.38
0/2        NCS1K4-1.2TL-K9       3.0   LC_CPU_MOD_FW        CURRENT    75.20     75.20
0/2        NCS1K4-1.2TL-K9       1.0   LC_OPT_MOD_FW        CURRENT     1.38      1.38
0/3        NCS1K4-1.2TL-K9       3.0   LC_CPU_MOD_FW        CURRENT    75.20     75.20
0/3        NCS1K4-1.2TL-K9       1.0   LC_OPT_MOD_FW        CURRENT     1.38      1.38
0/RP0      NCS1K4-CNTLR-K9       5.0   CSB_IMG           S  CURRENT     0.200     0.200
0/RP0      NCS1K4-CNTLR-K9       5.0   TAM_FW               CURRENT    36.08     36.08
0/RP0      NCS1K4-CNTLR-K9       1.14  BIOS              S  CURRENT     5.50      5.50
0/RP0      NCS1K4-CNTLR-K9       5.4   BP_SSD               CURRENT    75.00     75.00
0/RP0      NCS1K4-CNTLR-K9       5.0   CPU_FPGA             CURRENT     1.14      1.14
0/RP0      NCS1K4-CNTLR-K9       5.4   CPU_SSD              CURRENT    75.00     75.00
0/RP0      NCS1K4-CNTLR-K9       3.18  POWMAN_CFG           CURRENT     3.40      3.40
0/PM0      NCS1K4-DC-PSU         0.1   PO-PriMCU            CURRENT     1.12      1.12
0/PM1      NCS1K4-DC-PSU         0.1   PO-PriMCU            CURRENT     1.12      1.12
0/SC0      NCS1004               2.0   BP_FPGA              CURRENT     1.25      1.25
0/SC0      NCS1004               2.0   XGE_FLASH            CURRENT    18.04     18.04
```

To upgrade POWMAN_CFG manually refer to the example given below.

Example

FPD upgrade initiated:

```
RP/0/RP0/CPU0:ios#upgrade hw-module location 0/RP0 fpd POWMAN_CFG
```

FPD moved to RELOAD REQ state:

```
0/RP0      NCS1K4-CNTLR-K9       3.18  POWMAN_CFG           RLOAD REQ   2.50      2.50
```

RP reload complete:

```
(sysadmin-vm:0_RP0# hw-module location 0/RP0 reload noprompt),  POWMAN_CFG upgrade completed
```

Firmware Upgrade

Table 5: Feature History

Feature Name	Release Information	Feature Description
FPD Upgrade Support for SSDs	Cisco IOS XR Release 7.5.2	The FPDs of the SSDs on the chassis and on the route processor can be upgraded. This feature allows you to maintain the FPD versions of SSDs with latest firmware included with enhancements and bug fixes. If an FPD upgrade is due, the **One Or More FPDs Need Upgrade Or Not In Current State** alarm is raised on the route processor.

After a software upgrade to the latest release, it is mandatory to upgrade the FPD of the RP and the line cards. Use the following task to upgrade the firmware version of the line cards.

Note The Provisioning In Progress alarm is raised on the slice or the line card during the FPD upgrade and automatically clears after the FPD upgrade. This alarm is non-traffic affecting.

Note Upgrade the FPDs of OTN-XP card in the following sequence:

1. LC_CPU_MOD_FW
2. LC_DP_MOD_FW
3. LC_CFP2_PORT_<0/1>

From R7.5.2, the FPDs of the SSDs on the chassis and the route processor can be upgraded. The FPD of the chassis SSD is BP_SSD and the FPD on the route processor SSD is CPU_SSD. FPD upgrades of BP_SSD and CPU_SSD is non-traffic impacting.

Procedure

Step 1 Use the **show hw-module fpd** command to check the status of the FPD.

You can verify the status of the FPDs of the line cards in the following example.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Fri May 29 11:17:52.980 UTC

                                                                      FPD Versions
                                                                      ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
--------------------------------------------------------------------------------
0/0        NCS1K4-1.2T-K9        2.0   LC_CPU_MOD_FW        CURRENT   21.19   21.19
0/0        NCS1K4-1.2T-K9        1.0   LC_OPT_MOD_FW        CURRENT    2.04    2.04
0/1        NCS1K4-OTN-XP         3.0   LC_CPU_MOD_FW        NEED UPGD 21.18   21.18
0/1        NCS1K4-OTN-XP         3.0   LC_DP_MOD_FW         CURRENT    6.10    6.10
0/2        NCS1K4-OTN-XP         3.0   LC_CPU_MOD_FW        NEED UPGD 21.18   21.18
0/2        NCS1K4-OTN-XP         3.0   LC_DP_MOD_FW         CURRENT    6.10    6.10
0/3        NCS1K4-OTN-XP         3.0   LC_CPU_MOD_FW        NEED UPGD 21.18   21.18
0/3        NCS1K4-OTN-XP         3.0   LC_DP_MOD_FW         CURRENT    6.10    6.10
0/RP0      NCS1K4-CNTLR-K9       4.0   CSB_IMG           S  CURRENT    0.200   0.200
0/RP0      NCS1K4-CNTLR-K9       4.0   TAM_FW               CURRENT   36.08   36.08
0/RP0      NCS1K4-CNTLR-K9       1.14  BIOS              S  CURRENT    4.30    4.30
0/RP0      NCS1K4-CNTLR-K9       4.0   CPU_FPGA             CURRENT    1.14    1.14
0/PM0      NCS1K4-DC-PSU         0.1   PO-PriMCU            CURRENT    1.12    1.12
0/PM1      NCS1K4-DC-PSU               PO-PriMCU            NOT READY
0/SC0      NCS1004               2.0   BP_FPGA              CURRENT    1.25    1.25
0/SC0      NCS1004               2.0   XGE_FLASH            CURRENT   18.04   18.04
```

From R7.5.2, you can verify the status of the FPDs of the SSDs in the following example.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Thu Oct  7 12:44:43.532 UTC

Auto-upgrade:Disabled
                                                                        FPD Versions
                                                                        ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
--------------------------------------------------------------------------------
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_CPU_MOD_FW        CURRENT    21.31     21.31
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.26      1.26
0/1        NCS1K4-2-QDD-C-K9     0.0   LC_CPU_MOD_FW        CURRENT    21.31     21.31
0/1        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.26      1.26
0/2        NCS1K4-2-QDD-C-K9     1.0   LC_CPU_MOD_FW        CURRENT    21.31     21.31
0/2        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.26      1.26
0/3        NCS1K4-2-QDD-C-K9     0.0   LC_CPU_MOD_FW        CURRENT    21.31     21.31
```

```
0/3        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW          CURRENT     1.26      1.26
0/RP0      NCS1K4-CNTLR-K9       4.0   CSB_IMG           S    CURRENT     0.200     0.200
0/RP0      NCS1K4-CNTLR-K9       4.0   TAM_FW                 CURRENT    36.08     36.08
0/RP0      NCS1K4-CNTLR-K9       1.14  BIOS              S    CURRENT     5.30      5.30
0/RP0      NCS1K4-CNTLR-K9       5.4   BP_SSD                 NEED UPGD  71.00     71.00
0/RP0      NCS1K4-CNTLR-K9       4.0   CPU_FPGA               CURRENT     1.14      1.14
0/RP0      NCS1K4-CNTLR-K9       5.4   CPU_SSD                NEED UPGD  71.00     71.00
0/PM1      NCS1K4-AC-PSU         0.1   PO-PriMCU              NEED UPGD   2.51      2.51
0/SC0      NCS1004               2.0   BP_FPGA                CURRENT     1.25      1.25
0/SC0      NCS1004               2.0   XGE_FLASH              CURRENT    18.04     18.04
```

Step 2 Use the **upgrade hw-module** command to upgrade the FPDs.

Example:

The following example shows how to upgrade the FPD image of a line card.

```
RP/0/RP0/CPU0:ios# upgrade hw-module location all fpd all
```

Upgrades the FPDs of line cards. The FPD upgrade process for line cards may take three to five minutes. The device automatically reloads after upgrading and it comes up with current status for all FPDs including BIOS.

Example:

From R7.5.2, the following example shows how to upgrade the FPD image of BP_SSD.

```
RP/0/RP0/CPU0:ios# upgrade hw-module location 0/RP0 fpd BP_SSD
```

Example:

From R7.5.2, the following example shows how to upgrade the FPD image of CPU_SSD.

```
RP/0/RP0/CPU0:ios# upgrade hw-module location 0/RP0 fpd CPU_SSD
```

Step 3 Use the **show hw-module fpd** command to verify the FPD status.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Fri May 29 11:30:24.492 UTC

Auto-upgrade:Disabled
                                                                          FPD Versions
                                                                          ==============
Location   Card type              HWver FPD device       ATR Status    Running   Programd
-------------------------------------------------------------------------------------------

0/0        NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW             CURRENT    21.31     21.31

0/0        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26      1.26

0/1        NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW             CURRENT    21.31     21.31

0/1        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26      1.26

0/2        NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW             CURRENT    21.31     21.31

0/2        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26      1.26

0/3        NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW             CURRENT    21.31     21.31

0/3        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26      1.26

0/RP0      NCS1K4-CNTLR-K9   1.14  BIOS              S       RLOAD REQ   5.10      5.10

0/RP0      NCS1K4-CNTLR-K9   5.4   BP_SSD                    RLOAD REQ   71.00     71.00
```

```
0/RP0     NCS1K4-CNTLR-K9   4.0   CPU_FPGA                  CURRENT      1.14      1.14

0/RP0     NCS1K4-CNTLR-K9   5.4   CPU_SSD                   RLOAD REQ   71.00     71.00

0/PM1     NCS1K4-AC-PSU     0.1   PO-PriMCU                 CURRENT      2.70      2.70

0/SC0     NCS1004           2.0   BP_FPGA                   CURRENT     1.25      1.25

0/SC0     NCS1004           2.0   XGE_FLASH                 CURRENT    18.04     18.04
```

Step 4 Reload NCS 1004 using the **hw-module location 0/RP0 reload** command if FPDs are in RLOAD REQ state.

You can verify the status of the FPDs after the upgrade. If the upgrade fails, the status displays as UPGD_FAIL. Otherwise, the FPD status displays as CURRENT.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Fri May 29 11:35:24.492 UTC

Auto-upgrade:Disabled
                                                                                FPD Versions
                                                                                ==============
Location   Card type             HWver FPD device       ATR Status    Running   Programd
-------------------------------------------------------------------------------------------
0/0        NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW              CURRENT    21.31     21.31

0/0        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW              CURRENT     1.26      1.26

0/1        NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW              CURRENT    21.31     21.31

0/1        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW              CURRENT     1.26      1.26

0/2        NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW              CURRENT    21.31     21.31

0/2        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW              CURRENT     1.26      1.26

0/3        NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW              CURRENT    21.31     21.31

0/3        NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW              CURRENT     1.26      1.26

0/RP0      NCS1K4-CNTLR-K9   1.14  BIOS              S        CURRENT     5.30      5.30

0/RP0      NCS1K4-CNTLR-K9   5.4   BP_SSD                     CURRENT    75.00     75.00

0/RP0      NCS1K4-CNTLR-K9   4.0   CPU_FPGA                   CURRENT     1.14      1.14

0/RP0      NCS1K4-CNTLR-K9   5.4   CPU_SSD                    CURRENT    75.00     75.00

0/PM1      NCS1K4-AC-PSU     0.1   PO-PriMCU                  CURRENT     2.70      2.70

0/SC0      NCS1004           2.0   BP_FPGA                    CURRENT     1.25      1.25

0/SC0      NCS1004           2.0   XGE_FLASH                  CURRENT    18.04     18.04
```

Note FPD upgrades from R7.0.1 to later releases do not have an impact on traffic. For R7.0.0 to R7.0.1 upgrade, there is an impact on traffic while upgrading the LC_OPT_MOD_FW FPD.

Note FPD upgrade of LC_CPU_MOD_FW FPD does not have an impact on traffic. However, there is an impact on traffic while upgrading the LC_DP_MOD_FW FPD.