Perform System Upgrade and Install Feature Packages

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

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

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

The topics covered in this chapter are:

Upgrade the System

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

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

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

Note

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

View Supported Software Upgrade or Downgrade Versions

Table 1: Feature History Table

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

Table 2: Feature History

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

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

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

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

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

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

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

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

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

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

View All Supported Software Upgrade from Running Version

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

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

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

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

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

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

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

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

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

View Supported Releases from Current Version to an ISO Version

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

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

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

View Supported Releases from Running Version to an ISO Version

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

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

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

Pre and Post-Upgrade Installation Health Checks

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

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

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

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

Upgrade precheck:

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

Upgrade post check:

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

Installation Profile Creation

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

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

config

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

end

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

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

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

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

Use the following configuration to report health check:

config

grpc local-connection

Netconf-yang agent

commit

The following is a sample to display health check states:

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

 Internal Structure INFO

 Current state: Disabled

 Reason: Success

 Netconf Config State: Enabled

 Grpc Config State: Enabled

 Nosi state: Initialized
```

```
 Appmgr conn state: Connected

 Nosi lib state: Not ready

 Nosi client: Valid client
```

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

config

healthcheck cadence *healthcheck_cadence_interval*

commit

The following is a sample to display health check report:

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

Healthcheck report
Last Update Time:
METRICS REPORT

cpu
  State: Normal

free-memory
  State: Normal

filesystem
  State: Normal

shared-memory
  State: Normal

platform
  State: Normal

redundancy
  State: Normal

fpd
  State: Normal

asic-errors
  State: Normal

fabric-stats
  State: Normal

process-status
  State: Normal

process-resource
  State: Normal

communication-timeout
  State: Normal

config-inconsistency
  State: Normal

system-clock
  State: Normal
```

```
pci-monitoring
  State: Normal

hw-monitoring
  State: Normal

wd-monitoring
  State: Normal

lc-monitoring
  State: Normal
```

Software Upgrade and Downgrade Matrix

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

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

Install Packages

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

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

Standard packages are:

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

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

Workflow for Install Process

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

Install Packages

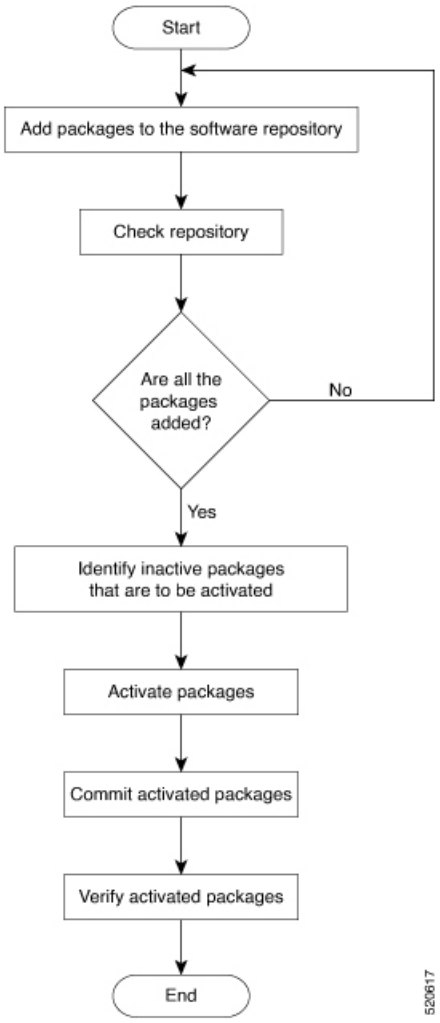
Complete this task to upgrade the system or install a patch. You can perform the system upgrade using an ISO image file and the patch installation using packages and SMUs. This task also enables you to install *.tar* files. The *.tar* file contains multiple packages and SMUs that are merged into a single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

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

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

The following flowchart displays workflow for installing a package:

Figure 1: Installing Packages Workflow



Before you begin

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

Procedure

Step 1 Execute one of these commands:

- **install add source** *<tftp transfer protocol>/package_path/ filename1 filename2 ...*

- **install add source** *<ftp or sftp transfer protocol>//user@server:/package_path/ filename1 filename2 ...*

Example:

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


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

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

Note install operation over IPv6 is not supported.

Step 2 **show install request**

Example:

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

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

Step 3 **show install repository**

Example:

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


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

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

Step 4 **show install inactive**

Example:

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


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

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

Step 5 **install activate** *package_name*

Example:

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


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


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

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

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

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

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

install activate ncs1004-xr-7.2.1 force
```

Or

Using the **install update** command:

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

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

Step 6 **show install active**

Example:

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


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

Displays packages that are active.

Step 7 **install commit system**

Example:

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

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

Commits the newly active software.

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

Installing Packages: Related Commands

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

What to do next

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

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

(Optional) Install Prepared Packages

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

The advantages of preparing before activation are:

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

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

Procedure

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

For details, see Install Packages.

Step 2 **show install repository**

Example:

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

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

Step 3 Execute one of these commands:

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

Example:

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

Or

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

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

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

Step 4 **show install prepare**

Example:

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

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

Step 5 **install activate** *package_name*

Example:

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

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

Step 6 **show install active**

Displays packages that are active.

Step 7 **install commit system**

Example:

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

Commits the recently activated software.

Installing Packages: Related Commands

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

What to do next

- After performing a system upgrade, upgrade FPD by using the **upgrade hw-module location all fpd all** command from the Cisco IOS XR mode. The progress of FPD upgrade process can be monitored using the **show hw-module fpd** command.

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

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

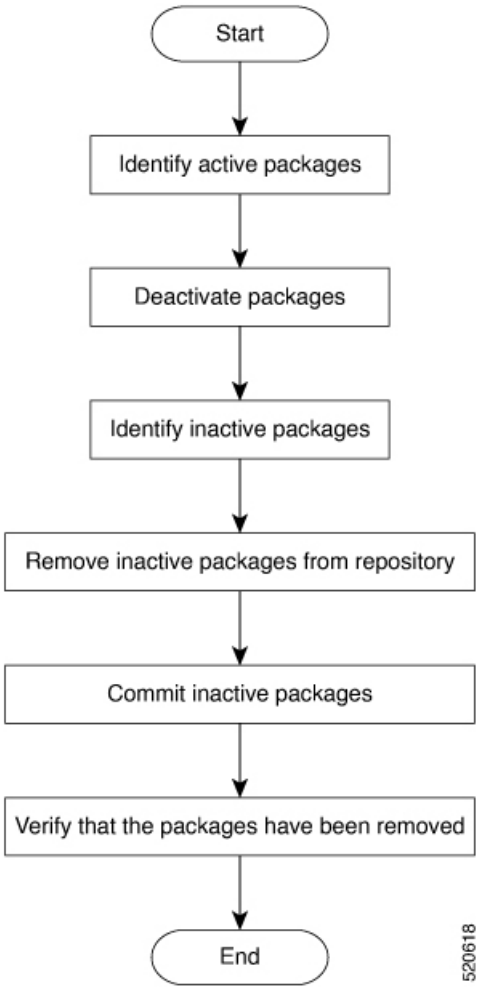
Uninstall Packages

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

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

The following flowchart shows a workflow for uninstalling a package:

Figure 2: Uninstalling Packages Workflow



Procedure

Step 1 **show install active**

Example:

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

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

Displays active packages. You can deactivate only active packages.

Step 2 Execute one of these commands:

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

Example:

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

Or

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

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

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

Step 3 **show install inactive**

Example:

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

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

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

Step 4 **install remove** *package_name*

Example:

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

The inactive packages are removed from the repository.

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

Step 5 **install commit system**

Example:

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

Commits the newly active software.

Step 6 **show install repository**

Example:

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

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

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

What to do next

Install required packages. See Install Packages.

FPD Automatic Upgrade

Table 3: Feature History

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

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

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

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

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

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

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

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

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

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

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

Example

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

0/SC0      NCS1004           2.0   BP_FPGA                    CURRENT     1.25      1.25

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

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

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

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

Example

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

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

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

To upgrade POWMAN_CFG manually refer to the example given below.

Example

FPD upgrade initiated:

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

FPD moved to RELOAD REQ state:

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

RP reload complete:

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

Firmware Upgrade

Table 4: Feature History

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

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

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

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

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

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

Procedure

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

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

Example:

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

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

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

Example:

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

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

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

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

Example:

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

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

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

Example:

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

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

Example:

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

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

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

Example:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

0/SC0     NCS1004           2.0   BP_FPGA                   CURRENT     1.25      1.25

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

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

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

Example:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

0/SC0      NCS1004           2.0   BP_FPGA                    CURRENT     1.25      1.25

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

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

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