System Setup and Software Installation Guide for Cisco NCS 1001

First Published: 2019-11-07

Last Modified: 2024-07-19

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 1001** 1

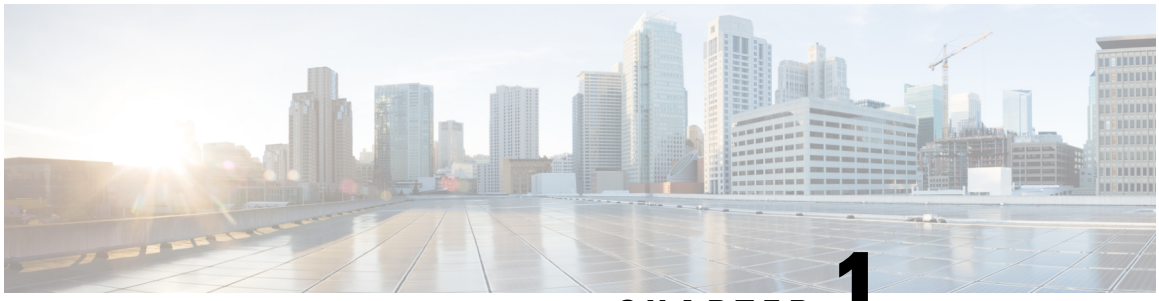
- Cisco NCS 1001 Overview 1
- Boot Sequence 2
- Boot NCS 1001 2
- Boot NCS 1001 Using USB Drive 3
- Boot Using iPXE 5
  - Setup DHCP Server 6
  - Boot Using iPXE 8
- Boot NCS 1001 Using Zero Touch Provisioning (ZTP) 8
  - Fresh Boot Using DHCP for ZTP 9
  - Build your Configuration File 11
  - Invoke ZTP Manually through CLI 12
  - Invoke ZTP Through Reload 13
  - ZTP Logging 15
  - Generate Tech Support Information for ZTP 17
  - IPv6 Support for ZTP 18
- Boot NCS 1001 Using Golden ISO 18
- Verify Boot Operation 19
- Accessing Consoles 20
- Configure Management Interface 22
- Configure Telnet 24
- Configure SSH 24
- Perform Clock Synchronization with NTP Server 25

CHAPTER 2 **Perform Preliminary Checks** 27

- Verify Status of Hardware Components 27

Verify Node Status 31
Verify Software Version 33
Verify Firmware Version 34
Verify Management Interface Status 36
Verify Alarms 37
Verify Environmental Parameters 38
Verify Inventory 40

CHAPTER 3 **Perform System Upgrade and Install Feature Packages** 43
Upgrade the System 43
Software Upgrade and Downgrade Matrix 43
Software Compatibility Matrix 44
Upgrade the Firmware 45
Upgrade BIOS and Daisy Duke FPDs 46
Upgrade Control FPGA and Control BKP FPDs 48
Upgrade PSM 49
Upgrade EDFA 51
Upgrade FPDs 52
Install Packages 56
Workflow for Install Process 56
Creating Repository to Access Files for Upgrading IOS XR Software 56
Create and Configure a Local Repository 57
Create and Configure an External Repository 58
Install Packages 59
Uninstall Packages 65



CHAPTER 1

Bring-up Cisco NCS 1001

After installing the hardware, boot the Cisco NCS 1001 system. You can connect to the XR console port and power on the system. NCS 1001 completes the boot process using the pre-installed operating system (OS) image. If no image is available, NCS 1001 can be booted using the iPXE boot or an external bootable USB drive.

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.

- Cisco NCS 1001 Overview, on page 1
- Boot Sequence, on page 2
- Boot NCS 1001, on page 2
- Boot NCS 1001 Using USB Drive, on page 3
- Boot Using iPXE, on page 5
- Boot NCS 1001 Using Zero Touch Provisioning (ZTP), on page 8
- Boot NCS 1001 Using Golden ISO, on page 18
- Verify Boot Operation, on page 19
- Accessing Consoles, on page 20
- Configure Management Interface, on page 22
- Configure Telnet, on page 24
- Configure SSH, on page 24
- Perform Clock Synchronization with NTP Server, on page 25

Cisco NCS 1001 Overview

Cisco NCS 1001 (NCS1001-K9) is 1 RU chassis that addresses the growing bandwidth needs of data center DWDM applications. It provides a DWDM line system that is optimized for data center environments and is optimized for point-to-point applications at maximum capacity. NCS 1001 supports up to three optical modules. The modules can be amplifiers, protection switching modules, or OTDR modules.

NCS 1001 has the following components:

- Removable control card
- Four removable fans
- Two removable 600W AC power supply modules (PSU)
- Three slots for optical modules. The Optical Amplifier Module (NCS1K-EDFA), Protection Switching Module (NCS1K-PSM), and Optical Time Domain Reflectometer (NCS1K-OTDR) module can be inserted in these slots.

  The optical modules can be inserted in slots 1 to 3. The optical modules can be inserted and removed from the slots while the system is operational. In amplified configuration, the Optical Amplifier module can be inserted in any slot. In protected configuration, the protect Optical Amplifier module is inserted in slot 1, Protection Switching Module in slot 2, and working Optical Amplifier module in slot 3. The OTDR line card can be inserted in any slot.

Boot Sequence

The boot sequence in NCS 1001 that you need to follow is:

1. Boot using SSD (hard disk)
2. Boot using USB drive
3. Boot using iPXE

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

Boot NCS 1001

Use the console port to connect to NCS 1001. By default, the console port connects to the XR mode. If required, subsequent connections can be established 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 115200 bps, 8 data bits, 1 stop bit and no parity.

Step 3 Power on the NCS 1001.

To turn on the power shelves, press the power switch up. As NCS 1001 boots up, the boot process details are displayed 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 the NCS 1001 more time to complete the initial boot procedure; then press **Enter**.

Important If the boot process fails, it may be because the pre-installed image on the NCS 1001 is corrupt. In this case, the NCS 1001 can be booted using an external bootable USB drive.

Boot NCS 1001 Using USB Drive

The bootable USB drive is used to re-image the NCS 1001 for the purpose of system upgrade or to boot the NCS 1001 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.

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

Before you begin

- You need a USB drive with a storage capacity of at least 4 GB.
- NCS 1001 software image can be downloaded from this location.
- Copy the compressed boot file from the software download page at cisco.com to your local machine. The file name for the compressed boot file is in the format *ncs1001-usb-boot-<release_number>.zip*. For example, *ncs1001-usb-boot-7.1.1.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.

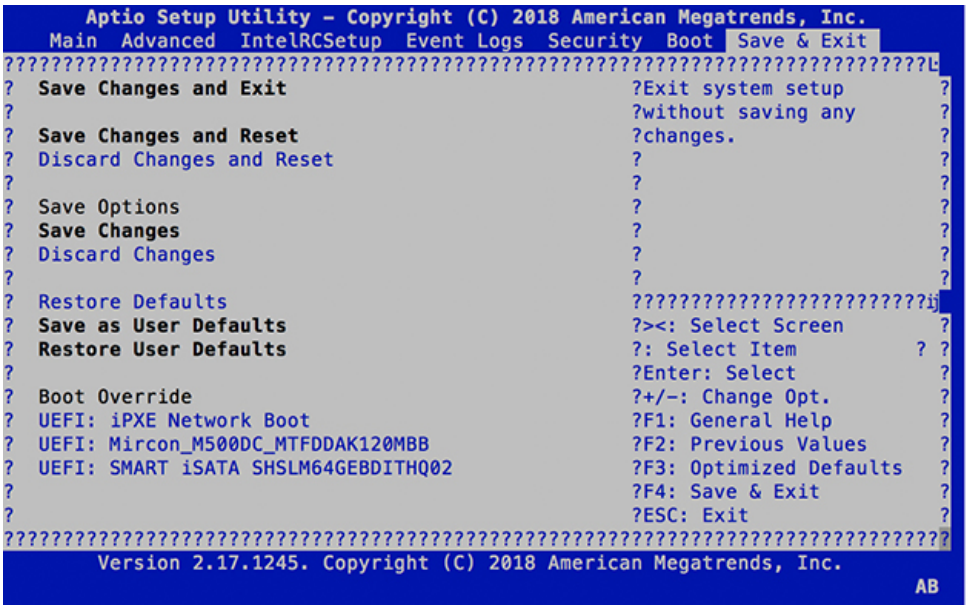
Note The content of the zipped file ("EFI" and "boot" directories) must be extracted directly in the root folder of the USB drive. If the unzipping application places the extracted files in a new folder, move the "EFI" and "boot" directories to the root folder of the USB drive.

Step 5 Insert the USB drive in one of the four USB ports of NCS 1001 after unplugging any other USB drive.

Step 6 Reboot NCS 1001 using power cycle or console.

Step 7 Press Esc to enter BIOS.

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



Step 9 Choose **UEFI based USB device**.

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 1001 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 re-image 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 boot loader and provides the flexibility to choose the image that the system will boot based on the Platform Identifier (PID), the Serial Number, or the management mac-address. iPXE must be defined in the DHCP server configuration file.

Note For IPv6 configuration, see **Step 2** in Setup DHCP Server, on page 6.

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 ncs1001
   {
   hardware ethernet ab:cd:ef:01:23:45;
   fixed-address <ip address>;
   filename "http://<httpserver-address>/<path-to-image>/ncs1001-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/ncs1001-mini-x-7.1.1.iso";
       } else {
           filename "http://10.89.205.127/box1/StartupConfig.cfg";
       }
       fixed-address 10.89.205.202;
    }
```

For example, for ipv6:

1. Use serial number of the chassis:

   The serial number of the chassis is derived from the XR command 'show inventory' and is used as an identifier. The S/N must be converted in an ipv6 DUID format.

   ```
   host ncs1001 {
     host-identifier  option dhcp-client-identifier "<IPV6-DIUD>";
     filename
   "<http,tftp>://<IPv6-dhcp-server-address>/<hardware-platform>-mini-x.iso";
   }
   ```

   Example

   ```
   host mys-p1b-212 {

      # PID: NCS1001-K9        , VID: V01, SN: CAT2018B02M

      host-identifier option dhcp6.client-id
   00:02:00:00:00:09:43:41:54:32:30:31:38:42:30:32:4d:00;

      if exists dhcp6.user-class and substring(option dhcp6.user-class, 2, 4) =
   "iPXE" {
        option dhcp6.bootfile-url
   "http://[2001:420:4491:2005::227:11]/rosco/mys-p1b-212/ncs1001-mini-mod.iso";
      }
      else {
        option dhcp6.bootfile-url
   "http://[2001:420:4491:2005::227:11]/rosco/mys-p1b-212/ztp.ipv6.sh";
      }
   }
   ```

   Here a simple shell script that converts from chassis S/N to DUID

   Example

   ```
   #! /bin/sh

   # Comply with IPv6 EN-DUID - see DHCPv6 RFC for detail
   ## 00:02 = Indicate Enterprise number based DUID
   ## 00:00:00:09 = CIsco Enterprise number
   ## 00 = Terminator

   SERIALNUMBER=$1
   en_duid=0002
   cisco_en=00000009

   sn=`xxd -l11 -pu <<< ${SERIALNUMBER}`
   null=00
   DHCPv6_DUID=`sed 's/\(..\)/\1:/g;s/:$//' <<< ${en_duid}${cisco_en}${sn}${null}`

   echo $DHCPv6_DUID
   ```

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
Wed Dec 23 15:29:57.376 UTC
Reload hardware module ? [no,yes]
```

The following example shows the output of the command:

```
iPXE 1.0.0+ (3e573) -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP TFTP VLAN EFI ISO9660 NBI Menu
Trying net0...
net0: c4:72:95:a6:14:e1 using dh8900cc on PCI01:00.1 (open)
[Link:up, TX:0 TXE:0 RX:0 RXE:0]
Configuring (net0 c4:72:95:a6:14:e1)..................... Ok << Talking to DHCP/PXE server to
 obtain network information
net0: 10.37.1.101/255.255.0.0 gw 10.37.1.0
net0: fe80::c672:95ff:fea6:14e1/64
net0: 2001:1800:5000:1:c672:95ff:fea6:14e1/64 gw fe80::20c:29ff:fefb:b9fe
net1: fe80::c672:95ff:fea6:14e3/64 (inaccessible)
Next server: 10.37.1.235
Filename: http://10.37.1.235/ncs1001/ncs1001-mini-x.iso
http://10.37.1.235/ncs1001/ncs1001-mini-x.iso ncs1000/ncs1001-mini-x.iso... 58% << Downloading
 file as indicated by DHCP/PXE server to boot install image
```

Boot NCS 1001 Using Zero Touch Provisioning (ZTP)

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

ZTP provides multiple options, such as:

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

Benefits of Using ZTP

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

- ZTP helps you to remotely provision a router anywhere in the network. Thus eliminates the need to send an expert to deploy network devices and reduces IT cost.

- Automated provisioning using ZTP can remove delay and increase accuracy and thus is cost-effective and provides better customer experience.

  By automating repeated tasks, ZTP allows network administrators to concentrate on more important stuff.

- ZTP process helps you to quickly restore service. Rather than troubleshooting an issue by hand, you can reset a system to well-known working status.

Prerequisites:

ZTP does not execute, if a username is already configured in the system.

Note For IPv6 configuration, see **Step 2** in Setup DHCP Server, on page 6.

ZTP is initiated in one of the following ways:

- **Automated Fresh Boot:**

  Fresh Boot: When you boot the device, the ZTP process initiates automatically if the device does not have a prior configuration. During the process, the router receives the details of the configuration file from the DHCP server. Use this method for devices that has no preloaded configuration. See Fresh Boot Using DHCP for ZTP, on page 9.

  You must define the configuration file or the bootscript that is downloaded from the DHCP server:

- **Configuration File**: The first line of the file must contain **!! IOS XR configuration**", to process the file as a configuration. If you are trying to bring up ten new nodes, you have to define ten configuration files. See Build your Configuration File, on page 11.

- **Manual Invocation using CLI:** Use this method when you want to forcefully initiate ZTP on a fully configured device, using CLI. See Invoke ZTP Manually through CLI, on page 12.

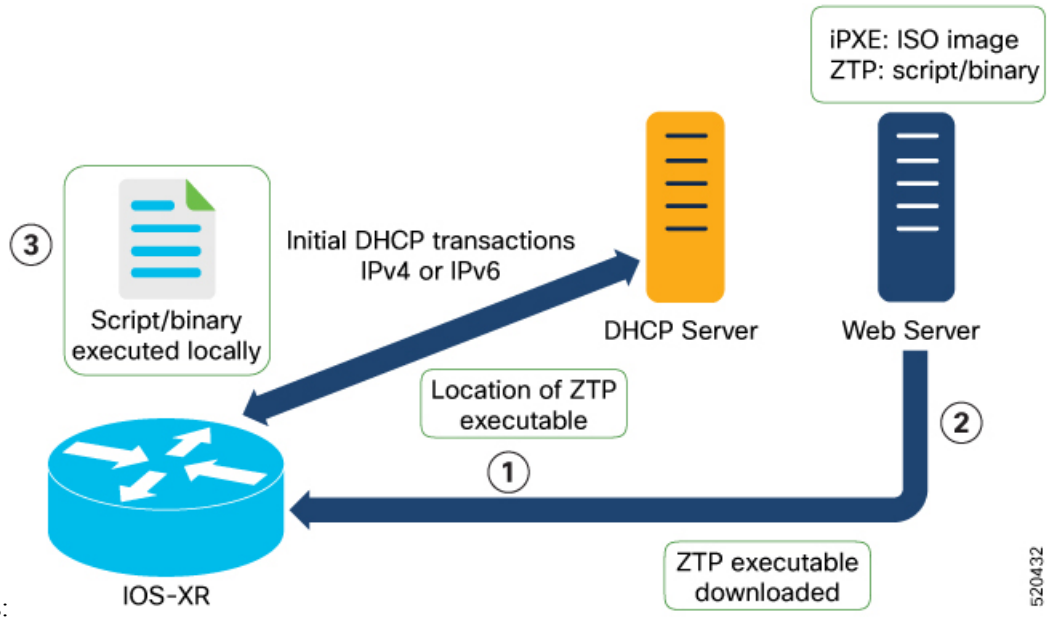
Fresh Boot Using DHCP for ZTP

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

Fresh Boot Using DHCP

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

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



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

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

1. ZTP sends DHCP request to fetch the ZTP configuration file or user script. To help the Bootstrap server uniquely identify the device, ZTP sends below DHCP option
   - DHCP(v4/v6) client-id=Serial Number
   - DHCPv4 option 124: Vendor, Platform, Serial-Number
   - DHCPv6 option 16: Vendor, Platform, Serial-Number

   The following is the default sequential flow of the ZTP process:
   - ZTP sends IPv4 DHCP request first on all the management port. In case there is a failure, then ZTP sends IPv6 DHCP request on all the management port.
   - ZTP sends IPv4 DHCP request first on all the data port. In case there is a failure, then ZTP sends IPv6 DHCP request on all the data port.

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

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

   DHCP server should be configured to respond with the DHCP options.
   - DHCPv4 using BOOTP filename to supply script/config location.
   - DHCPv4 using Option 67 (bootfile-name) to supply script/config location.
   - DHCPv6 using Option 59 (OPT_BOOTFILE_URL) to supply script/config location
   - For example, for IPv4:

```
host mys-p1b-209-Ztp {
option dhcp-client-identifier 00:02:00:00:00:09:43:41:54:32:31:30:37:42:30:4d:44:00;

  filename "http://192.0.2.10/ncs1000/mys-p1b-209-Ztp/-mini-x.iso";

}
```

For example, for IPv6:

```
host mys-p1b-209-Ztp {
                # PID: NCS1001-K9        , VID: V01, SN: CAT2107B0MD
                # needed for ztp
                host-identifier option dhcp6.client-id
00:02:00:00:00:09:43:41:54:32:31:30:37:42:30:4d:44:00;


                if exists dhcp6.user-class and substring(option dhcp6.user-class,
2, 4) = "iPXE" {
                        option dhcp6.bootfile-url
"http://[2001:DB8::4491:2005::227:11]/ncs1001/mys-p1b-209/ncs1001-mini-mod.iso";
                }
                else {
                        option dhcp6.bootfile-url
"http://[2001:DB8::4491:2005::227:11]/ncs1001/mys-p1b-209/ztp.ipv6.sh";
                }
        }
```

3. The network device downloads the file from the web server using the URI location that is provided in the DHCP response.
4. The device receives a configuration file or script file from the HTTP server.

Note

- If the downloaded file content starts with "!! IOS XR" it is considered as a configuration file.
- If the downloaded file content starts with #! /bin/bash, #! /bin/sh or #!/usr/bin/python it is considered as a script file.

5. The device applies the configuration file or executes the script or binary in the default bash shell.
6. The Network device is now up and running.

Build your Configuration File

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

The configuration file content starts with !! IOS XR.

The following is the sample configuration file for IPv4. You can automate all the configurations.

```
!! IOS XR Configuration version = 6.3.2
!
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
```

The following is the sample configuration file for IPv6.

```
!! IOS XR Configuration version = 7.10.1
!
telnet vrf default ipv6 server max-servers 20
!
vty-pool default 0 20 line-template default
!
interface MgmtEth0/RP0/CPU0/0
 ipv6 address dhcp6
 no shutdown
!
router static
 address-family ipv6 unicast
  2001:db8:1000::/36 2001:db8:2000:2::1
!
end
```

Invoke ZTP Manually through CLI

Manual ZTP can be invoked through CLI commands. This manual way helps you to provision the router in stages. Ideal for testing out ZTP configuration without a reboot. If you want to invoke a ZTP on an interface (data ports or management port), you don't have to bring up and configure the interface first. You can execute the ztp initiate command, even if the interface is down, ZTP script brings it up and invoke dhclient. So ZTP could run over all interfaces no matter it is up or down.

Use the ztp initiate, ztp terminate, and ztp clean commands to force ZTP to run over more interfaces.

- ztp initiate—Invokes a new ZTP DHCP session. Logs can be found in /disk0:/ztp/ztp.log.
- ztp terminate—Terminates any ZTP session in progress.
- ztp clean—Removes only the ZTP state files.

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

Procedure

Step 1 (optional) **ztp clean**

Example:

```
RP/0/RP0/CPU0:ios#ztp clean
Fri Apr 29 06:49:29.760 UTC
This would remove all ZTP temporary files.
Would you like to proceed? [no]: yes
All ZTP operation files have been removed.
ZTP logs are present in /var/log/ztp*.log for logrotate.
```

```
Please remove manually if needed.
If you now wish ZTP to run again from boot, do 'conf t/commit replace' followed by reload.
```

Removes all the ZTP logs and saved settings.

Step 2 **ztp initiate**

Example:

```
RP/0/RP0/CPU0:ios#ztp initiate
Fri Jun 17 11:44:08.791 UTC
Initiating ZTP may change your configuration.
Interfaces might be brought up if they are in shutdown state
Would you like to proceed? [no]: yes
ZTP will now run in the background.
Please use "show logging" or look at /var/log/ztp.log to check progress.
RP/0/RP0/CPU0:ios#
```

Use the **show logging** command or see the /var/log/ztp.log to check progress.

Reboots the Cisco NCS 1001 system.

Step 3 (Optional) **ztp terminate**

Example:

```
RP/0/RP0/CPU0:ios#ztp terminate
Fri Apr 29 06:38:59.238 UTC
This would terminate active ZTP session if any (this may leave your system in a partially
configured state)
Would you like to proceed? [no]: yes
Terminating ZTP
No ZTP process running
```

Terminates the ZTP process.

Note For IPv6 configuration, see **Step 2** in Setup DHCP Server, on page 6.

Invoke ZTP Through Reload

The ZTP process can be automatically invoked by using the reload command.

Procedure

Step 1 **configure**

Example:

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

Enters the configuration mode.

Step 2 **commit replace**

Example:

```
Fri Apr 29 06:48:46.236 UTC
RP/0/RP0/CPU0:ios(config)#commit replace
Fri Apr 29 06:48:53.199 UTC
```

```
This commit will replace or remove the entire running configuration. This
operation can be service affecting.
Do you wish to proceed? [no]: yes
RP/0/RP0/CPU0:ios(config)#
RP/0/RP0/CPU0:ios(config)#end
```

Removes the entire running configuration.

Step 3 **ztp clean**

Example:

```
RP/0/RP0/CPU0:ios#ztp clean
Fri Apr 29 06:49:29.760 UTC
This would remove all ZTP temporary files.
Would you like to proceed? [no]: yes
All ZTP operation files have been removed.
ZTP logs are present in /var/log/ztp*.log for logrotate.
Please remove manually if needed.
If you now wish ZTP to run again from boot, do 'conf t/commit replace' followed by reload.
```

Removes all the ZTP logs and saved settings.

Step 4 **reload**

Example:

```
RP/0/RP0/CPU0:ios#admin reload location 0/RP0 all
Fri Apr 29 06:50:29.760 UTC
Reload node ? [no,yes] yes
```

```
RP/0/RP0/CPU0:ios#admin hw-module location 0/RP0 reload
Fri Apr 29 06:52:29.760 UTC
Reload hardware module ? [no,yes] yes
```

After the node comes up, you can check that the ZTP is initiated and the configuration has been restored successfully.

```
RP/0/RP0/CPU0:Apr 29 06:55:33.242 UTC: pyztp2[377]: %INFRA-ZTP-4-CONFIG_INITIATED : ZTP has
 initiated config load and commit operations
RP/0/RP0/CPU0:Apr 29 06:55:39.263 UTC: ifmgr[381]: %PKT_INFRA-LINK-3-UPDOWN : Interface
GigabitEthernet0/0/0/0, changed state to Down
RP/0/RP0/CPU0:Apr 29 06:55:39.287 UTC: osa_driver[183]: %PKT_INFRA-FM-4-FAULT_MINOR :
ALARM_MINOR :PROV-INPROGRESS :DECLARE :GigabitEthernet0/0/0/0:
RP/0/RP0/CPU0:Apr 29 06:55:39.287 UTC: osa_driver[183]: %PKT_INFRA-FM-4-FAULT_MINOR :
ALARM_MINOR :PROV-INPROGRESS :DECLARE :Osc0/0/0/0:
RP/0/RP0/CPU0:Apr 29 06:55:39.287 UTC: ifmgr[381]: %PKT_INFRA-LINK-3-UPDOWN : Interface
GigabitEthernet0/0/0/0, changed state to Up
RP/0/RP0/CPU0:Apr 29 06:55:39.716 UTC: osa_driver[183]: %PKT_INFRA-FM-4-FAULT_MINOR :
ALARM_MINOR :PROV-INPROGRESS :CLEAR :Osc0/0/0/0:
RP/0/RP0/CPU0:Apr 29 06:55:39.728 UTC: osa_driver[183]: %PKT_INFRA-FM-4-FAULT_MINOR :
ALARM_MINOR :PROV-INPROGRESS :CLEAR :GigabitEthernet0/0/0/0:
RP/0/RP0/CPU0:Apr 29 06:55:47.904 UTC: osa_driver[183]: %PKT_INFRA-FM-4-FAULT_MINOR :
ALARM_MINOR :PROV-INPROGRESS :DECLARE :Ots0/0/0/1:

User Access Verification

Username: cisco
Password:
ios con0/RP0/CPU0 is now available
```

Reboots the Cisco NCS 1001 system.

ZTP Logging

ZTP logs its operation on the flash file system in the directory /disk0:/ztp/. ZTP logs all the transaction with the DHCP server and all the state transition.

The following example displays the execution of a simple configuration script that is downloaded from a management interface:

```
2023-05-12 14:43:18,406   5845 [Env          ] INF: MgmtDhcp4Fetcher fetcher created.
2023-05-12 14:43:18,482   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:idle.
Processing work: [privileged] start an engine. done = False
2023-05-12 14:43:18,484   5845 [Engine       ] INF: MgmtDhcp4Fetcher, current state:active:
 state changed to active
2023-05-12 14:43:18,508   5845 [Engine      ] DEB: ZAdmin, current state:active. Processing
 work: Monitor fetcher work for ZAdmin. done = False
2023-05-12 14:43:18,585   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: epoch work. done = False
2023-05-12 14:43:18,586   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: [privileged] getting engine status. done = False
2023-05-12 14:43:18,587   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: Bringing up interfaces before next retry. done = False
2023-05-12 14:43:18,589   5845 [Port         ] DEB: <Port count=1>: bringing interface(s)
up "MgmtEth0/RP0/CPU0/0"
2023-05-12 14:43:18,624   5845 [Port         ] DEB: Saving 1 interfaces to
/disk0:/ztp/xr_config/interface_list
2023-05-12 14:43:18,626   5845 [Engine      ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: Filtering up interfaces for MgmtDhcp4Fetcher. done = False
2023-05-12 14:43:18,627   5845 [Management   ] DEB: Determining operstate of interface:
brXRmgmt1
2023-05-12 14:43:18,666   5845 [Port         ] DEB: Filtered up interfaces: [Name:
MgmtEth0/RP0/CPU0/0 (Type: Management) (Up: False)]
2023-05-12 14:43:18,670   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: Setup interfaces for MgmtDhcp4Fetcher. done = False
2023-05-12 14:43:18,671   5845 [Env          ] INF: Env::getVlanIDs: vlan.mode:2
2023-05-12 14:43:18,672   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: Start Dhclient for MgmtDhcp4Fetcher. done = False
2023-05-12 14:43:18,687   5845 [Port         ] DEB: <Dhclient count=1>: started dhclient
using "ip netns exec xrnns /sbin/dhclient -4 -cf /etc/dhcp/dhclient.conf.ztp -lf
/var/lib/dhcp/dhclient.leases.ztp -sf /etc/dhcp/dhclient-script.ztp2 brXRmgmt1"
2023-05-12 14:43:19,090   5845 [Engine      ] DEB: ZAdmin, current state:active. Processing
 work: Checking for username configuration. done = False
2023-05-12 14:43:19,630   5845 [Engine      ] DEB: ZAdmin, current state:active. Processing
 work: Monitor fetcher work for ZAdmin. done = False
2023-05-12 14:43:19,692   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: [privileged] getting engine status. done = False
2023-05-12 14:43:20,696   5845 [Engine      ] DEB: ZAdmin, current state:active. Processing
 work: Monitor fetcher work for ZAdmin. done = False
2023-05-12 14:43:20,797   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: [privileged] getting engine status. done = False
2023-05-12 14:43:21,099   5845 [Engine      ] DEB: ZAdmin, current state:active. Processing
 work: Sending standby sync message. done = False
2023-05-12 14:43:21,212   5845 [Engine      ] DEB: ZAdmin, current state:active. Processing
 work: [privileged] getting engine status. done = False
2023-05-12 14:43:21,700   5845 [Engine       ] DEB: MgmtDhcp4Fetcher, current state:active.
 Processing work: Monitor dhclient for MgmtDhcp4Fetcher on interface ['brXRmgmt1']. done =
 False
2023-05-12 14:43:21,704   5845 [MgmtDhcp4Fetcher] DEB: Received DHCP4 response
2023-05-12 14:43:21,705   5845 [MgmtDhcp4Fetcher] INF: (dhclient env) reason=BOUND
```

```
2023-05-12 14:43:21,706   5845 [MgmtDhcp4Fetcher] INF: (dhclient env) interface=brXRmgmt1
2023-05-12 14:43:21,706   5845 [MgmtDhcp4Fetcher] INF: (dhclient env)
new_ip_address=10.58.227.177
2023-05-12 14:43:21,707   5845 [MgmtDhcp4Fetcher] INF: (dhclient env)
new_network_number=10.58.227.0
2023-05-12 14:43:21,708   5845 [MgmtDhcp4Fetcher] INF: (dhclient env)
new_subnet_mask=255.255.255.0
2023-05-12 14:43:21,708   5845 [MgmtDhcp4Fetcher] INF: (dhclient env)
new_broadcast_address=10.58.227.255
2023-05-12 14:43:21,709   5845 [MgmtDhcp4Fetcher] INF: (dhclient env) new_routers=10.58.227.1
2023-05-12 14:43:21,710   5845 [MgmtDhcp4Fetcher] INF: (dhclient env)
new_dhcp_server_identifier=10.58.227.11
2023-05-12 14:43:21,711   5845 [MgmtDhcp4Fetcher] INF: (dhclient env)
new_domain_name=cisco.com
2023-05-12 14:43:21,711   5845 [MgmtDhcp4Fetcher] INF: (dhclient env)
new_domain_name_servers=198.51.100.3 198.51.100.1
2023-05-12 14:43:21,712   5845 [MgmtDhcp4Fetcher] INF: (dhclient env)
new_filename=http://10.58.227.11/rosco/mys-p1b-212/ztp.sh
2023-05-12 14:43:21,713   5845 [MgmtDhcp4Fetcher] INF: (dhclient env) new_ip6_prefixlen=64
2023-05-12 14:43:21,714   5845 [Engine      ] INF: MgmtDhcp4Fetcher, current state:active,
 exit code:success
2023-05-12 14:43:21,815   5845 [Engine      ] DEB: ZAdmin, current state:active. Processing
 work: Monitor fetcher work for ZAdmin. done = False
2023-05-12 14:43:21,828   5845 [Port        ] DEB: Dhclient processes:
root      7033  0.0  0.0  31096  7312 ?        Ss   14:46   0:00 /sbin/dhclient -4 -cf
/etc/dhcp/dhclient.conf.ztp -lf /var/lib/dhcp/dhclient.leases.ztp -sf
/etc/dhcp/dhclient-script.ztp2 brXRmgmt1
root      7052  0.0  0.0  20316  1592 ?        S    14:46   0:00 /bin/sh -c ps aux | grep
dhclient
root      7054  0.0  0.0  16248   948 ?        Sl   14:46   0:00 grep dhclient
2023-05-12 14:43:21,830   5845 [Port        ] DEB: <Dhclient count=1>: dhclient 4 is
stopped: keepIpAddress=True
2023-05-12 14:43:21,831   5845 [Engine      ] INF: MgmtDhcp4Fetcher, current state:final,
 exit code:success: state changed to final
2023-05-12 14:43:21,832   5845 [Engine      ] DEB: MgmtDhcp4Fetcher, current state:final,
 exit code:success. Processing work: [privileged] getting engine status. done = False
2023-05-12 14:43:21,834   5845 [MgmtDhcp4Fetcher] DEB: dhcp: shutdown : Entry
2023-05-12 14:43:21,933   5845 [Engine      ] DEB: MgmtDhcp4Fetcher, current state:final,
 exit code:success. Processing work: [privileged] prepare engine shutdown. done = False
2023-05-12 14:43:22,035   5845 [Engine      ] DEB: MgmtDhcp4Fetcher, current state:final,
 exit code:success. Processing work: [privileged] shutting down MgmtDhcp4Fetcher engine.
done = False
2023-05-12 14:43:22,036   5845 [Engine      ] INF: MgmtDhcp4Fetcher, current state:final,
 exit code:shutdown
2023-05-12 14:43:22,037   5845 [Engine      ] INF: MgmtDhcp4Fetcher, exit code:shutdown:
state changed to None
2023-05-12 14:43:22,038   5845 [Engine      ] DEB: MgmtDhcp4Fetcher, exit code:shutdown:
breaking engine loop after shutdown
2023-05-12 14:43:22,039   5845 [Engine      ] DEB: ZAdmin, current state:active. Processing
 work: Setup fetching. done = False
2023-05-12 14:43:22,039   5845 [Engine      ] DEB: MgmtDhcp4Fetcher, exit code:shutdown:
end of event loop
2023-05-12 14:43:22,052   5845 [Env         ] DEB: No authentication required for Mgmt
Interface
2023-05-12 14:43:22,053   5845 [Env         ] DEB: No authentication required when initiated
 using CLI
2023-05-12 14:43:22,055   5845 [Xr          ] DEB: Writing to file
/tmp/ztp2-fzwmlfid/sysdb_cfg_cmd.tmp
2023-05-12 14:43:22,181   5845 [Xr          ] DEB: No inconsistency found in config
2023-05-12 14:43:23,460   5845 [Xr          ] DEB: Applying TPA default route
2023-05-12 14:43:23,523   5845 [Xr          ] DEB: No IPv4 Address assigned to linux
management interface
2023-05-12 14:43:23,524   5845 [Xr          ] DEB: Applying IPv4 configuration
2023-05-12 14:43:23,525   5845 [Xr          ] DEB: Validating IP Address: 10.58.227.177
```

```
2023-05-12 14:43:23,527   5845 [Xr          ] DEB: Applying IPv4 gateway route configuration
2023-05-12 14:43:23,527   5845 [Xr            ] DEB: Validating DHCP server identifier IP
Address: 10.58.227.11
2023-05-12 14:43:23,528   5845 [Xr          ] DEB: Validating Gateway IP Address: 10.58.227.1
2023-05-12 14:43:23,530   5845 [Xr            ] DEB: Configuring domain name with
domain-name-server 198.51.100.3 198.51.100.1
2023-05-12 14:43:23,532   5845 [Configuration] DEB: Config file type is IOS XR config.
Replace False
2023-05-12 14:43:23,534   5845 [Configuration] DEB: Applying following config:
tpa
 vrf default
  address-family ipv4
   default-route mgmt
  address-family ipv6
   default-route mgmt

interface MgmtEth0/RP0/CPU0/0
no ipv4 address
ipv4 address 10.58.227.177 255.255.255.0
no shutdown

tpa
 vrf default
  address-family ipv4
   default-route mgmt
router static
 address-family ipv4 unicast
  0.0.0.0/0 10.58.227.1

domain name cisco.com

domain name-server 198.51.100.3

domain name-server 198.51.100.1
```

Generate Tech Support Information for ZTP

When you have a problem in the ZTP process that you cannot resolve, the resource of last resort is your Cisco Systems technical support representative. To analyze a problem, your technical support representative needs certain information about the situation and the symptoms that you are experiencing. To speed up the problem isolation and resolution process, collect the necessary data before you contact your representative.

Use the **show tech-support ztp** command to collect all debugging information of the ZTP process.

Example:

```
RP/0/RP0/CPU0:R1#show tech-support ztp
Thu Jun 15 08:33:27.531 UTC
++ Show tech start time: 2022-Jul-28.083327.UTC ++
Thu Jul 28 08:33:28 UTC 2022 Waiting for gathering to complete
..
Thu Jul 15 08:33:34 UTC 2022 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-R1-ZTP-2022-Jul-28.083327.UTC.tgz
++ Show tech end time: 2022-Jul-28.083334.UTC ++
RP/0/RP0/CPU0:R1#
```

In the above example, the tech support information is saved as .tgz file in the specified location. This information can be shared with the Cisco Technical Support representatives for troubleshooting the ZTP process.

IPv6 Support for ZTP

Table 1: Feature History

Feature Name	Release Information	Description
IPv6 Support for ZTP	Cisco IOS XR Release 7.10.1	From this release, the DHCP server supports Zero Touch Provisioning (ZTP) to bring up the NCS 1001 nodes with IPv6 addressing. The DHCP configuration file must be updated with the dhcp6.client id and IPv6 address-based bootfile URL. IPv6 addressing ensures efficient and secure management of the devices.

From Release 7.10.1, you can bring up the NCS 1001 nodes that are enabled with IPv6, using the DHCP configuration file updated with dhcp6.client id and IPv6 address based bootfile URL. See IPv6 configuration file.

Boot NCS 1001 Using Golden ISO

Golden ISO is a feature provided to user for building customized ISO using mini ISO, required SMUs and IOS-XR configuration.

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

Step 1 : Boot the system with mini ISO. This can be done using iPXE or USB boot.

Step 2 : Install, add, and activate all the relevant SMUs/optional packages on to NCS 1001. NCS 1001 reloads on reload of any SMUs.

Step 3 : Apply IOS-XR configuration.

Benefits of Golden ISO

- Saves installation effort and time.
- System gets ready in a single command and single boot.

Golden ISO is built using ‘gisobuild.py’script, which is available at /pkg/bin/gisobuild.py location.

Prerequisites

- The tools 'mount','rm','cp','umount','zcat','chroot','mkisofs' must be available and the user must have privilege to execute these tools.
- Python version must be 2.7
- The gisobuild.py script can be run either on a Linux machine or a NCS 1001 system. Destination must be an EXT file system. FAT32, NTFS file systems are not supported.

- If gisobuild.py is running on a NCS 1001 system, the environment variable PYTHONPATH must be set as export PYTHONPATH = /pkg/bin.
- System must have at least 3 GB to 4 GB of free disk space.
- Mini iso is mandatory.

  argument -r RPMREPO is mandatory.
- Kernel version of the system must be greater than 3.16 or the version of kernel of cisco iso.
- User must have proper permission for security rpm(k9sec-rpm) in rpm repository, otherwise security rpm would be ignored for Golden ISO creation.

Limitations

- install operation over IPv6 is not supported.

Golden ISO file is created in the following format:

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

Example: ncs1001-golden-x-7.1.1.14I-V1.iso

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

Example: ncs1001-goldenk9-x-7.1.1.14I-V1.iso

Boot NCS 1001 using GISO

The following steps are used to boot NCS 1001 using giso image.

Step 1 : Create the giso image using the gisobuild.py script available at /pkg/bin.

Step 2 : Create the usb zip package using the following command.

/create_usb_zip ncs1001 ncs1001xxxxx-giso.iso

Step 3 : Extract and copy the content of zip package and copy in the USB to be used for boot.

Step 4 : Insert the USB in the usb port under test.

Step 5 : Reboot the system and install the new image.

Step 6 : After the system reboots, check the configuration using show running-config command, release using show version command, and the installed packages using show install active command.

Verify Boot Operation

Procedure

Step 1 After the boot operation, reload the NCS 1001.

Step 2 **show version**

Example:

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

```
Tue Jan 14 12:31:05.745 CET
Cisco IOS XR Software, Version 7.1.1
Copyright (c) 2013-2019 by Cisco Systems, Inc.
Build Information:
Built By : nkhai
Built On : Tue Jan 7 16:31:55 PST 2020
Built Host : iox-lnx-071
Workspace : /auto/iox-lnx-071-san1/prod/7.1.1/ncs1001/ws
Version : 7.1.1
Location : /opt/cisco/XR/packages/
Label : 7.1.1
cisco NCS-1001 () processor
```

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

Accessing Consoles

Table 2: Feature History

Feature Name	Release	Description
Console Swap for NCS 1001	Cisco IOS XR Release 7.8.1	Console swap feature provides a quicker and simpler way to toggle between the following console sessions using a keyboard shortcut: • from XR to Admin console • from Admin to Host console • from Host to XR console

NCS 1001 has three types of consoles to interact with it. After entering the root username and password, you are logged in to the XR console. From the XR console, you can switch to the System Admin console and then to the host console using CLI commands.

The following table lists the console session available on NCS 1001.

Table 3: Console Types

Console Type	Functions
XR Console	Run the regular CLI commands to configure and manage the node.
System Admin Console	Perform all system administration and hardware management setups.
Host Console	Run the Linux commands such as pwd, scp, cp, traceroute, ls -la and so on.

From Release 7.8.1, you can enter **Ctrl+O** to swap between the console session, host session, and XR session. This keyboard shortcut enables you to toggle between consoles without using several CLI commands. However, you can still use the CLI commands to toggle between the console sessions.

The following table lists the CLI to move between consoles.

Table 4: Source and Target Console Swap for NCS 1001

Changing Console Session		Command Prompt	Keyboard Shortcut	Notes
From	To			
XR console	System Admin console	**XR console** RP/0/RP0/CPU0:ios#**admin** **System Admin console** sysadmin-vm:0_RP0#	CTRL+O **Example** **RP/0/RP0/CPU0#** Disconnecting from 'default-sdr--1' console. Continue(Y/N)? (Enter -> Y and then <enter> to confirm) Connecting to 'default-sdr--1' console Connecting to 'sysadmin' console ▒▒▒▒▒▒▒▒▒▒ System Admin Username: <enter username> Password: <enter password> **sysadmin-vm:0_RP0#**	When entering the System Admin console for the first time, you must provide the username and password to continue with the System Admin console. To return to the XR console from the System Admin console using CLI, enter **exit**.
System Admin console	Host console	**System Admin console** sysadmin-vm:0_RP0#**run** sysadmin-vm:0_RP0#**ssh 10.0.2.16** **Host console** [host:~]$	CTRL+O **Example** **sysadmin-vm:0_RP0#** Disconnecting from 'sysadmin' console. Continue(Y/N)? (Enter -> Y and then <enter> to confirm) Connecting to 'host' console host login:<username> Password:<password> **[host:/]$**	When entering the host console for the first time, you must provide the username and password to continue with the host console. To access the host console, use the internal host IP address 10.0.2.16 using SSH.

Changing Console Session		Command Prompt	Keyboard Shortcut	Notes
From	To			

Host console	XR console	**Host console**
		`[host:~]$exit`
		`logout`
		`Connection to 10.0.2.16 closed.`
		`[sysadmin-vm:0_RP0:~]$`
		`[sysadmin-vm:0_RP0:~]$exit`
		`exit`
		`sysadmin-vm:0_RP0#`
		`sysadmin-vm:0_RP0#exit`
		`Thu Oct 13 10:08:17.162 UTC+00:00`
		`RP/0/RP0/CPU0#`
		XR console
		RP/0/RP0/CPU0:ios#
			CTRL+O
			Example
			`[host:/]$`
			`Disconnecting from host console. Continue(Y/N)? (Enter -> Y and then <enter> to confirm)`
			`Connecting to 'default-sdr--1' console`
			`RP/0/RP0/CPU0#`
				When toggling from host console to XR console using CLI, you must enter **exit** to switch to System Admin console. Then in Admin console, enter **exit** twice to switch to XR console.

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 need to configure a default (static) route for the NCS 1001.

The range of supported MTU of management plane is 64 to 1514 bytes.

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:

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

For IPv4, use the following command.

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

For IPv6, use the following command.

ipv6 address *ipv6-address subnet-mask*

Example:

```
RP/0/RP0/CPU0:ios(config-if)# ipv6 address 2001:420:4491:2000::229:118/64
```

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:

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

For IPv4, use the following command

Example:

```
RP/0/RP0/CPU0:ios(config)# router static address-family ipv4 unicast 0.0.0.0/0 198.51.100.2
```

For IPv6, use the following command.

Example:

```
RP/0/RP0/CPU0:ios(config)# router static address-family ipv6 unicast ::/0
2001:420:4491:2000::228:2
```

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

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

end-Prompts user to take one of these actions:

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

What to do next

Configure Telnet, on page 24 and Configure SSH, on page 24.

Configure Telnet

With a terminal emulation program, 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 Telnet servers are allowed. 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, on page 24

Configure SSH

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

Before you begin

- Install the ncs1001-k9sec package on the NCS 1001. For details about package installation, see Install Packages, on page 59.
- 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 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 1001.

What to do next

Perform Clock Synchronization with NTP Server, on page 25

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 need to be synchronized with the clock of a NTP server. In this task you will configure a 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 and connect to the management port.

Procedure

Step 1 **configure**

Example:

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

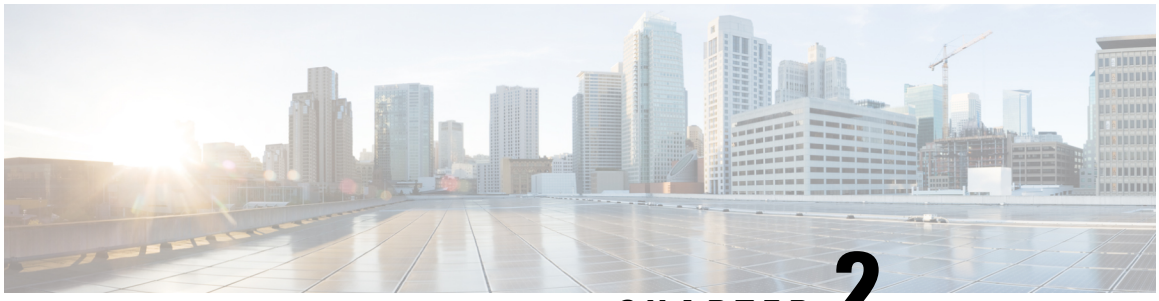
Enters XR Configuration mode.

Step 2 **ntp server** *server_address*

Example:

```
RP/0/RP0/CPU0:ios# ntp server 198.51.100.4
```

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



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 when these checks are performed, 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, on page 27
- Verify Node Status, on page 31
- Verify Software Version, on page 33
- Verify Firmware Version, on page 34
- Verify Management Interface Status, on page 36
- Verify Alarms, on page 37
- Verify Environmental Parameters, on page 38
- Verify Inventory, on page 40

Verify Status of Hardware Components

To verify the status of all the hardware components installed on the NCS 1001, perform the following procedure.

Before you begin

Ensure that all the required hardware components have been installed on the NCS 1001. For installation details, see *Cisco Network Convergence System 1001 Hardware Installation Guide*.

Procedure

Step 1 **show platform**

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

Example:

```
RP/0/RP0/CPU0:ios# show platform
Sun Mar  5 02:33:53.075 CET
Node              Type                       State             Config state
--------------------------------------------------------------------------------

0/0               NCS1001-K9                 OPERATIONAL       NSHUT
0/3               NCS1K-EDFA                 OPERATIONAL       NSHUT
0/RP0/CPU0        NCS1K-CNTLR2(Active)       IOS XR RUN        NSHUT
0/FT0             NCS1K1-FAN                 OPERATIONAL       NSHUT
0/FT1             NCS1K1-FAN                 OPERATIONAL       NSHUT
0/FT2             NCS1K1-FAN                 OPERATIONAL       NSHUT
0/FT3             NCS1K1-FAN                 OPERATIONAL       NSHUT
```

a) If the 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 from the **show sdr** command in Cisco IOS XR mode.

```
RP/0/RP0/CPU0:ios# show sdr
Sun Mar  5 02:37:09.174 CET
Type                 NodeName       NodeState      RedState       PartnerName
--------------------------------------------------------------------------------

NCS1001-K9           0/0            OPERATIONAL                   N/A

NCS1K-EDFA           0/3            OPERATIONAL                   N/A

RP                   0/RP0/CPU0     IOS XR RUN     ACTIVE         NONE

NCS1K-CNTLR2         0/RP0          OPERATIONAL                   N/A

NCS1K1-FAN           0/FT0          OPERATIONAL                   N/A

NCS1K1-FAN           0/FT1          OPERATIONAL                   N/A

NCS1K1-FAN           0/FT2          OPERATIONAL                   N/A

NCS1K1-FAN           0/FT3          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 for each node in the system.

Example:

```
sysadmin-vm:0_RP0# show platform
Sun Mar  5  01:38:22.282 UTC
Location  Card Type               HW State      SW State      Config State
--------------------------------------------------------------------------------
0/0       NCS1001-K9              OPERATIONAL   N/A           NSHUT
0/3       NCS1K-EDFA              OPERATIONAL   N/A           NSHUT
0/RP0     NCS1K-CNTLR2            OPERATIONAL   OPERATIONAL   NSHUT
0/FT0     NCS1K1-FAN              OPERATIONAL   N/A           NSHUT
0/FT1     NCS1K1-FAN              OPERATIONAL   N/A           NSHUT
0/FT2     NCS1K1-FAN              OPERATIONAL   N/A           NSHUT
```

```
0/FT3     NCS1K1-FAN              OPERATIONAL   N/A           NSHUT
```

Verify that all components of the NCS 1001 are displayed in the result. 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 experienced some internal failure.
- PRESENT—Node is in the shutdown state.
- OFFLINE—User has changed the node state to OFFLINE. The node is accessible for diagnostics.

Software states:

- OPERATIONAL—Software is operating normally and is fully functional.
- SW_INACTIVE—Software is not completely operational.
- FAILED—Software is operational but the card has experienced some internal failure.
- N/A—Valid option for modules where software is not running.

Step 4 **show platform detail**

Displays the hardware and software states, and other details of the node.

Example:

```
sysadmin-vm:0_RP0# show platform detail
Sun Mar  5  01:39:45.411 UTC

Platform Information for 0/0
 PID :               NCS1001-K9
 Description :       "Network Convergence System 1001 line system 3 slots"
 VID/SN :            V00
 HW Oper State :     OPERATIONAL
 SW Oper State :     N/A
 Configuration :     "NSHUT RST"
 HW Version :        0.1
 Last Event :        HW_EVENT_OK
 Last Event Reason : "HW Event OK"

Platform Information for 0/3
 PID :               NCS1K-EDFA
 Description :       "Network Convergence System 1000 amplifier module"
 VID/SN :            V01
 HW Oper State :     OPERATIONAL
 SW Oper State :     N/A
 Configuration :     "NSHUT RST"
 HW Version :        0.1
 Last Event :        HW_EVENT_OK
 Last Event Reason : "HW Operational"

Platform Information for 0/RP0
 PID :               NCS1K-CNTLR2
 Description :       "Network Convergence System 1000 Controller 2"
 VID/SN :            V01
 HW Oper State :     OPERATIONAL
```

```
 SW Oper State :     OPERATIONAL
 Configuration :     "NSHUT RST"
 HW Version :        0.1
 Last Event :        HW_EVENT_OK
 Last Event Reason : UNKNOWN

Platform Information for 0/FT0
 PID :               NCS1K1-FAN
 Description :       "Network Convergence System 1001 Fan"
 VID/SN :            V01
 HW Oper State :     OPERATIONAL
 SW Oper State :     N/A
 Configuration :     "NSHUT RST"
 HW Version :        0.0
 Last Event :        HW_EVENT_OK
 Last Event Reason : "HW Operational"

Platform Information for 0/FT1
 PID :               NCS1K1-FAN
 Description :       "Network Convergence System 1001 Fan"
 VID/SN :            V01
 HW Oper State :     OPERATIONAL
 SW Oper State :     N/A
 Configuration :     "NSHUT RST"
 HW Version :        0.0
 Last Event :        HW_EVENT_OK
 Last Event Reason : "HW Operational"
```

Step 5 **show inventory**

Displays the details of the physical entities of the NCS 1001 when you execute this command in the Cisco IOS XR EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# show inventory
Sun Mar  5 02:42:04.865 CET
NAME: "0/0", DESCR: "Network Convergence System 1001 line system 3 slots"
PID: NCS1001-K9        , VID: V00, SN: CAT2018B033

NAME: "0/3", DESCR: "Network Convergence System 1000 amplifier module"
PID: NCS1K-EDFA        , VID: V01, SN: IIF2044002L

NAME: "0/3-PORT-0", DESCR: "Cisco SFP Pluggable Optics Module"
PID: ONS-SC-Z3-1510    , VID: V02 , SN: FNS200801EK

NAME: "0/RP0", DESCR: "Network Convergence System 1000 Controller 2"
PID: NCS1K-CNTLR2      , VID: V01, SN: CAT2051B0R5

NAME: "0/RP0-SFP-PORT", DESCR: "Unqualified SFP Pluggable Optics Module"
PID: UNQUALIFIED-SFP   , VID: N/A, SN: N/A

NAME: "Rack 0", DESCR: "Network Convergence System 1001 line system 3 slots"
PID: NCS1001-K9        , VID: V00, SN: CAT2018B033

NAME: "0/FT0", DESCR: "Network Convergence System 1001 Fan"
PID: NCS1K1-FAN        , VID: V01, SN: N/A

NAME: "0/FT1", DESCR: "Network Convergence System 1001 Fan"
PID: NCS1K1-FAN        , VID: V01, SN: N/A

NAME: "0/FT2", DESCR: "Network Convergence System 1001 Fan"
PID: NCS1K1-FAN        , VID: V01, SN: N/A

NAME: "0/FT3", DESCR: "Network Convergence System 1001 Fan"
```

```
PID: NCS1K1-FAN        , VID: V01, SN: N/A

NAME: "0/PM0", DESCR: "Network Convergence System 1000 2KW AC PSU 2"
PID: NCS1K-2KW-AC2     , VID: V01, SN: POG2049JT21

NAME: "0/PM1", DESCR: "Network Convergence System 1000 2KW AC PSU 2"
PID: NCS1K-2KW-AC2     , VID: V01, SN: POG2049JT01
```

Verify Node Status

You can verify the operational status of all the nodes using the **show platform** command. You can execute this command independently from both the Cisco IOS XR EXEC and System Admin EXEC modes.

To verify the operational status of all the nodes, perform the following procedure.

Procedure

Step 1 **show platform**

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

Example:

```
RP/0/RP0/CPU0:ios# show platform
Sun Mar  5 02:53:27.755 CET
Node              Type                       State             Config state
--------------------------------------------------------------------------------

0/0               NCS1001-K9                 OPERATIONAL       NSHUT
0/3               NCS1K-EDFA                 OPERATIONAL       NSHUT
0/RP0/CPU0        NCS1K-CNTLR2(Active)       IOS XR RUN        NSHUT
0/FT0             NCS1K1-FAN                 OPERATIONAL       NSHUT
0/FT1             NCS1K1-FAN                 OPERATIONAL       NSHUT
0/FT2             NCS1K1-FAN                 OPERATIONAL       NSHUT
0/FT3             NCS1K1-FAN                 OPERATIONAL       NSHUT
```

If the Cisco IOS XR is not operational, no output is shown in the result. In this case, verify the state of SDR on the node using the **show sdr** command in the System Admin EXEC mode.

Step 2 **admin**

Enters System Admin EXEC mode.

Example:

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

Step 3 **show platform**

Displays information and status for each node in the system.

Example:

```
sysadmin-vm:0_RP0# show platform
Sun Mar  5  01:56:15.749 UTC
Location  Card Type              HW State      SW State      Config State
--------------------------------------------------------------------------------
```

```
0/0       NCS1001-K9              OPERATIONAL   N/A           NSHUT
0/3       NCS1K-EDFA              OPERATIONAL   N/A           NSHUT
0/RP0     NCS1K-CNTLR2            OPERATIONAL   OPERATIONAL   NSHUT
0/FT0     NCS1K1-FAN              OPERATIONAL   N/A           NSHUT
0/FT1     NCS1K1-FAN              OPERATIONAL   N/A           NSHUT
0/FT2     NCS1K1-FAN              OPERATIONAL   N/A           NSHUT
0/FT3     NCS1K1-FAN              OPERATIONAL   N/A           NSHUT
```

Verify that all the modules of NCS 1001 are displayed in the result. 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 experienced some internal failure.
- PRESENT—Node is in the shutdown state.
- OFFLINE—User has changed the node state to OFFLINE. The node is accessible for diagnostics.

Software states:

- OPERATIONAL—Software is operating normally and is fully functional.
- DIAG_MODE—User has changed the card state to OFFLINE for diagnosis.
- SW_INACTIVE—Software is not completely operational.
- FAILED—Software is operational but the card has experienced some internal failure.
- N/A—Valid option for modules where software is not running.

Step 4 **show platform detail**

Displays the hardware and software states, and other details of the node.

Example:

```
sysadmin-vm:0_RP0# show platform detail
Sun Mar  5  01:57:40.918 UTC

Platform Information for 0/0
 PID :               NCS1001-K9
 Description :       "Network Convergence System 1001 line system 3 slots"
 VID/SN :            V00
 HW Oper State :     OPERATIONAL
 SW Oper State :     N/A
 Configuration :     "NSHUT RST"
 HW Version :        0.1
 Last Event :        HW_EVENT_OK
 Last Event Reason : "HW Event OK"

Platform Information for 0/3
 PID :               NCS1K-EDFA
 Description :       "Network Convergence System 1000 amplifier module"
 VID/SN :            V01
 HW Oper State :     OPERATIONAL
 SW Oper State :     N/A
 Configuration :     "NSHUT RST"
 HW Version :        0.1
```

```
 Last Event :        HW_EVENT_OK
 Last Event Reason : "HW Operational"

Platform Information for 0/RP0
 PID :               NCS1K-CNTLR2
 Description :       "Network Convergence System 1000 Controller 2"
 VID/SN :            V01
 HW Oper State :     OPERATIONAL
 SW Oper State :     OPERATIONAL
 Configuration :     "NSHUT RST"
 HW Version :        0.1
 Last Event :        HW_EVENT_OK
 Last Event Reason : UNKNOWN

Platform Information for 0/FT0
 PID :               NCS1K1-FAN
 Description :       "Network Convergence System 1001 Fan"
 VID/SN :            V01
 HW Oper State :     OPERATIONAL
 SW Oper State :     N/A
 Configuration :     "NSHUT RST"
 HW Version :        0.0
 Last Event :        HW_EVENT_OK
 Last Event Reason : "HW Operational"

Platform Information for 0/FT1
 PID :               NCS1K1-FAN
 Description :       "Network Convergence System 1001 Fan"
 VID/SN :            V01
 HW Oper State :     OPERATIONAL
 SW Oper State :     N/A
 Configuration :     "NSHUT RST"
 HW Version :        0.0
 Last Event :        HW_EVENT_OK
 Last Event Reason : "HW Operational"
```

Verify Software Version

The NCS 1001 is shipped with the Cisco IOS XR software pre-installed. Verify that the latest version of the software is installed. If a newer version is available, perform a system upgrade. This will install the newer version of the software and provide the latest feature set on the NCS 1001.

To verify the version of Cisco IOS XR software running on the NCS 1001, 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
Mon Feb 28 15:52:01.424 UTC
Cisco IOS XR Software, Version 7.3.2
```

```
Copyright (c) 2013-2021 by Cisco Systems, Inc.

Build Information:
Built By     : deenayak
Built On     : Mon Jul 28 01:19:52 PST 2020
Built Host   : iox-lnx-071
Workspace    : /auto/srcarchive15/prod/7.3.2/ncs1001/ws
Version      : 7.3.2
Location     : /opt/cisco/XR/packages/
Label        : 7.3.2
cisco NCS-1001 () processor
```

What to do next

Verify the result to ascertain whether a system upgrade is required. If the upgrade is required, see the Perform System Upgrade and Install Feature Packages, on page 43 chapter.

Verify Firmware Version

The firmware on various hardware components of the NCS 1001 must be compatible with the installed Cisco IOS XR image. Incompatibility may cause the NCS 1001 to malfunction.

To verify the firmware version, perform the following procedure.

Procedure

show hw-module fpd

```
RP/0/RP0/CPU0:ios#show hw-module fpd
Thu Jan 16 15:28:28.146 CEST                                                                    FPD
 Versions

=================
Location      Card type             HWver     FPD device        ATR     Status      Running
   Programd
-------------------------------------------------------------------------------------------------
0/0           NCS1001-K9             0.1       Control_BKP        B      CURRENT
    1.10
0/0           NCS1001-K9             0.1       Control_FPGA              CURRENT       1.10
    1.10
0/1           NCS1K-EDFA             0.0       FW_EDFAv1                 CURRENT       1.60
    1.60
0/2           NCS1K-PSM              0.0       FW_PSMv1                  CURRENT       1.51
    1.51
0/3           NCS1K-EDFA             0.0       FW_EDFAv1                 CURRENT       1.60
    1.60
0/RP0         NCS1K-CNTLR2          0.1       BIOS_Backup        BS     CURRENT       15.10
   15.10
0/RP0         NCS1K-CNTLR2          0.1       BIOS_Primary       S      CURRENT       15.10
   15.10
0/RP0         NCS1K-CNTLR2           0.1       Daisy_Duke_BKP     BS     CURRENT
    0.20
0/RP0         NCS1K-CNTLR2           0.1       Daisy_Duke_FPGA    S      CURRENT       0.20
    0.20
```

Displays the firmware information of various hardware components of the NCS 1001 in the Cisco IOS XR EXEC mode.

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

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

What to do next

Upgrade all the FPDs using the **upgrade hw-module location all fpd all** command in the Cisco IOS XR EXEC mode. After an 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 control card. 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.

If Firmware Upgrade Fails

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

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
Sun Mar  5 03:21:33.272 CET
MgmtEth0/RP0/CPU0/0 is up, line protocol is up
  Interface state transitions: 1
  Hardware is Management Ethernet, address is 6c9c.ed50.2aa2 (bia 6c9c.ed50.2aa2
)
  Internet address is 10.58.229.131/22
  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 2d12h
  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 16000 bits/sec, 22 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4959018 packets input, 462164262 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 3531513 broadcast packets, 1419827 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     20720 packets output, 1284846 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
```

In the above result, 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
Sun Mar  5 03:22:45.830 CET
Interface Type          Total     UP        Down      Admin Down
--------------          -----     --        ----      ----------
ALL TYPES               2         2         0         0
--------------
IFT_ETHERNET            1         1         0         0
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
Sun Mar  5 03:23:55.330 CET

               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
```

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 the *Bring-up NCS 1001* chapter.
- 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
  Sun Mar  5 03:25:26.191 CET
  interface MgmtEth0/RP0/CPU0/0
   ipv4 address 10.58.229.131 255.255.252.0
  !
  ```

  In the above 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
Sun Mar  5 03:27:57.137 CET

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

```
--------------------------------------------------------------------------------
0/3             Critical     Controller       03/02/2017 14:51:45 CET    Ots0/3/
0/2 - Output OTS Power Reading Below The Fail-Low Threshold

0/3             Minor        Controller       03/04/2017 06:32:27 CET    Optics0
/3/0/4 - Optics Low Receive Power
```

What to do next

For more information about alarms and steps to clear them, see the *Alarm Troubleshooting* chapter of the *Cisco NCS 1001 Troubleshooting Guide*.

Verify Environmental Parameters

The **show environment** command displays the environmental parameters of the NCS 1001.

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** | **fan** | **power** | **voltages** | **current** | **temperatures**] [**location** | *location*]

Displays the environmental parameters of the NCS 1001.

Example:

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

```
sysadmin-vm:0_RP0# show environment fan
Sun Mar  5  02:33:51.700 UTC
=====================================
                        Fan speed (rpm)
Location     FRU Type           FAN_0
-------------------------------------
0/FT0        NCS1K1-FAN         11640
0/FT1        NCS1K1-FAN         11640
0/FT2        NCS1K1-FAN         11400
0/FT3        NCS1K1-FAN         11640
0/PM0        NCS1K-2KW-AC2       9696
0/PM1        NCS1K-2KW-AC2       9760
```

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

```
sysadmin-vm:0_RP0# show environment temperatures location 0/RP0
Sun Mar  5  02:34:55.985 UTC
==============================================================================

Location  TEMPERATURE                 Value   Crit Major Minor Minor Major  Crit

          Sensor                    (deg C)   (Lo) (Lo)   (Lo)   (Hi)   (Hi)   (Hi)

------------------------------------------------------------------------------

0/RP0
          Thermistor 1                 40    -10     0     0    55    55    85

          Thermistor 2                 41    -10     0     0    55    55    85

          Hot Spot Temperature         40    -10     0     0    55    55    85
```

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

```
sysadmin-vm:0_RP0# show environment power
Sun Mar  5  02:36:17.380 UTC
==============================================================================

CHASSIS LEVEL POWER INFO: 0
==============================================================================

   Total output power capacity (N + 1)             :    2000W +    2000W
   Total output power required                     :     269W
   Total power input                               :     211W
   Total power output                              :      67W

Power Group 0:
==============================================================================

   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
==============================================================================

   0/PM0       2kW-AC      235.0      0.4     12.0      1.1    OK

Total of Power Group 0:         94W/  0.4A        13W/  1.1A

Power Group 1:
==============================================================================

   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
==============================================================================

   0/PM1       2kW-AC      234.5      0.5     12.0      4.5    OK

Total of Power Group 1:        117W/  0.5A        54W/  4.5A

==============================================================================

   Location     Card Type            Power       Power       Status
                                     Allocated   Used
                                     Watts       Watts
==============================================================================

   0/0          NCS1001-K9             30          -       ON
   0/1                -                68          -       RESERVED
   0/2                -                68          -       RESERVED
   0/3          NCS1K-EDFA             68          -       ON
```

```
   0/RP0        NCS1K-CNTLR2            35           -       ON
   0/FT0        NCS1K1-FAN               0           -       ON
   0/FT1        NCS1K1-FAN               0           -       ON
   0/FT2        NCS1K1-FAN               0           -       ON
   0/FT3        NCS1K1-FAN               0           -       ON
```

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

```
sysadmin-vm:0_RP0# show environment voltages location 0/RP0
Sun Mar  5  02:37:24.468 UTC
================================================================================

Location  VOLTAGE                    Value   Crit Minor Minor  Crit
          Sensor                     (mV)    (Lo) (Lo)  (Hi)   (Hi)
--------------------------------------------------------------------------------

0/RP0
          VP1P0_CPU                  1002    900   950  1050  1100
          CPU_CORE_VCC                713    400   450  1350  1400
          CPU_CORE_VNN                952    400   450  1350  1400
          VP1P1                      1077    990  1050  1160  1210
          VP1P2                      1206   1080  1140  1260  1320
          VP1P35_DDR                 1353   1220  1280  1420  1490
          VP1P35                     1346   1220  1280  1420  1490
          VP1P5                      1503   1350  1430  1580  1650
          VP1P8_CPU                  1801   1620  1710  1890  1980
          VP3P3_STBY                 3323   2970  3140  3470  3630
          VP3P3                      3346   2970  3140  3470  3630
          VP5P0                      5029   4500  4750  5250  5500
          VP12P0                    12047  10800 11400 12600 13200
          VREF                       1224   1190  1200  1240  1250
          12V Input Voltage         11208   8000 10000 14000 16000
```

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 the NCS 1001.

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

Procedure

Step 1 **show inventory**

Displays the details of the NCS 1001 when you execute this command in the Cisco IOS XR EXEC mode.

Example:

```
RP/0/RP0/CPU0:ios# show inventory
```

```
Sun Mar  5  02:42:57.359 UTC

 Name: Rack 0               Descr: Network Convergence System 1001 line system 3 slots
 PID: NCS1001-K9            VID: V00                  SN: CAT2018B033

 Name: 0/0                  Descr: Network Convergence System 1001 line system 3 slots
 PID: NCS1001-K9            VID: V00                  SN: CAT2018B033

 Name: 0/3                  Descr: Network Convergence System 1000 amplifier module
 PID: NCS1K-EDFA            VID: V01                  SN: IIF2044002L

 Name: 0/RP0-SFP-PORT       Descr: Unqualified SFP Pluggable Optics Module
 PID: UNQUALIFIED-SFP       VID:                      SN:

 Name: 0/RP0                Descr: Network Convergence System 1000 Controller 2
 PID: NCS1K-CNTLR2          VID: V01                  SN: CAT2051B0R5

 Name: 0/FT0                Descr: Network Convergence System 1001 Fan
 PID: NCS1K1-FAN            VID: V01                  SN: N/A

 Name: 0/FT1                Descr: Network Convergence System 1001 Fan
 PID: NCS1K1-FAN            VID: V01                  SN: N/A

 Name: 0/FT2                Descr: Network Convergence System 1001 Fan
 PID: NCS1K1-FAN            VID: V01                  SN: N/A

 Name: 0/FT3                Descr: Network Convergence System 1001 Fan
 PID: NCS1K1-FAN            VID: V01                  SN: N/A

 Name: 0/PM0                Descr: Network Convergence System 1000 2KW AC PSU 2
 PID: NCS1K-2KW-AC2         VID: V01                  SN: POG2049JT21

 Name: 0/PM1                Descr: Network Convergence System 1000 2KW AC PSU 2
 PID: NCS1K-2KW-AC2         VID: V01                  SN: POG2049JT01
```

Step 2 **admin**

Enters System Admin EXEC mode.

Example:

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

Step 3 **show inventory**

Displays inventory information for all the physical entities of the NCS 1001.

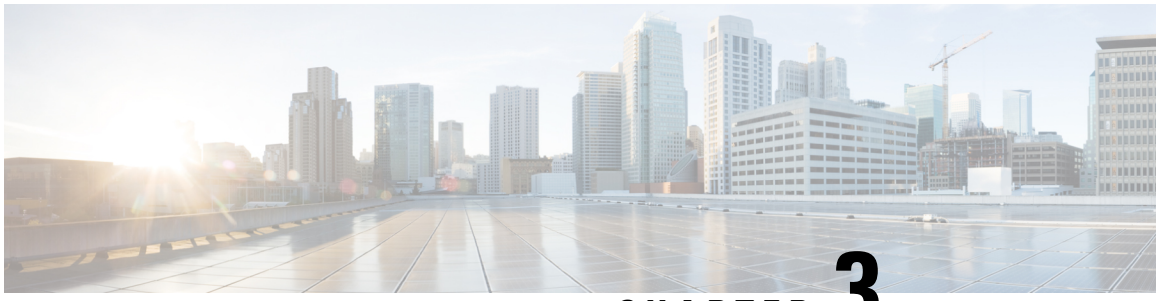
Example:

```
sysadmin-vm:0_RP0# show inventory
Sun Mar  5  02:44:30.350 UTC

 Name: Rack 0               Descr: Network Convergence System 1001 line system 3 slots
 PID: NCS1001-K9            VID: V00                  SN: CAT2018B033

 Name: 0/0                  Descr: Network Convergence System 1001 line system 3 slots
 PID: NCS1001-K9            VID: V00                  SN: CAT2018B033

 Name: 0/3                  Descr: Network Convergence System 1000 amplifier module
 PID: NCS1K-EDFA            VID: V01                  SN: IIF2044002L

 Name: 0/RP0-SFP-PORT       Descr: Unqualified SFP Pluggable Optics Module
 PID: UNQUALIFIED-SFP       VID:                      SN:
```

```
Name: 0/RP0                Descr: Network Convergence System 1000 Controller 2
PID: NCS1K-CNTLR2          VID: V01                  SN: CAT2051B0R5

Name: 0/FT0                Descr: Network Convergence System 1001 Fan
PID: NCS1K1-FAN            VID: V01                  SN: N/A

Name: 0/FT1                Descr: Network Convergence System 1001 Fan
PID: NCS1K1-FAN            VID: V01                  SN: N/A

Name: 0/FT2                Descr: Network Convergence System 1001 Fan
PID: NCS1K1-FAN            VID: V01                  SN: N/A

Name: 0/FT3                Descr: Network Convergence System 1001 Fan
PID: NCS1K1-FAN            VID: V01                  SN: N/A

Name: 0/PM0                Descr: Network Convergence System 1000 2KW AC PSU 2
PID: NCS1K-2KW-AC2         VID: V01                  SN: POG2049JT21

Name: 0/PM1                Descr: Network Convergence System 1000 2KW AC PSU 2
PID: NCS1K-2KW-AC2         VID: V01                  SN: POG2049JT01
```

In the above 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 for the chassis or node.



CHAPTER 3

Perform System Upgrade and Install Feature Packages

The system upgrade and package installation processes are executed using **install** commands on the NCS 1001. The processes involve adding and activating the iso images (*.iso*), feature packages (*.rpm*), and software maintenance upgrade files (*.smu*) on the NCS 1001. These files are accessed from a network server and then activated on the NCS 1001. If the installed package or SMU causes any issue, it can be uninstalled.

The topics covered in this chapter are:

- Upgrade the System, on page 43
- Software Upgrade and Downgrade Matrix , on page 43
- Software Compatibility Matrix, on page 44
- Upgrade the Firmware, on page 45
- Install Packages, on page 56

Upgrade the System

Upgrading the system is the process of installing a new version of the Cisco IOS XR operating system on the NCS 1001. The NCS 1001 comes pre-installed with the Cisco IOS XR image. However, you can install the new version in order to keep features up to date. The system upgrade operation is performed from the XR mode. However, during system upgrade, the operating systems that run both on the XR and the System Admin get upgraded.

System upgrade is done by installing a base package–Cisco IOS XR Core Bundle plus Manageability Package. The file name for this bundle is *ncs1001-mini-x-7.10.1.iso*. Install this ISO image using **install** commands. For more information about the install process, see Workflow for Install Process, on page 56.

Software Upgrade and Downgrade Matrix

The following table lists the upgrade and downgrade paths supported for Cisco NCS 1001.

Upgrade Path		Downgrade Path	
Source Release	**Destination Release**	**Source Release**	**Destination Release**
R7.3.1, 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, R7.3.1

Software Compatibility Matrix

The following table describes the software compatibility for all firmware.

Table 5: Software Compatibility Matrix

FPD	R6.2.1	R6.2.2	R6.3.1	R6.3.2	R6.5.1	R6.5.2	R7.0.0	R7.0.1	R7.1.1	R7.1.2	R7.2.1	R7.3.1 and R7.3.2	R7.5.1, R7.5.2, and R7.7.1	R7.8.1, R7.9.1, and 7.10.1
FW_PSMv1	1.38	1.38	1.43	1.45	1.45	1.51	1.51	1.51	1.51	1.51	1.51	1.51	1.51	1.51
FW_PSMv2	0.09	0.09	0.12	0.14	0.14	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16	0.16
FW_PSMv3														1.64 only for 7.10.1
Control_ BKP	1.07	1.09	1.09	1.09	1.10	1.10	1.10	1.10	1.10	1.10	1.10	1.10	1.10	1.10
Control_ FPGA	1.07	1.09	1.09	1.09	1.10	1.10	1.10	1.10	1.10	1.10	1.10	1.10	1.10	1.10
FW_EDFAv1	1.39	1.39	1.43	1.43	1.43	1.51	1.54	1.55	1.56	1.56	1.56	1.60	1.60 for R7.5.1 and 1.61 for R7.5.2 and R7.7.1	1.61
FW_EDFAv2	0.12	0.12	0.28	0.31	0.37	0.37	0.39	0.40	0.40	0.40	0.40	0.43	0.43	0.45
FW_OTDR_p	NA	NA	NA	NA	5.02	5.02	6.02	6.02	6.02	6.02	6.02	6.03	6.03	6.03
FW_OTDR_s	NA	NA	NA	NA	1.47	1.51	1.51	1.51	1.51	1.51	1.51	1.51	1.51	1.51
PO-PriMCU (AC)	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.0	4.0	4.0	4.0

FPD	R6.2.1	R6.2.2	R6.3.1	R6.3.2	R6.5.1	R6.5.2	R7.0.0	R7.0.1	R7.1.1	R7.1.2	R7.2.1	R7.3.1 and R7.3.2	R7.5.1, R7.5.2, and R7.7.1	R7.8.1, R7.9.1, and 7.10.1
PO-PriMCU (DC)	NA	1.10	1.10	1.10	1.10	1.10	1.10	1.14	1.14	1.14	1.14	1.14	1.14	2.01
BIOS_ Backup	13.50	13.60	13.80	14.20	14.20	14.20	14.20	14.50	14.60	14.60	15.10	15.10	15.10	15.10
BIOS_ Primary	13.50	13.60	13.80	14.20	14.20	14.20	14.20	14.50	14.60	14.60	15.10	15.10	15.10	15.10 for 7.8.1 and 7.9.1; 15.30 for 7.10.1
Daisy_ Duke_ BKP	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.20	0.20	0.20	0.20	0.20	0.20	0.20
Daisy_ Duke_ FPGA	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.20	0.20	0.20	0.20	0.20	0.20	0.20

Upgrade the Firmware

Use the following procedure to upgrade the firmware.

Attention If you are upgrading FPDs from R7.8.1 to later releases, refer to Upgrade FPDs, on page 52 for serialized upgrade.

Note The output of this procedure is related to R7.7.1. The FPDs to be installed for later releases are different. Refer to Software Compatibility Matrix, on page 44 for FPD versions.

Note The BIOS and Daisy Duke FPD upgrade from R6.3.x and R6.5.x to R7.1.1, R7.1.2, R7.3.1, R7.3.2, R7.5.1, R7.5.2, R7.7.1, R7.8.1, R7.9.1, or R7.10.1 must be executed with proper steps. We recommend that you read through the entire procedure before performing any upgrade steps.

Procedure

Perform the procedures in the following sequence.

a. Upgrade BIOS and Daisy Duke FPDs, on page 46
b. Upgrade Control FPGA and Control BKP FPDs, on page 48
c. Upgrade PSM, on page 49
d. Upgrade EDFA, on page 51

Upgrade BIOS and Daisy Duke FPDs

Attention This procedure is valid only until Release 7.7.1.

From R7.0.1 and later, the upgrade procedure also updates the secure boot keys.

Caution Ensure that secure boot keys are updated prior to other FPD upgrades. If BIOS and Daisy Duke FPGA FPDs are upgraded without updating the secure boot keys, it can lead to RMA of the device.

Note

- BIOS downgrade is not supported once BIOS FPD is upgraded to 15.10.
- The 15.10 BIOS FPD version does not have issues for software images prior to R7.2.1. If the user needs to downgrade the software image prior to R7.2.1, the BIOS FPDs always show the status as "NEED UPGRADE".

Before you begin

- For software upgrades from any release to R7.0.1 and later, disable auto-fpd upgrade using the **fpd auto-upgrade disable** command.
- Install SMUs for R6.3.2 and R6.5.2 software to upgrade the FPDs with secure boot keys and then upgrade the software to R7.0.1 and later.

Procedure

Step 1 Enter the **show hw-module fpd** command from IOS XR console.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                                FPD Versions
                                                                                ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   NEED UPGD          1.09
0/0        NCS1001-K9            0.1   Control_FPGA         NEED UPGD  1.09    1.09
0/1        NCS1K-EDFA            0.0   FW_EDFAv2            NEED UPGD  0.31    0.31
0/2        NCS1K-PSM             0.0   FW_PSMv2             NEED UPGD  0.12    0.12
0/3        NCS1K-EDFA            0.0   FW_EDFAv2            NEED UPGD  0.31    0.31
0/RP0      NCS1K-CNTLR2          0.1   BIOS_Backup      BS  NEED UPGD         13.80
0/RP0      NCS1K-CNTLR2          0.1   BIOS_Primary      S  NEED UPGD 13.80   13.80
0/RP0      NCS1K-CNTLR2          0.1   Daisy_Duke_BKP   BS  NEED UPGD          0.17
0/RP0      NCS1K-CNTLR2          0.1   Daisy_Duke_FPGA   S  NEED UPGD  0.17    0.17
```

Step 2 Enter the **upgrade hw-module location 0/RP0 fpd all** command from IOS XR console to upgrade the BIOS and Daisy Duke FPDs.

Step 3 Enter the **show hw-module fpd** command again from IOS XR console to view the status of BIOS and Daisy Duke FPDs.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                                FPD Versions
                                                                                ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   NEED UPGD          1.09
0/0        NCS1001-K9            0.1   Control_FPGA         NEED UPGD  1.09    1.09
0/1        NCS1K-EDFA            0.0   FW_EDFAv2            NEED UPGD  0.31    0.31
0/2        NCS1K-PSM             0.0   FW_PSMv2             NEED UPGD  0.12    0.12
0/3        NCS1K-EDFA            0.0   FW_EDFAv2            NEED UPGD  0.31    0.31
0/RP0      NCS1K-CNTLR2          0.1   BIOS_Backup      BS  RLOAD REQ          15.10
0/RP0      NCS1K-CNTLR2          0.1   BIOS_Primary      S  RLOAD REQ 13.80   15.10
0/RP0      NCS1K-CNTLR2          0.1   Daisy_Duke_BKP   BS  CURRENT            0.20
0/RP0      NCS1K-CNTLR2          0.1   Daisy_Duke_FPGA   S  RLOAD REQ  0.17    0.20
```

Step 4 Enter the **admin** command to change to admin console.

Step 5 Enter the **hw-module location 0/RP0 reload** command to reload NCS 1001.

The system reboots within few seconds.

Step 6 Enter the **show hw-module fpd** command from the admin console to view the status of BIOS and Daisy Duke FPDs.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                                FPD Versions
                                                                                ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   NEED UPGD          1.09
0/0        NCS1001-K9            0.1   Control_FPGA         NEED UPGD  1.09    1.09
0/1        NCS1K-EDFA            0.0   FW_EDFAv2            NEED UPGD  0.31    0.31
0/2        NCS1K-PSM             0.0   FW_PSMv2             NEED UPGD  0.12    0.12
0/3        NCS1K-EDFA            0.0   FW_EDFAv2            NEED UPGD  0.31    0.31
0/RP0      NCS1K-CNTLR2          0.1   BIOS_Backup      BS  CURRENT            15.10
0/RP0      NCS1K-CNTLR2          0.1   BIOS_Primary      S  CURRENT    15.10   15.10
```

```
0/RP0      NCS1K-CNTLR2          0.1   Daisy_Duke_BKP   BS  CURRENT           0.20
0/RP0      NCS1K-CNTLR2          0.1   Daisy_Duke_FPGA   S  CURRENT    0.20   0.20
```

What to do next

Upgrade Control FPGA and Control BKP FPDs, on page 48

Upgrade Control FPGA and Control BKP FPDs

Attention This procedure is valid only until Release 7.7.1.

Upgrade the Control FPGA and Control BKP FPDs before upgrading the FPDs of PSM and EDFA optical modules.

Caution Traffic loss might occur if the following steps are not followed.

Procedure

Step 1 Enter the **show hw-module fpd** command from admin console.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                          FPD Versions
                                                                         =================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   NEED UPGD          1.09
0/0        NCS1001-K9            0.1   Control_FPGA         NEED UPGD  1.09    1.09
```

Step 2 Enter the **upgrade hw module location 0/0 fpd Control_FPGA** command from admin console to upgrade the Control FPGA FPD.

Note Wait for Control FPGA FPD status to reach the RLOAD REQ state.

Step 3 Enter the **show hw-module fpd** command from IOS XR console to view the status of Control FPGA FPD.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                          FPD Versions
                                                                         =================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   NEED UPGD          1.09
0/0        NCS1001-K9            0.1   Control_FPGA         RLOAD REQ  1.09    1.09
```

Step 4 Enter the **upgrade hw-module location 0/0 fpd Control_BKP** command from admin console to upgrade the Control BKP FPD.

Note Wait for Control BKP FPD status to reach the CURRENT state.

Step 5 Enter the **show hw-module fpd** command from IOS XR console to view the status of Control BKP FPD.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                          FPD Versions
                                                                          ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   CURRENT            1.10
0/0        NCS1001-K9            0.1   Control_FPGA         RLOAD REQ  1.09    1.10
```

Step 6 Enter the **hw-module location 0/RP0 reload** command from admin console to reload NCS 1001.

The system reboots within few seconds.

Step 7 Enter the **show hw-module fpd** command from the admin console to view the status of Control FPGA and Control BKP FPDs.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                          FPD Versions
                                                                          ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   CURRENT            1.10
0/0        NCS1001-K9            0.1   Control_FPGA         CURRENT  1.10      1.10
```

What to do next

Upgrade PSM, on page 49

Upgrade PSM

Attention This procedure is valid only until Release 7.7.1.

Note When you upgrade the FW_PSMv1 FPD from 1.38 to 1.43 or higher version, traffic is affected for around 120 seconds.

Note When you upgrade the FW_PSMv1 FPD from 1.43 to higher version, traffic is affected.

Perform the following steps to upgrade PSM in section protection configuration.

Procedure

Step 1 Enter the **show hw-module fpd** command from IOS XR console.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                              FPD Versions
                                                                             =================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------------
0/2        NCS1K-PSM             0.0   FW_PSMv1         NEED UPGD       a.bc    x.yz
```

Step 2 Enter the **show controllers ots 0/2/0/* summary** command to check the port status.

If the output shows **Ots0_2_0_2 Protected Active**, switch the PSM state to **Ots0_2_0_1 Working Active** and **Ots0_2_0_2 Protected Standby**.

Step 3 **config**

Step 4 Enter the **no hw-module location 0/RP0/CPU0 slot 2 psm lockout-from WORKING** to move the PSM state to **Ots0_2_0_1 Working Active** without any lockout in place.

Step 5 **commit**

Step 6 Enter the **hw-module slot 2 manual-switch-to WORKING** command from IOS XR console to switch the traffic manually from the protect to the working path.

PSM switch causes traffic loss for less than 50 ms.

Step 7 Enter the **show controllers ots 0/2/0/* summary** command to check the output.

If the switch to the Working port is successful, **Ots0_2_0_1 Working** port is reported as **Active**. If the switch to the Working port is successful, check whether the far-end node is also active on the same port.

Step 8 Enter the **show controllers ots 0/2/0/* summary** command on the far-end node to verify that **Ots0_2_0_1 Working** port is reported as **Active**.

Note If the status of PSM Working port is still Standby, it indicates that the previous switch command was not successful.

Failure to switch to the Working path indicates that the Working path is alarmed, or a **lockout-from working** is intentionally set in the configuration. In both the cases, further troubleshooting of the overall Working path (near-end node to far-end node) is required to resolve outstanding problems.

When both the near-end and far-end nodes are **Active** on the Working port, proceed with the following upgrade steps.

Step 9 Enter the **upgrade hw module location 0/2 fpd FW_PSMv1** command from IOS XR console to upgrade the PSMv1 FPD.

If the FPD type is FW_PSMv2, the above command changes to **upgrade hw module location 0/1 fpd FW_PSMv2**.

If the configuration includes path protection topology, FW_ PSMv1 upgrade is traffic-affecting and can be done using the force option as follows:

Enter the **upgrade hw module location 0/2 fpd FW_PSMv1 force** command from IOS XR console to upgrade the PSMv1 FPD.

Step 10 Enter the **show hw-module fpd** command from the admin console to view the status of PSM FPD.

Example:

```
RP/0/RP0/CPU0:ios# show hw-module fpd
                                                                          FPD Versions
                                                                          ================
Location   Card type              HWver FPD device       ATR Status   Running Programd
-----------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   CURRENT            1.10
0/0        NCS1001-K9            0.1   Control_FPGA         CURRENT    1.10    1.10
0/1        NCS1K-EDFA            0.0   FW_EDFAv2            CURRENT    0.43    0.43
0/2        NCS1K-PSM             0.0   FW_PSMv2             CURRENT    0.16    0.16
0/3        NCS1K-EDFA            0.0   FW_EDFAv1            CURRENT    1.60    1.60
0/3        NCS1K-EDFA            0.0   FW_EDFAv1            CURRENT    1.60    1.60
```

Note Wait for PSM FPD status to reach the CURRENT state.

What to do next

Upgrade EDFA, on page 51

Upgrade EDFA

Attention This procedure is valid only until Release 7.7.1.

To upgrade each EDFA module present in NCS 1001, you must identify the correct location, based on the specific FPD device.

Procedure

Step 1 Enter the **upgrade hw module location 0/1 fpd FW_EDFAv1 force** command from IOS XR console to upgrade the EDFA FPD.

If the FPD type is FW_EDFAv2, the above command changes to **upgrade hw module location 0/1 fpd FW_EDFAv2 force**.

Step 2 Enter the **show hw-module fpd** command from IOS XR console to view the status of EDFA FPD.

Note Wait for EDFA FPD status to reach the CURRENT state.

Example:

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

                                                                          FPD Versions
                                                                          ================
Location   Card type             HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------------
0/0        NCS1001-K9            0.1   Control_BKP      B   CURRENT           1.10
0/0        NCS1001-K9            0.1   Control_FPGA         CURRENT    1.10    1.10
0/1        NCS1K-EDFA            0.0   FW_EDFAv2            CURRENT    0.43    0.43
0/2        NCS1K-PSM             0.0   FW_PSMv2             CURRENT    0.16    0.16
0/3        NCS1K-EDFA            0.0   FW_EDFAv1            CURRENT    1.60    1.60
0/3        NCS1K-EDFA            0.0   FW_EDFAv1            CURRENT    1.60    1.60
```

Note When you upgrade the FW_EDFAv1 FPD from 1.38 to 1.43 or higher version, traffic is affected for around 120 seconds due to restart of line amplifier. FW_EDFAv2 FPD is not affected by this issue.

Step 3 (Only for FW_EDFAv1 FPD) Enter the **admin** command to change to admin console.

Step 4 (Only for FW_EDFAv1 FPD) Enter the **hw-module location 0/slot reload** command to perform hardware reset of the EDFA module.

Step 5 (Only for FW_EDFAv1 FPD) After the reload, check the state of EDFA modules using the **show controllers ots 0/slot/0/0** and **show controllers ots 0/slot/0/0** commands.

Example:

```
RP/0/RP0/CPU0:ios# show controllers ots 0/1/0/0
Fri Jan 22 10:14:29.305 CET
 Controller State: Down
 Transport Admin State: In Service
 Port Type: Com
 Laser State: Off
 Optics Status::
```

Step 6 (Only for FW_EDFAv1 FPD) If the **Laser State** field is reported as **Off**, restart the laser using the **controller ots 0/slot/0/***port* **osri on** and **controller ots 0/slot/0/***port***osri off** commands.

Upgrade FPDs

Table 6: Feature History

Feature Name	Release	Description
FPD Upgrade Enhancement	Cisco IOS XR Release 7.8.1	FPD upgrade is made easy with a new command **upgrade hw-module location all fpd all**. It performs the end-to-end upgrade of all FPD modules with a single execution. As a result, the need to make progressive upgrades is eliminated.

From Release 7.8.1, the upgrade of the NCS 1001 FPD devices is serialized and requires no manual intervention. The command works only when the FPD devices are in **NEED UPGD** status.

You can also use the **upgrade hw-module location all fpd all force** command to force the upgrade of the FPD devices. This command upgrades all the components forcefully even if the FPDs are in the current version.

Note The **upgrade hw-module location all fpd all force** command on FW_PSMv1 from 1.43 to higher version is traffic-affecting.

The FPD devices upgrade in the following sequence:

1. **Control_BKP**

   Control_FPGA

   Note After upgrade of **Control_BKP** and **Control_FPGA** FPDs, the NCS 1001 controller cards reload automatically.

2. FPDs of NCS 1001 cards in slots 1, 2, and 3
3. **BIOS_Backup**

   BIOS_Primary

   Daisy_Duke_BKP

   Daisy_Duke_FPGA

Procedure

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

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

The following output shows the details of the FPD devices.

```
                                                                    FPD Versions
Location     Card type    HWver   FPD device           ATR    Status       Running
Programd
0/0          NCS1001-K9   0.1     Control_BKP          B      NEED UPGD    1.09

0/0          NCS1001-K9   0.1     Control_FPGA                NEED UPGD    1.09

0/1          NCS1K-EDFA   0.0     FW_EDFAv1                   NEED UPGD    1.43
1.43
0/2          NCS1K-OTDR   0.0     FW_OTDR_p                   NEED UPGD    6.02
6.02
0/2          NCS1K-OTDR   0.0     FW_OTDR_s                   NEED UPGD    1.47
1.47
0/3          NCS1K-EDFA   0.0     FW_EDFAv1                   NEED UPGD    1.43
1.43
0/RP0        NCS1K-CNTLR2 0.1     BIOS_Backup          BS     NEED UPGD    13.80

0/RP0        NCS1K-CNTLR2 0.1     BIOS_Primary         S      NEED UPGD    13.80
13.80
0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_BKP       BS     NEED UPGD    0.20
```

```
0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_FPGA       S      NEED UPGD     0.20
0.20
```

Step 2 To upgrade all the FPD devices, execute the following command:

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

Step 3 To check the status of the FPD devices, execute the following command:

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

The following output shows the status of **Control_BKP** and **Control_FPGA** as **Current** and **RLOAD REQ**.

Note The **Control_BKP** and **Control_FPGA** FPD devices reload automatically.

```
                                                                        FPD Versions
Location     Card type    HWver   FPD device            ATR    Status      Running
Programd
0/0          NCS1001-K9   0.1     Control_BKP           B      Current     1.10

0/0          NCS1001-K9   0.1     Control_FPGA                 RLOAD REQ   1.10

0/1          NCS1K-EDFA   0.0     FW_EDFAv1                    NEED UPGD   1.43
1.43
0/2          NCS1K-OTDR   0.0     FW_OTDR_p                    NEED UPGD   6.02
6.02
0/2          NCS1K-OTDR   0.0     FW_OTDR_s                    NEED UPGD   1.47
1.47
0/3          NCS1K-EDFA   0.0     FW_EDFAv1                    NEED UPGD   1.43
1.43
0/RP0        NCS1K-CNTLR2 0.1     BIOS_Backup           BS     NEED UPGD   13.80

0/RP0        NCS1K-CNTLR2 0.1     BIOS_Primary          S      NEED UPGD   13.80
13.80
0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_BKP        BS     NEED UPGD   0.20

0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_FPGA       S      NEED UPGD   0.20
0.20
```

Step 4 After the status of the **Control_BKP** and **Control_FPGA** FPD devices becomes **Current**, repeat the previous step to check the status of other FPDs.

The following output shows that all the optical cards are upgraded with the status as **Current**.

```
                                                                        FPD Versions
Location     Card type    HWver   FPD device            ATR    Status      Running
Programd
0/0          NCS1001-K9   0.1     Control_BKP           B      Current     1.10

0/0          NCS1001-K9   0.1     Control_FPGA                 Current     1.10

0/1          NCS1K-EDFA   0.0     FW_EDFAv1                    Current     1.43
1.43
0/2          NCS1K-OTDR   0.0     FW_OTDR_p                    Current     6.02
6.02
0/2          NCS1K-OTDR   0.0     FW_OTDR_s                    Current     1.47
1.47
0/3          NCS1K-EDFA   0.0     FW_EDFAv1                    Current     1.43
1.43
0/RP0        NCS1K-CNTLR2 0.1     BIOS_Backup           BS     NEED UPGD   13.80

0/RP0        NCS1K-CNTLR2 0.1     BIOS_Primary          S      NEED UPGD   13.80
13.80
0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_BKP        BS     NEED UPGD   0.20
```

```
0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_FPGA       S      NEED UPGD     0.20
0.20
```

Step 5 To see if all the FPD devices are upgraded, use the following command:

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

The following output shows the status of the BIOS and Daisy_Duke FPDs as **RLOAD REQ**.

```
                                                                          FPD Versions
Location     Card type    HWver   FPD device            ATR    Status      Running
Programd
0/0          NCS1001-K9   0.1     Control_BKP           B      Current     1.10

0/0          NCS1001-K9   0.1     Control_FPGA                 Current     1.10

0/1          NCS1K-EDFA   0.0     FW_EDFAv1                    Current     1.43
1.43
0/2          NCS1K-OTDR   0.0     FW_OTDR_p                    Current     6.02
6.02
0/2          NCS1K-OTDR   0.0     FW_OTDR_s                    Current     1.47
1.47
0/3          NCS1K-EDFA   0.0     FW_EDFAv1                    Current     1.43
1.43
0/RP0        NCS1K-CNTLR2 0.1     BIOS_Backup           BS     RLOAD REQ   15.10

0/RP0        NCS1K-CNTLR2 0.1     BIOS_Primary          S      RLOAD REQ   15.10
15.10
0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_BKP        BS     RLOAD REQ
0.20
0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_FPGA       S      RLOAD REQ   0.20
0.20
```

Step 6 To reload the BIOS and Daisy_Duke FPDs, execute the following command:

```
RP/0/RP0/CPU0:ios#hw-module location 0/RP0 reload
```

Step 7 Use the **show hw-module fpd** command to check the status of the upgraded FPD devices.

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

The following output shows the details of the upgraded FPD devices with their status highlighted as **Current**.

```
                                                                          FPD Versions
Location     Card type    HWver   FPD device            ATR    Status      Running
Programd
0/0          NCS1001-K9   0.1     Control_BKP           B      Current     1.10

0/0          NCS1001-K9   0.1     Control_FPGA                 Current     1.10

0/1          NCS1K-EDFA   0.0     FW_EDFAv1                    Current     1.43
1.43
0/2          NCS1K-OTDR   0.0     FW_OTDR_p                    Current     6.02
6.02
0/2          NCS1K-OTDR   0.0     FW_OTDR_s                    Current     1.47
1.47
0/3          NCS1K-EDFA   0.0     FW_EDFAv1                    Current     1.43
1.43
0/RP0        NCS1K-CNTLR2 0.1     BIOS_Backup           BS     Current     15.10

0/RP0        NCS1K-CNTLR2 0.1     BIOS_Primary          S      Current     15.10
15.10
0/RP0        NCS1K-CNTLR2 0.1     Daisy_Duke_BKP        BS     Current
0.20
```

```
0/RP0          NCS1K-CNTLR2 0.1      Daisy_Duke_FPGA        S       Current         0.20
0.20
```

Install Packages

Packages and software patches (SMU) can be installed on NCS 1001. Installing a package on NCS 1001 installs specific features that are part of that package. Cisco IOS XR software is divided into various software packages; this enables you to select the features to run on NCS 1001. Each package contains components that perform a specific set of NCS 1001 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	ncs1001-iosxr-px-k9-7.10.1.tar	Contains required core packages, including OS, Admin, Base, Forwarding, SNMP Agent, FPD, and Alarm Correlation and Netconf-yang, Telemetry, Extensible Markup Language (XML) Parser, HTTP server packages.
Individually-Installable Optional Packages		
Cisco IOS XR Security Package	ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm	Support for Encryption, Decryption, IP Security (IPSec), Secure Socket Layer (SSL), and Public-key infrastructure (PKI).

Workflow for Install Process

To install a package, see Install Packages, on page 59. To uninstall a package, see Uninstall Packages, on page 65. The workflow for installation and uninstallation processes are depicted in individual flowcharts in their respective subsections.

Creating Repository to Access Files for Upgrading IOS XR Software

To install packages (RPM), code upgrades, and updates in XR, you need to copy the required RPMs to a reachable repository to download and install. You can host the repository locally on the router or on a remote server that can be accessed via FTP, HTTP, or HTTPS.

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

- IP address of the server

- Port number of the server

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

- FTP: ftp://[;]/
- HTTP: http://[;]/
- HTTPS: https://[;]/
- Local: file:///

  The path to the repository must be under /harddisk:/ location, for example, the URL for HTTP server is http://172.16.0.0:3333/.

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

Create and Configure a Local Repository

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

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

The following process explains how to set up a local RPM repository on the router.

Procedure

Step 1 Create a directory locally on the router's /harddisk, for example, “new_repo”.

```
[node0_RP0_CPU0:/harddisk:]$mkdir /harddisk\:/new_repo
```

Step 2 Copy the required RPMs and ISO files (using the copy or scp command) from the server to the local directory on the router.

Step 3 Access the shell of the router using run the command and untar the RPMs.

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

Step 4 Exit from the shell.

Step 5 Configure the local repository.

```
RP/0/RP0/CPU0:ios# install repository new_repo url file:/harddisk:/new_repo
RP/0/RP0/CPU0:ios#install commit
RP/0/RP0/CPU0:ios# show running-config install repository new_repo
Mon Mar  6 16:46:45.891 IST install
 repository new_repo   url file:/harddisk:/new_repo  !
!
```

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

Create and Configure an External Repository

To create an external repository, use a server that can be reached over HTTP, HTTPS, or FTP. The following instructions are applicable to Linux distribution systems. Using an external repository provides a central common repository to be used across devices. This eliminates the need to copy files for future updates to each router individually. It also serves as a single source when new RPMs (bug fixes, packages, and updates) are made available. This is the recommended method to setup a repository.

Ensure that you have completed the following tasks:

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

Procedure

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

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

Step 2 Convert the directory to a repository by running ‘createrepo </path/to/repo-dir/>’ . This creates a directory named **repodata** with the metadata of all the RPMs.

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

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

Step 3 Configure the external repository.

```
RP/0/RP0/CPU0:ios# install repository new_repo url file:/harddisk:/new_repo
RP/0/RP0/CPU0:ios#install commit
 RP/0/RP0/CPU0:ios# show running-config install repository new_repo
Mon Mar  6 16:46:45.891 IST install
 repository new_repo   url file:/harddisk:/new_repo  ! !
```

Verify connectivity to the server and check the contents of the repository.

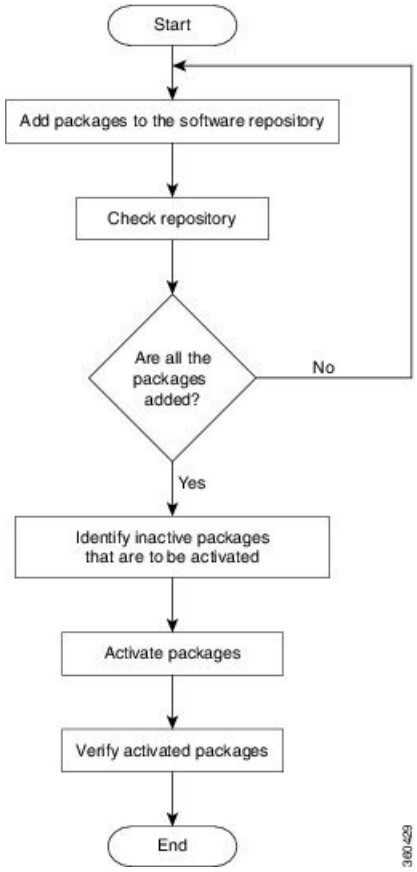
Install Packages

Complete this task to upgrade the system or install a patch. The system upgrade is done using an ISO image file, while the patch installation is done using packages and SMUs. This task is also used to install *.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 one RPM per component, without dependency on the card type.

Note To install a System Admin package or a 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.

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

Figure 1: Installing Packages Workflow



Note Disable auto-fpd upgrade before start of software upgrade.

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

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, on page 22.
- You need to create either local or external repository to copy the tar file from FTP or TFTP server. For more information, See Creating Repository to Access Files for Upgrading IOS XR Software .
- Copy the package to be installed either on the NCS 1001 hard disk or on a network server to which the NCS 1001 has access.
- When ncs1001-k9sec package is not installed, use only FTP or TFTP to copy files or during the **install add** operation.

Procedure

Step 1 Log into the Cisco software download site with your Cisco user ID and password.

Step 2 Click **Browse All** to see the product categories.

Step 3 Select the software either by searching across all product categories or by entering the complete product name or a partial string in the search box.

Example:

For example, NCS1001 software download page is available at https://software.cisco.com/download/home/286315098/type

Step 4 Download the Cisco IOS tar file either to FTP or TFTP server.

Step 5 Copy the tar file from the FTP or TFTP server either to router's harddisk or external repository.

Example:

```
RP/0/RP0/CPU0:ios#copy tftp:ncs1001-iosxr-px-k9-7.10.1.tar harddisk
RP/0/RP0/CPU0:ios#copy ftp:ncs1001-iosxr-px-k9-7.10.1.tar harddisk
```

Note This operation may take time, depending on the size of the files being added. For details about configuring the repository, see Creating Repository to Access Files for Upgrading IOS XR Software

Step 6 Execute **install add** command to extract and install the packages from the tar file.

- **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: ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
```

or

```
RP/0/RP0/CPU0:ios#install add source tftp://10.58.230.32/mystique/iso/7.10.1/
ncs1001-mini-x-7.10.1.iso ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm


Thu Jul 25 14:26:43.661 CEST
Jul 25 14:26:47 Install operation 13 started by root:
 install add source tftp://10.58.230.32/mystique/iso/7.10.1
ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm ncs1001-mini-x-7.10.1.iso
Jul 25 14:26:49 Install operation will continue in the background
```

Note
- A space must be provided between the *package_path* and *filename*.
- Install operation over IPv6 is not supported.

Step 7 Execute **show install repository** to display packages that are added to the repository.

Example:

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

Step 8 (Optional) Execute the **show install request** command to display the operation ID of the add operation and its status. The operation ID can be used later to execute the activate command.

Example:

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


User root, Op Id 13
install add
ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
ncs1001-mini-x-7.10.1.iso

The install add operation 13 is 30% complete

........
........
Jul 25 14:46:36 Install operation 13 finished successfully
```

Step 9 Execute **show install log** *operation ID* to display packages that are added to the repository.

Example:

```
RP/0/RP0/CPU0:ios#show install log 13


Thu Jul 25 14:48:53.270 CEST
Jul 25 14:26:47 Install operation 13 started by root:
 install add source tftp://10.58.230.32/mystique/iso/7.10.1
ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm ncs1001-mini-x-7.10.1.iso
Jul 25 14:26:48 Action 1: install add action started
Jul 25 14:26:49 Install operation will continue in the background
Jul 25 14:46:34 Packages added:
Jul 25 14:46:34     ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 25 14:46:34     ncs1001-mini-x-7.10.1.iso
Jul 25 14:46:34 Action 1: install add action completed successfully
Jul 25 14:46:36 Install operation 13 finished successfully
Jul 25 14:46:36 Ending operation 13
```

Packages are displayed only after the `install add` operation is complete.

Step 10 Execute **show install inactive** to display inactive packages that are present in the repository. Only inactive packages can be activated.

Example:

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


Thu Jul 25 14:51:45.852 CEST
2 inactive package(s) found:
    ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
    ncs1001-mini-x-7.10.1.iso
```

Step 11 Execute one of the following commands for the pre-activation checks and load individual components of the installable files onto the router setup.

- **install prepare**
- **install prepare id**

```
RP/0/RP0/CPU0:ios#install prepare ncs1001-mini-x-7.10.1.iso
ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
or
RP/0/RP0/CPU0:ios#install prepare id 5
Fri Jul 26 11:36:41.163 CEST
Jul 26 11:36:45 Install operation 5 started by root:
install prepare pkg ncs1001-mini-x-7.10.1.iso pkg ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 26 11:36:46 Package list:
Jul 26 11:36:46 ncs1001-mini-x-7.10.1.iso
Jul 26 11:36:46 ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 26 11:36:53 Install operation will continue in the background
Could not start this install operation. Install operation 5 is still in progress
RP/0/RP0/CPU0:152#Jul 26 11:48:57 Install operation 5 finished successfully
```

The prepare process takes place. This operation is performed in asynchronous mode. The **install prepare** command runs in the background, and the EXEC prompt is returned.**Install prepare** is the first step of the activation process. If you use the operation ID, all packages that were added in the specified operation are prepared together. For example, if 5 packages are added in operation 5, by executing the **install prepare id 5** command, all 5 packages are prepared together. You do not have to prepare the packages individually.

Step 12 Execute one of the following commands for the package activation. **install activate** *package_name*

- **Install activate** *package_name*
- **Install activate id** *operation_id*

Example:

```
RP/0/RP0/CPU0:ios#install activate ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
ncs1001-mini-x-7.10.1.iso

Thu Jul 25 14:53:27.564 CEST

Jul 25 14:53:30 Install operation 14 started by root:
  install activate pkg ncs1001-k9sec-1.0.0.0-r7101 ncs1001-mini-x-7.10.1
Jul 25 14:53:30 Package list:
Jul 25 14:53:30     ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 25 14:53:31     ncs1001-mini-x-7.10.1.iso

This install operation will reload the system, continue?
 [yes/no]:[yes]   yes

Install operation will continue in the background
```

```
RP/0/RP0/CPU0:ios#show install log 14

Thu Jul 25 15:11:49.780 CEST
Jul 25 14:53:30 Install operation 14 started by root:
  install activate pkg ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm ncs1001-mini-x-7.10.1.iso
Jul 25 14:53:30 Package list:
Jul 25 14:53:30     ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 25 14:53:31     ncs1001-mini-x-7.10.1.iso
Jul 25 14:53:37 Action 1: install prepare action started
Jul 25 14:55:17 The prepared software is set to be activated with reload upgrade
Jul 25 14:55:18 This install operation will reload the system, continue?
 [yes/no]:[yes] yes
Jul 25 14:55:18 Install operation will continue in the background
Jul 25 14:55:18 Start preparing new VM for reload upgrade
Jul 25 15:06:17 All the above nodes completed System Upgrade prepare.
Jul 25 15:06:18 Action 1: install prepare action completed successfully
Jul 25 15:06:19 Action 2: install activate action started
Jul 25 15:06:19 The software will be activated with reload upgrade
Jul 25 15:06:22 Following nodes are available for System Upgrade activate:
Jul 25 15:06:22  0/RP0
Jul 25 15:11:09 Action 2: install activate action completed successfully
Jul 25 15:11:10 Action 2: install activate action completed successfully
Jul 25 15:11:20 Install operation 14 finished successfully
Jul 25 15:11:21 Ending operation 14
```

The package configurations are made active on the NCS 1001. As a result, new features and software fixes take effect. This operation is performed in asynchronous mode. The **install activate** command runs in the background, and the EXEC prompt is returned.

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 ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm

install activate ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm force
```

or

Using the install update command:

```
install update source repository ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
```

If you use the operation ID, all packages that were added in the specified operation are activated together. For example, if 5 packages are added in operation 2, all the 5 packages are activated together. You do not have to activate the packages individually.

Step 13 Execute **show install active** to display active packages. You can verify from the result that the same image and package versions are active on all RPs and LCs

Example:

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


Thu Jul 25 17:04:47.600 CEST
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv48
  Active Packages: 2
        ncs1001-xr-7.10.1 version=7.10.1 [Boot image]
        ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
```

Displays packages that are active.

Step 14 Execute **install commit** to commit the Host, XR, and System Admin active software.

Example:

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


Thu Jul 25 17:05:27.364 CEST
Jul 25 17:05:30 Install operation 15 started by root:
  install commit system
Jul 25 17:05:31 Install operation will continue in the background

Jul 25 17:05:55 Install operation 15 finished successfully
```

Note
- If you perform a manual or automatic system reload without completing the transaction with the install commit command during system upgrade, 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'.
- On Multi-SDR mode, you can use the **install commit sdr** to commit just the sdr from where the CLI is being triggered.

Step 15 Execute **show install commit** command to display the committed packages.

Example:

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


Thu Jul 25 17:07:54.255 CEST
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv48
  Committed Packages: 2
        ncs1001-xr-7.10.1 version=7.10.1[Boot image]
        ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
```

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 1001 if any FPD status is in RLOAD REQ state. If CTRL FPGA is in RLOAD REQ state, use the **hw-module location 0/0 reload** command. If Daisy Duke or BIOS is 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 the NCS 1001. See Uninstall Packages, on page 65.

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

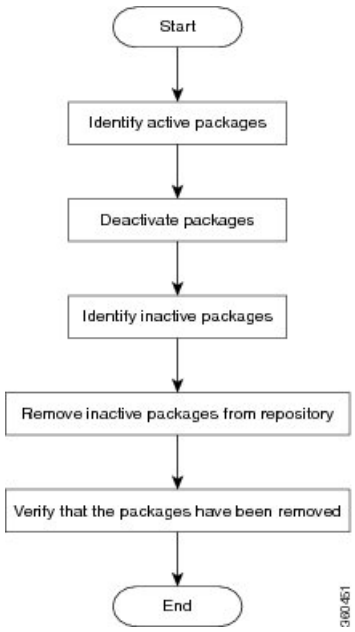
Uninstall Packages

Complete this task to uninstall a package. All the NCS 1001 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 vice versa.

Note Installed ISO images cannot be uninstalled. Also, kernel SMUs that install 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 workflow for uninstalling a package is shown in this flowchart.

Figure 2: Uninstalling Packages Workflow



Procedure

Step 1 **show install active**

Example:

```
RP/0/RP0/CPU0:ios#show install active
Thu Jul 25 16:23:36.579 CEST
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv48
  Active Packages: 2
        ncs1001-xr-7.10.1 version=7.10.1 [Boot image]
        ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
```

Displays active packages. Only active packages can be deactivated.

Step 2 **show install repository**

Example:

```
show install repository


Thu Jul 25 16:52:03.432 CEST
2 package(s) in XR repository:
    ncs1001-mini-x-7.10.1.iso
    ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
```

Step 3 Execute one of these commands:

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

Example:

```
RP/0/RP0/CPU0:ios#install deactivate ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
```

or

```
RP/0/RP0/CPU0:ios#install deactivate id 48
```

All features and software patches associated with the package are deactivated. You can specify multiple package names and deactivate them simultaneously.

If you use the operation ID, all packages that were added in the specified operation are deactivated together. You do not have to deactivate the packages individually.

```
Thu Jul 25 16:23:52.789 CEST
Jul 25 16:23:56 Install operation 48 started by root:
  install deactivate pkg ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 25 16:23:56 Package list:
Jul 25 16:23:56     ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 25 16:24:11 Install operation will continue in the background
Jul 25 16:26:38 Install operation 48 finished successfully
```

Step 4 **show install inactive**

Example:

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


Thu Jul 25 16:27:54.005 CEST
1 inactive package(s) found:
    ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
```

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

Step 5 **install remove** *package_name*

Example:

```
RP/0/RP0/CPU0:ios#install remove ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm


Thu Jul 25 16:30:11.870 CEST
Jul 25 16:30:14 Install operation 49 started by root:
  install remove ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 25 16:30:14 Package list:
Jul 25 16:30:15     ncs1001-k9sec-1.0.0.0-r7101.x86_64.rpm
Jul 25 16:30:16 Install operation will continue in the background
Jul 25 16:30:21 Install operation 49 finished successfully
```

The inactive packages are removed from the repository.

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

Step 6 **show install repository**

Example:

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


Thu Jul 25 16:52:03.432 CEST
.. package(s) in XR repository:
    ncs1001-mini-x-7.10.1.iso
```

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

What to do next

Install required packages. See Install Packages, on page 59.