Cisco NCS 1010 setup and upgrade workflow

Use this reference to review how Cisco NCS 1010 setup and software upgrade topics are organized.

NCS 1010 comes preinstalled with IOS XR software. You can upgrade NCS 1010 by installing a new version of the software. We recommend that you keep the software up-to-date to ensure that NCS 1010 works with the latest features and bug fixes.

- During an upgrade:
  - The newer software replaces the currently active software on NCS 1010.
  - Packages (RPMs) that have the same name and version in the current and target release versions are not removed or reinstalled.

Software and firmware compatibility matrix

These tables provide the compatibility of FPGA firmware versions for each hardware type and supported software release.

The following information supports software and firmware compatibility matrix:

- Use this reference to review the related information.

Table 1: FPGA firmware compatibility

Hardware Type	FPGA	R7.7.1	R7.9.1	R7.10.1	R7.11.1	R7.11.2	R24.2.1	R24.3.1	R25.1.1	R25.3.1	R25.4.1	R26.1.1	R26.2.1
NCS1K-OLT-R-C	OLT	1	1.12	1.16	3	3	3.14	3.16	3.32	3.4	3.44	3.44	3.48
	Raman-1	1	1.04	1.04	3	3	3.14	3.16	3.32	3.32	3.42	3.42	3.48
NCS1K-OLT-C	OLT	1	1.12	1.16	3	3	3.14	3.16	3.32	3.4	3.44	3.44	3.48
NCS1K-ILA-2R-C	ILA	1	1.12	1.16	3.02	3.02	3.16	3.16	3.32	3.4	3.44	3.44	3.48
	Raman-1	1	1.04	1.04	3	3	3.16	3.16	3.32	3.32	3.42	3.42	3.48
	Raman-2	1	1.04	1.04	3	3	3.16	3.16	3.32	3.32	3.42	3.42	3.48
NCS1K-ILA-R-C	ILA	1	1.12	1.16	3.02	3.02	3.16	3.16	3.32	3.4	3.44	3.44	3.48
	Raman-1	1	1.04	1.04	3	3	3.16	3.16	3.32	3.32	3.42	3.42	3.48
NCS1K-ILA-C	ILA	1	1.12	1.16	3.02	3.02	3.14	3.16	3.32	3.4	3.44	3.44	3.48
NCS1K-OLT-L	OLT	NA	1.02	1.04	3	3	NA	NA	NA	NA	NA	NA	3.48
NCS1K-ILA-L	ILA	NA	1	1.02	3	3	NA	NA	NA	NA	NA	NA	3.48
NCS1010-SA	HIU-ADMConfig	2.1	2.1	2.1	2.1	2.1	2.1	2.1	2.1	2.1	2.1	2.1	2.1
	IoFpga	1.12	1.12	1.12	1.16	1.16	1.18	1.19	1.19	1.27	1.27	1.27	1.27
	IoFpgaGolden	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01
	SsdIntelS4510	11.32	11.32	11.32	11.32	11.32	11.51	11.51	11.51	11.51	11.51	11.51	11.51
	SsdMicron5300	11.32	11.32	0.01	—	—	—	—	—	—	—	—	—

Table 2: FPGA firmware compatibility for NCS1010-AC-PSU power supply unit

FPGA	R7.7.1	R7.9.1	R7.10.1	R7.11.1	R7.11.2	R24.2.1	R24.3.1	R25.1.1	R25.3.1	R25.4.1	R26.1.1	R26.2.1
AP-PriMCU	1.03	1.03	1.03	1.03	1.03	1.03	1.03	1.03	1.03	1.03	1.03	2.03
AP-SecMCU	2.01	2.01	2.01	2.01	2.01	2.01	2.01	2.01	2.01	2.01	2.01	2.03

Table 3: FPGA firmware compatibility for NCS1010-CNTLR-K9 controller card

FPGA	R7.7.1	R7.9.1	R7.10.1	R7.11.1	R7.11.2	R24.2.1	R24.3.1	R25.1.1	R25.3.1	R26.1.1	R26.2.1
BIOS	4.1	4.2	4.2	4.6	4.6	4.8	4.8	5	5	6.1	6.1
BIOS-Golden	4.1	4.1	4.1	4.1	4.1	4.1	4.1	4.1	4.1	4.1	4.60
CPU_FPGA	1.02	1.11	1.11	1.11	1.11	1.11	1.13	1.13	1.13	1.13	1.13

CpuFpgaGolden	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01	1.01
ADMConfig	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4	3.4
SsdIntelS4510	11.32	11.32	11.32	11.32	11.32	11.51	11.51	11.51	11.51	11.51	11.51
TamFw	6.13	6.13	6.13	6.13	6.13	6.13	6.13	6.13	6.13	6.13	6.13
TamFwGolden	6.11	6.11	6.11	6.11	6.11	6.11	6.11	6.11	6.11	6.11	6.11

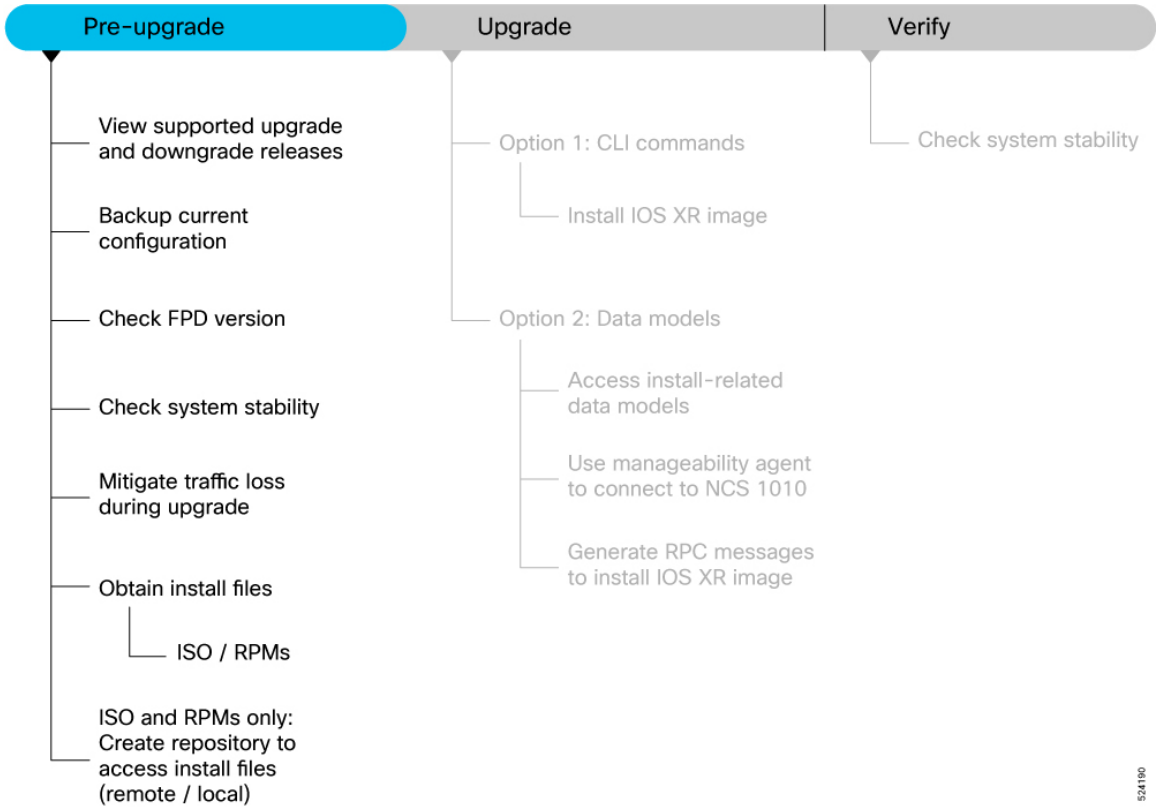
Software upgrade plan

Before you upgrade the software version, prepare NCS 1010 to ensure that the upgrade process is seamless.

Details

Pre-upgrade workflow image for NCS 1010

Figure 1: NCS 1010 Pre-upgrade workflow



Supported upgrade and downgrade releases

Use this reference to review view supported upgrade and downgrade releases.

This section provides the supported upgrade and downgrade paths for NCS 1010. Consider the following guidelines when performing an upgrade or downgrade:

Note Downgrading from software release 7.11.1 or later to any earlier version is traffic-affecting and may result in a CMA process traceback.

- When downgrading the software image from release 24.4.x to an earlier version, we recommend to manually downgrade the line card firmware as well to prevent any impact on various functionalities.
- It is recommended to perform the upgrade with FPD auto-upgrade enabled to ensure the FPD versions are up to date and to prevent potential upgrade-related issues.

- The following table lists the upgrade and downgrade paths supported for Cisco NCS 1010.

Source Release	Destination Release	Bridge SMU	Source Release	Destination Release	Target SMU
2531	2541	NA	2541	2531	NA
2511	2541	CSCwn69606	2541	2511	NA
2431	2541	CSCwm77418	2541	2431	CSCwm77418
7112	2541	CSCwm77418,CSCwk75706	2541	7112	CSCwm77418
2541	2611	NA	2611	2541	NA
2531	2611	NA	2611	2531	NA
2511	2611	CSCwn69606	2611	2511	NA
2431	2611	CSCwm77418	2611	2431	CSCwm77418
7112	2611	CSCwm77418, CSCwk75706	2611	7112	CSCwm77418

Back up the current configuration

Use this task to backup current configuration.

The ability to recover from a disaster is an essential part of any system maintenance plan. We recommend you backup the configurations in a secure remote location and verify that the transfer is a success, both before and after upgrade.

Before you begin

Follow these steps to backup current configuration.

Procedure

Step 1 Create a backup of the running configuration to one of the following locations based on your requirement:

Example:

```
RP/0/RP0/CPU0:ios#copy running-config harddisk:/running_config-<mmddyyyy>
Destination filename [running_config-<mmddyyyy>]?
Building configuration...
[OK]
Verifying checksum...  OK (0xDCF1)
```

```
RP/0/RP0/CPU0:ios#scp harddisk:/ running_config-<mmddyyyy>
user:password@<ip-address>:<location>
```

- Copy the configuration to the `harddisk:` location on NCS 1010.
- Copy the configuration to a remote server. Ensure NCS 1010 has root access to the server.

Step 2 Verify that the configuration is backed up.

Field programmable devices

A Field Programmable Device (FPD) refers to any programmable hardware device on a chassis, which includes a Field Programmable Gate Array (FPGA). NCS 1010 uses several FPDs that are necessary for chassis, route processor, line cards, and power modules to function properly. Before upgrading the software, check whether the latest FPDs are available on NCS 1010.

Details

Table 4: Feature History

Feature Name	Release Information	Feature Description
FPD Upgrade for Passive Modules	Cisco IOS XR Release 7.10.1	You can now perform FPD upgrade of the breakout modules and multiplexer/demultiplexer modules. It is essential to upgrade the passive modules to ensure the proper functioning of the modules. You can upgrade the FPD on all passive modules simultaneously or selectively upgrade the required modules.

Note FPD auto-upgrade is enabled by default on NCS 1010.

From Release 7.10.1, you can perform FPD upgrade for the breakout and multiplexer/demultiplexer modules. For the breakout modules, you can perform the FPD upgrade in both direct and indirect connections. You can upgrade all the passive modules at once or selectively upgrade the necessary modules as needed.

Note If the FPD in a given SSD is not supported by the current IOS XR software release, the status is displayed as *NOT READY* . The status will change once FPD support for these SSDs is enabled in future releases.

Table 5: NCS 1010 FPDs

Location	FPDs
RP	• ADMConfig • CpuFpga • CpuFpgaGolden • BIOS • BIOS-Golden • SsdIntelS4510 • SsdMicron5300 • SsdSmartModular • TamFw/ TamFwGolden
PM0 and PM1	• AP-PrimMCU • AP-SecMCU
LC	• ILA • OLT • Raman-1 • Raman-2
Rack	• IoFpga • IoFpgaGolden • EITU-ADMConfig • SsdIntelS4510 • SsdMicron5300 • SsdSmartModular

Location	FPDs
Breakout module	• BRK-8 • BRK-24
Multiplexer and demultiplexer modules	• MD-32-ACC • MD-32-NEO

Golden FPDs serve as backup FPDs for the primary FPDs. For example, **BIOS-Golden** is the backup Golden FPD for the **BIOS** primary FPD. If a primary FPD is corrupted, NCS 1010 boots with the corresponding Golden FPD. The Golden FPDs cannot be upgraded.

Check FPD Version

There are multiple types of FPDs for each type of module. The **show hw-module fpd** command provides information about each FPD.

```
RP/0/RP0/CPU0:ios#show hw-module fpd
Fri Feb 17 11:43:28.878 UTC

Auto-upgrade:Enabled
Attribute codes: B golden, P protect, S secure, A Anti Theft aware
                                                                                FPD Versions
                                                                               ==============
Location   Card type             HWver FPD device       ATR Status   Running Programd
Reload Loc
-----------------------------------------------------------------------------------------------
0/RP0/CPU0 NCS1010-CTLR-B-K9     1.0   ADMConfig            CURRENT    2.30    2.30
NOT REQ
0/RP0/CPU0 NCS1010-CTLR-B-K9     1.0   BIOS             S   CURRENT    4.40    4.40
  0/RP0
0/RP0/CPU0 NCS1010-CTLR-B-K9     1.0   BIOS-Golden      BS  CURRENT            4.40
  0/RP0
0/RP0/CPU0 NCS1010-CTLR-B-K9     1.0   CpuFpga          S   CURRENT    1.11    1.11
  0/RP0
0/RP0/CPU0 NCS1010-CTLR-B-K9     1.0   CpuFpgaGolden    BS  CURRENT            1.01
  0/RP0
0/RP0/CPU0 NCS1010-CTLR-B-K9     1.0   SsdIntelS4510    S   CURRENT   11.32   11.32
  0/RP0
0/RP0/CPU0 NCS1010-CTLR-B-K9     1.0   TamFw            S   CURRENT    6.13    6.13
  0/RP0
0/RP0/CPU0 NCS1010-CTLR-B-K9     1.0   TamFwGolden      BS  CURRENT            6.11
  0/RP0
0/PM0      NCS1010-AC-PSU        0.0   AP-PriMCU            CURRENT    1.03    1.03
NOT REQ
0/PM0      NCS1010-AC-PSU        0.0   AP-SecMCU            CURRENT    2.01    2.01
NOT REQ
0/PM1      NCS1010-AC-PSU        0.0   AP-PriMCU            CURRENT    1.03    1.03
NOT REQ
0/PM1      NCS1010-AC-PSU        0.0   AP-SecMCU            NEED UPGD  1.06    1.06
NOT REQ
0/0/NXR0   NCS1K-E-OLT-R-C       1.0   OLT              S   CURRENT    1.16    1.16
NOT REQ
0/0/NXR0   NCS1K-E-OLT-R-C       1.0   Raman-1          S   CURRENT    1.04    1.04
NOT REQ
0/Rack     NCS1010-SA            0.1   EITU-ADMConfig       CURRENT    1.04    1.04
NOT REQ
0/Rack     NCS1010-SA            0.1   IoFpga           S   CURRENT            1.12
NOT REQ
```

```
0/Rack      NCS1010-SA            0.1   IoFpgaGolden      BS  NEED UPGD  1.12     0.08
NOT REQ
0/Rack      NCS1010-SA            0.1   SsdIntelS4510     S   CURRENT    11.32    11.32
 0/Rack
0/1         NCS1K-MD-32E-C        0.1   MD-32-NEO         S   CURRENT    2.02     2.02
NOT REQ
0/2         NCS1K-MD-32O-C        10.2  MD-32-ACC         S   CURRENT    2.18     2.18
NOT REQ
0/3/0       NCS1K-BRK-8           1.0   BRK-8             S   CURRENT    2.08     2.08
NOT REQ
0/3/3       NCS1K-BRK-24          1.0   BRK-24            S   CURRENT    2.08     2.08
NOT REQ
```

If the status of any FPD is **NEED UPGD**, then the upgrade is required for that FPD. In this example, `IoFpgaGolden` FPD devices need an upgrade. You must ensure that FPDs are upgraded *before* upgrading NCS 1010.

The following table lists the NCS 1010 FPDs that are distributed across route processor (RP), power modules (PM), line cards (LC), and Rack.

The following table describes the significant fields in the output of the **show hw-module fpd** command.

Table 6: Description of Fields in show hw-module fpd Command

Field	Description
Location	Location of the FPD.
Card type	PID of the modules such as chassis, card, CPU, and PSU.
HWver	Hardware version where the FPD resides.
FPD device	Name of the FPD.
ATR	Attribute codes. The possible values are: • B - Golden Image • S - Secure Image • P - Protect Image The attribute code of the primary FPDs is S and the Golden FPDs is BS.
Status	Status of the FPD. See Table 7: Description of FPD Status Values in show hw-module fpd Command, on page 9.
Running	FPD image version that has been activated and currently running in the FPD device.
Programd	FPD image version that has been programmed into the FPD device, but might not be activated.
Reload Loc	Indicates whether reload of the location is required or not.

The following table describes the possible values of the Status field in the output of the **show hw-module fpd** command.

Table 7: Description of FPD Status Values in show hw-module fpd Command

FPD Status	Description
NOT READY	The driver that owns the FPD device has not initialized the FPD client to handle this device.
CURRENT	FPD version is up to date and upgrade is not required.
NEED UPGD	Upgrade is required for this FPD. Check the output of the **show fpd package** command to determine the recommended FPD version.
UPGD PREP	FPD is preparing for upgrade.
IN QUEUE	Upgrade of this FPD is in queue.
UPGD SKIP	FPD upgrade is not required. For example, • FPD version is up to date and compatible. • FPD image is protected.
UPGRADING	FPD upgrade started and the driver did not report the upgrade progress information yet.
%UPGD	Percentage of FPD upgrade completion.
RLOAD REQ	FPD upgrade is successfully completed and the FPD must be reloaded for the new version to take effect.
UPGD FAIL	FPD upgrade has failed. Check the syslog for failure reason. It could be a timeout or a failure that is reported by the driver.
UPGD DONE	FPD upgrade is successfully completed.

The **show fpd package** command is used to determine the FPDs that are supported with the current software release and the minimum hardware requirements for each FPD.

The following table describes the fields in the output of the **show fpd package** command.

Table 8: Description of Fields in show fpd package Command

Field	Description
Card Type	PID of the modules such as chassis, card, CPU, and PSU.
FPD Description	Description of the FPD.
Req Reload	Determines whether reload is required to activate the FPD image.

Field	Description
SW Ver	Recommended FPD software version for the associated module running the current Cisco IOS XR Software.
Min Req SW Ver	Minimum required FPD software version to operate the module.
Min Req Board Ver	Minimum required hardware version for the associated FPD. A minimum hardware requirement of version 0.0 indicates that all the hardware can support this FPD version.

Upgrade FPDs automatically

Use this task to upgrade FPDs automatically.

The automatic FPD upgrade upgrades the FPD version of all the modules to the latest version. When automatic FPD upgrade is enabled, all the FPDs (except the Golden FPDs) that are in NEED UPGD status are upgraded to CURRENT status during the software upgrade.

In NCS 1010, automatic FPD upgrade is enabled by default.

Before you begin

Follow these steps to upgrade FPDs automatically.

Procedure

Run the following commands to disable automatic FPD upgrade.

Example:

```
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
```

Upgrade FPDs manually

Use this task to upgrade FPDs manually.

Use the following procedure to upgrade the FPDs manually.

Note The Golden FPDs cannot be upgraded using the CLI.

Before you begin

Follow these steps to upgrade FPDs manually.

Procedure

Step 1 Run the **show hw-module fpd** command to display information about the current FPD version.

You can use this command to determine if you must upgrade the FPD.

Step 2 Run the **show alarms brief system active** command to display the active alarms.

You must upgrade the FPD when the

One Or More FPDs Need Upgrade Or Not In Current State

alarm is present.

Step 3 Run the **upgrade hw-module location [location-id] fpd [fpd name]** command to upgrade a specific FPD.

After upgrading the FPD, the user must wait for upgrade completion. The progress of the FPD upgrade can be monitored using the **show hw-module fpd** command.

Example:

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

Note
The FPDs of power modules belong to 0/PM0 and 0/PM1 locations. The FPDs belonging to both the PM locations cannot be simultaneously upgraded.

Step 4 Run the **reload location location-id** command to reload the FPDs belonging to a specific location with the new version.

The **Reload Loc** field in the output of **show hw-module fpd** command indicates whether the reload is required or not.

Example:

```
RP/0/RP0/CPU0:ios#reload location 0/RP0/CPU0
```

Step 5 (Optional) Run the **upgrade hw-module location all fpd all** command to upgrade all the FPDs at once.

Step 6 (Optional) Run the **upgrade hw-module [location [location-id | all]] fpd [fpd name] | all]** command to upgrade a specific FPD, all the FPDs, or the FPDs belonging to a specific location.

Example:

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

Note
The FPDs of power modules and SSDs cannot be forcefully upgraded.

FPD upgrades using YANG data models

Use this reference to review upgrading FPDs using Yang data models.

The following information supports upgrading FPDs using Yang data models:

- YANG is a data modeling language that helps to create configurations, retrieve operational data and execute actions. NCS 1010 acts on the data definition when these operations are requested using NETCONF RPCs. The data model handles the following types of requirements on NCS 1010 for FPD:

Operational Data	Native Data Model
Auto Upgrade: Enabling or disabling of automatic upgrade of FPD	Cisco-IOS-XR-fpd-infra-cfg.yang
Auto Reload: Enabling or disabling of automatic reload of FPD	Cisco-IOS-XR-fpd-infra-cfg.yang

FPD downgrade scenarios

Use this reference to review fPD downgrade scenarios.

When you downgrade from a higher release to lower release, the downgrade process of FPDs differs based on the higher and lower release firmware version.

- **Manual downgrade**
- When an FPD in the higher release runs a firmware that has an EVEN minor version, then the FPD does not downgrade automatically. The FPD requires manual downgrading using the force upgrade command[1] .
- For example, when you downgrade from R24.1.1 that has an FPD with an even firmware version 1.**10** to R7.11.1 that has the same FPD with firmware version 1.07, then the FPD does not downgrade automatically. The FPD must be manually downgraded using the force upgrade command[1] .
- **Automatic downgrade**
- When the change in the FPD firmware is in the major version, then the FPD automatically downgrades.
- For example. when you downgrade from R24.1.1 that has an FPD with firmware version **2**.10 to R7.11.1 that has the same FPD with a major difference in firmware version such as version **1**.07, then the FPD automatically downgrades.
- **Break release**
- When an FPD in the higher release runs a firmware that has an ODD minor version, then the FPD does not downgrade automatically. The FPD cannot be manually downgraded even with the force upgrade command[1] .
- For example, when you downgrade from R24.1.1 that has an FPD with odd firmware version 1.**19** to R7.11.1 that has the same FPD with firmware version 1.07, then the FPD does not downgrade automatically. Also, the FPD cannot be forced to downgrade manually using the force upgrade command[1] .
- **Minimum required firmware version**
- When an FPD in the lower release runs a firmware version that is less than the minimum version programmed in IDPROM of the FPD's respective cards, then the FPD does not downgrade automatically. The FPD cannot be manually downgraded even with the force upgrade command[1] .

[1] The force upgrade command is **upgrade hw-module location** *[location-id]* **fpd** *[fpd name]* **force**.

- For example, when you downgrade from R24.1.1 that has an FPD with firmware version 1.19 to R7.11.1 that has the same FPD with firmware version 1.07. If the minimum required firmware version that is programmed in IDPROM for that FPD is 1.09, then the FPD does not downgrade automatically. Also, the FPD cannot be forced to downgrade manually using the force upgrade command [1].

System stability checks

System stability checks are essential to measure the efficiency and ability of an upgrade to function over an extended period.

Details

At the EXEC prompt, execute the following commands to assess basic system stability checks before and after the software upgrade.

Command	Reason	Workaround
`show platform`	Verify that all nodes are in `IOS XR RUN/OPERATIONAL` state	NA

`show ipv4 interface brief`
Or
`show ipv6 interface brief`
Or
`show interfaces summary`
	Verify that all necessary interfaces are `UP`	NA

`show install active summary`	Verify that the proper set of packages are active	NA
`show install committed summary`	Verify that the proper set of committed packages are same as active	Execute ‘install commit’ command
`clear configuration inconsistency`	Verify/fix configuration file system	NA
`show hw-module fpd`	Ensure all the FPD versions status are CURRENT	Execute `upgrade hw-module fpd` command
`show media`	Display the current state of the disk storage media	To free up space, remove older .iso image files and bug fix .tar files.

Command	Reason	Workaround
`show media | i rootfs`	Display the current state of the root filesystem (rootfs). By default, the following files are stored in **rootfs** : • Older config commits • Older .iso image and .tar files for SMUs • All the extracted .tar files	The installation is blocked if it utilizes more than 92% of the disk space on the **rootfs** . To avoid this, we recommend maintaining: • Twice the free space of the .iso image file size when installing the software • At least two and a half times the size of the .tar file when installing SMUs To free up space in **rootfs** : • use the **clear install rollback id** *id* to remove older rollback points • consider storing all user data in the **harddisk:/** location
`show inventory`	Show chassis inventory information	NA
`show logging`	Capture show logging to check for any errors	NA

Install file sources

Use this reference to review obtain install files.

You can obtain the install files based on one of the following options that is best suited to your network:

- **Golden ISO:** You can build a customized golden ISO (GISO) image with the base ISO and the required RPMs to automatically upgrade the software.
- **Base ISO and Optional RPMs:** You can upgrade the software through the standard method where you install the ISO followed by the required RPMs.

Download install files from Cisco Software Center

Use this task to download install files from Cisco software center.

Obtain the install files (base ISO and RPMs) for the target release.

Before you begin

Follow these steps to download install files from Cisco software center.

Procedure

Step 1 Access the Cisco Software Download page.

For optimum website experience, we recommend any of the following browsers: Google Chrome, Mozilla Firefox or Internet Explorer.

Step 2 Click **Browse All** and navigate to NCS 1010 using **Optical Networking** > **Optical Data Center Interconnects** > **Network Convergence System 1000 Series** > **Network Convergence System 1010**.

Step 3 Select the Software Type: IOS XR Software or IOS XR Software Maintenance Upgrades (SMU).

Step 4 From the left pane, select the release.

For the selected release, the Software Download page displays the downloadable files. For more information, see Install ISO and RPMs, on page 17.

Step 5 Use your Cisco login credentials to download the files.

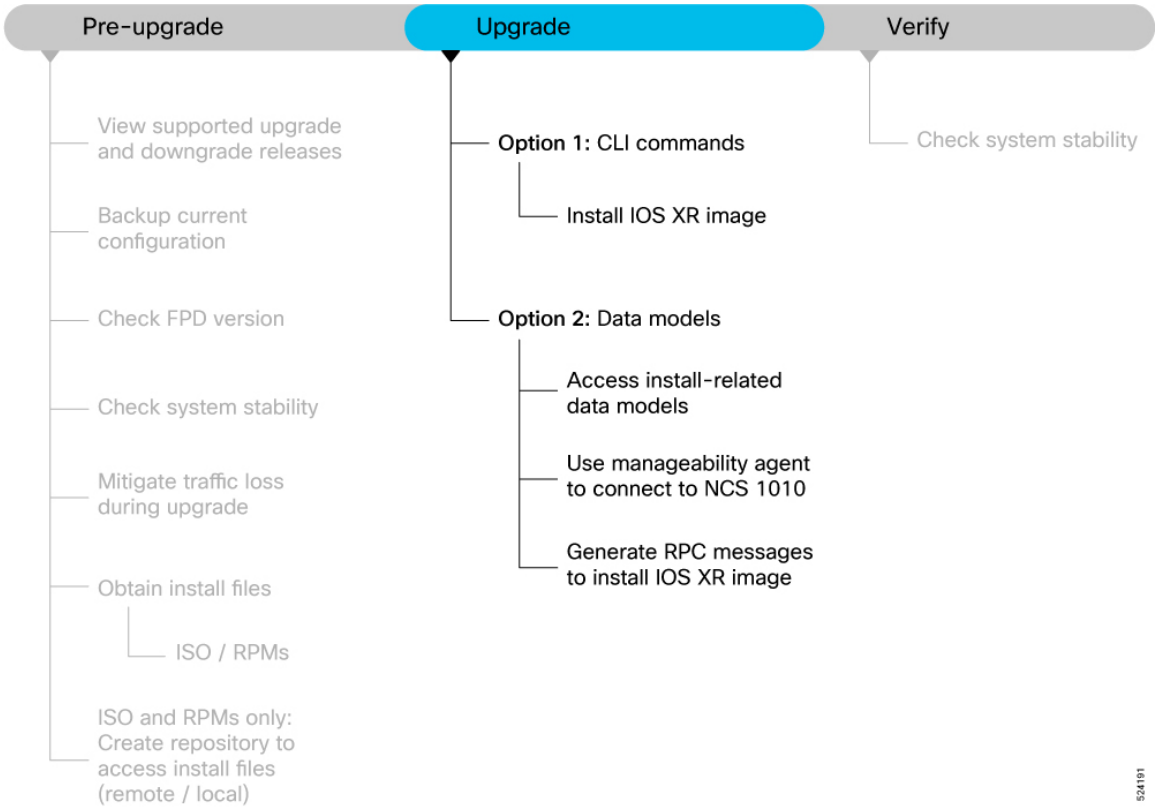
Software upgrade methods

Use this reference to review upgrade the software.

This section provides information about the processes involved in upgrading the IOS XR software on NCS 1010.

Note The NCS 1010 platform supports In-Service Software Upgrade (ISSU), and the software upgrade process is designed to be a non-impactful operation on network traffic.

- *Figure 2: NCS 1010 Upgrade workflow*



The Cisco IOS XR software can be upgraded using one of these methods:

- Upgrade NCS 1010 Using CLI Commands
- Upgrade NCS 1010 Using YANG Data Models

Supported upgrade and downgrade releases

Use this reference to review view supported upgrade and downgrade releases.

This section provides the supported upgrade and downgrade paths for NCS 1010. Consider the following guidelines when performing an upgrade or downgrade:

Note Downgrading from software release 7.11.1 or later to any earlier version is traffic-affecting and may result in a CMA process traceback.

- When downgrading the software image from release 24.4.x to an earlier version, we recommend to manually downgrade the line card firmware as well to prevent any impact on various functionalities.
- It is recommended to perform the upgrade with FPD auto-upgrade enabled to ensure the FPD versions are up to date and to prevent potential upgrade-related issues.

- The following table lists the upgrade and downgrade paths supported for Cisco NCS 1010.

Source Release	Destination Release	Bridge SMU	Source Release	Destination Release	Target SMU
2531	2541	NA	2541	2531	NA
2511	2541	CSCwn69606	2541	2511	NA
2431	2541	CSCwm77418	2541	2431	CSCwm77418
7112	2541	CSCwm77418,CSCwk75706	2541	7112	CSCwm77418
2541	2611	NA	2611	2541	NA
2531	2611	NA	2611	2531	NA
2511	2611	CSCwn69606	2611	2511	NA
2431	2611	CSCwm77418	2611	2431	CSCwm77418
7112	2611	CSCwm77418, CSCwk75706	2611	7112	CSCwm77418

CLI software upgrade method for Cisco NCS 1010

Use this reference to review upgrade NCS 1010 using CLI commands.

There are two options to upgrade your Cisco IOS XR software using the Command Line Interface (CLI):

- Base ISO and optional RPMs
- Golden ISO (GISO)

Install ISO and RPMs

Use this task to install ISO and RPMs.

Use this procedure to install the base ISO and optional RPMs.

Before you begin

Follow these steps to install ISO and RPMs.

Procedure

Step 1 Copy the ISO image to be installed either on the NCS 1010 hard disk or on a network server to which NCS 1010 has access.

Example:

```
RP/0/RP0/CPU0:ios#scp root@<ip-address>:/<dir>/1010-x64-release.iso harddisk:
```

Step 2 To verify data integrity, verify the md5 checksum of the copied file with the original MD5 values on CCO.

Example:

```
RP/0/RP0/CPU0:ios#show md5 file /harddisk:/1010-x64-release.iso
```

Step 3 Install the base image to upgrade the system.

Example:

```
RP/0/RP0/CPU0:ios#install replace /harddisk:/1010-x64-release.iso
```

The image is installed, the changes are applied through a reload or a restart of the system, and commits the changes. However, you do not have control over the timing of the reload or restart —these occur as soon as the package operation completes and the system is ready.

```
RP/0/RP0/CPU0:ios#install package replace /harddisk:/1010-x64-release.iso

RP/0/RP0/CPU0:ios#install apply [reload | restart]

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

- **Option 1:** Install ISO without control over reload timing.

  If you want to control when your system reloads (management of a network outage), we recommend that you schedule an upgrade window and perform an **install replace** , letting the system reload without intervention.

- **Option 2:** Install ISO with control over reload timing.

  Note
  Starting with upgrades to R2531 and later, this option is supported only if the ISO release is same as the running software release. This command is no longer supported for XR release upgrades. You may use the `install package replace` command to install optional RPMs or bug fixes.

  a. Install the image.

  b. Apply the changes.

  You can use either the `reload` or `restart` options based on the file that is installed. To determine whether a `reload` or `restart` is required, check the output of **show install request** command. The output indicates the required actions.

  c. Commit the operation.

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

  Note
  The **install commit** command must be executed immediately after software upgrades or SMU installations and before applying any new configuration changes or powering off the device to prevent loss of changes upon reboot.

Step 4 (Optional) After the base image is upgraded, install the additional packages. For more information, see Install additional RPMs and bug fixes.

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

Install golden ISO

Use this task to install golden ISO.

Use this procedure to install the Golden ISO (GISO) that contains the base ISO and a customized list of optional RPMs.

Golden ISO (GISO) upgrades NCS 1010 to a version that has a predefined list of bug fixes (sometimes also called software maintenance updates) with a single operation.

To update the system to the same release version with a different set of bug fixes:

- Create a GISO with the base version and all the bug fixes you require
- Use the **install replace** or **install package replace** commands to install the GISO.

The GISO can include bridging bug fixes for multiple source releases, and installs only the specific bridging bug fixes required for the target release.

The bridging bug fix RPMs can be used in the following scenarios:

- To resolve a bug that might stop upgrade.
- To meet the prerequisite requirements of a new release version that were not met by the earlier version.

Note The **install replace** command is supported only with GISO, but not with .rpm packages directly.

Before you begin

Follow these steps to install golden ISO.

Procedure

Step 1 Copy the GISO image file to the /harddisk: of NCS 1010.

Example:

```
RP/0/RP0/CPU0:ios#scp root@<ip-address>:/auto/tftp-test/1010-x64-release.iso harddisk:
```

Step 2 Install the GISO.

Example:

```
RP/0/RP0/CPU0:ios#install replace source-location/giso-name.iso
```

The

```
RP/0/RP0/CPU0:ios#install package replace source-location/giso-name.iso


RP/0/RP0/CPU0:ios#install apply [reload | restart]


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

...


RP/0/RP0/CPU0:ios#install package remove xr-cdp

Install remove operation 39.1.1 has started
Install operation will continue in the background
...
Packaging operation 39.1.1: 'install package remove xr-cdp' completed without error

RP/0/RP0/CPU0:ios#install apply
Thu Feb 02 11:13:09.015
Once the packaging dependencies have been determined, the install operation may have to reload the
system.
If you want more control of the operation, then explicitly use 'install apply restart' or 'install
apply reload' as
reported by 'show install request'.
Continue? [yes/no]:[yes] yes
RP/0/RP0/CPU0:Feb 02 11:13:12.771 : instorch[404]: %INSTALL-6-ACTION_BEGIN : Apply by restart 39.1
started
Install apply operation 39.1 has started
Install operation will continue in the background

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

- **Option 1:** Install GISO without control over reload timing.
  - **a.** Install GISO to upgrade to a new release, add or remove bugfixes or optional packages.

    *source-location*can be in the following location.
  - **b.** Local path to the GISO—files located in or under `/var/xr/disk1/`, `/harddisk:/` or `/misc/disk1/`

    This command runs the replace operation and applies the new version via NCS 1010 restart or reload, whichever is least impactful, given the change. For example, if you have a GISO that is the same as your base image except one bugfix, and that bugfix can be applied by process restart, the command will install the bugfix and apply by restart, no NCS 1010 reload occurs. However, you do not have control over the timing of the reload or restart—these operations occur as soon as the packaging is complete and the system is ready. If you want to control the timing of system reloads, we recommend that you schedule an upgrade window and run the **install replace** command, allowing the system to reload without manual intervention or network impact.
  - **c.** [Optional] Specify **reload** keyword to force reload for all operations. This may be useful if you want a reliable flow.
  - **d.** [Optional] Specify **commit** keyword for the install, apply and commit operations to be performed without user intervention.

- **Option 2:** Install GISO with control over reload timing.

  Note
  Starting with upgrades to R2531 and later, this option is supported only if the ISO release is same as the running software release. This command is no longer supported for XR release upgrades. You may use the `install package replace` command to install optional RPMs or bug fixes.

a. Install GISO to upgrade to a new release, add or remove bugfixes or optional packages. The functionality is similar to **install replace** command, except that the staging of packaging changes is performed using this command.

   The **install package replace** command does not apply the changes.

b. Apply the changes.

   You can use either the `reload` or `restart` options based on the change that is installed. You can only apply the changes by restarting the software if the difference between the GISO being installed and the running image is minimal such as bugfixes or package updates.

   To determine whether a `reload` or `restart` is required, check the output of **show install request** command. The output indicates the required actions.

Note
A GISO label is a string that identifies a GISO. Any install operation, such as adding or removing a package or modifying the software image (replace or package replace) will change the custom label to a system-generated default label. For example:

In this example, the software image is modified to remove the CDP package.

Apply the changes.

View the software version.

The

`GISO1`

custom label is replaced with the label

`24.3.1`

generated by the system.

Data model software upgrade method

Use this reference to review upgrade using data models.

The following information supports upgrade using data models:

- Data models are a programmatic way of configuring and collecting operational data of a network device. They replace the process of manual configuration and can be used to automate configuration tasks across heterogeneous devices in a network.

Access install-related data models

Use this task to access install-related data models.

You can use YANG data models to install and upgrade NCS 1010. The data models are packaged with the release image in the

`/pkg/yang`

directory.

Before you begin

Follow these steps to access install-related data models.

Procedure

Step 1 Navigate to the directory in the release image where the YANG data models are available.

Example:

```
RP/0/RP0/CPU0:ios#run
[node_RP0_CPU0:~]$cd /pkg/yang
```

Step 2 View the list of install-related data models on NCS 1010.

Example:

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

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

Date Model	Description
Cisco-IOS-XR-um-install-cfg	Unified data model that contains a collection of YANG definitions for Cisco IOS XR install package configuration, and augments the modules with configuration data.
Cisco-IOS-XR-install-oper	Operational data model to view details that are related to basic package information, active and committed packages, and fixes.
Cisco-IOS-XR-install-cfg	Configuration data model to specify the location of the install source.
Cisco-IOS-XR-install-act	Action model to perform basic install operations and software upgrade.
Cisco-IOS-XR-install-search-act	Action model that contains a collection of YANG definitions for install actions related to searching for package information.
Cisco-IOS-XR-install-augmented-oper	Augmented operational model that displays information aboutpackaging, atomic changes, and history of the install operation on the NCS 1010.
Cisco-IOS-XR-install-augmented-act	Action model to perform flexible install operations, includingcontrolling the exact timing of system reloads and rolling back to a previous commit.

Date Model	Description
Cisco-IOS-XR-shellutil-copy-act	Action model to copy files on the NCS 1010 from a source location.

You can also access the supported data models to install Cisco IOS XR software from the Github repository.

Manageability agent connections to Cisco NCS 1010

Use a manageability agent like NETCONF or gRPC to connect and communicate with NCS 1010. You can send Remote Procedure Calls (RPC) requests to configure or retrieve operational data from NCS 1010. NCS 1010 processes the request and responds to the request through an RPC response. You use the RPCs to send requests to install the software by populating the relevant parameters of a container and leaf in the data model. For more information about understanding the data model structure and using data models, see the *Cisco NCS 1010 Data Models Configuration Guide* .

Generate RPC messages to install an IOS XR image

Use this task to generate RPC messages to install IOS XR image.

This task supports Cisco NCS 1010 setup, deployment, upgrade, or maintenance workflows.

Before you begin

Not all software versions are supported as the target upgrade software version. You must review the supported upgrade and downgrade paths, hardware or software limitations, and bridging SMUs required for the version. For more information about checking the release support between the current and target versions, see Supported upgrade and downgrade releases, on page 4.

Follow these steps to generate RPC messages to install IOS XR image.

Procedure

Step 1 Invoke the **install-replace** RPC on the Cisco-IOS-XR-install-act.yang data model to upgrade NCS 1010.

Step 2 Configure the values of the `source-type`, `source`, and `file` parameters.

Step 3 Send `edit-config` NETCONF RPC request using the data model to configure the repository. Edit the values in the `repositories` parameters and send this request to NCS 1010 from the client.

Step 4 Apply the changes to activate the ISO on NCS 1010 using RPCs by using the `install-apply` RPC on the`Cisco-IOS-XR-install-augmented-act.yang` datamodel and send the RPC from the client to NCS 1010.

Example:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <install-apply xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-install-augmented-act">
   <apply-method>least-impactful</apply-method>
  </install-apply>
</rpc>
```

View the RPC response received from NCS 1010.

```
<?xml version="1.0"?>
  <rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <op-id xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-install-augmented-act">2.1</op-id>
  </rpc-reply>
```

In the response, NCS 1010 sends an ID indicating that the changes are applied successfully.

Step 5 Verify that the software upgrade is successful. Use the `get`RPCon `Cisco-IOS-XR-install-oper.yang` data model. Edit the `install` parameter and send an RPC request from the client to NCS 1010.

Example:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get>
   <filter>
    <install xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-install-oper">
     <request/>
    </install>
   </filter>
  </get>
</rpc>
```

View the RPC response received from NCS 1010.

```
<?xml version="1.0"?>
  <rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
    <install xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-install-oper">
     <request>
      <request>install commit</request>
      <state>success</state>
     <timestamp>2022-06-27 T02:52:07Z</timestamp>
    <operation-id>26</operation-id>
   </request>
  </install>
```

The state of the install operation in the RPC response indicates that the software and the RPMs are upgraded successfully.

What to do next

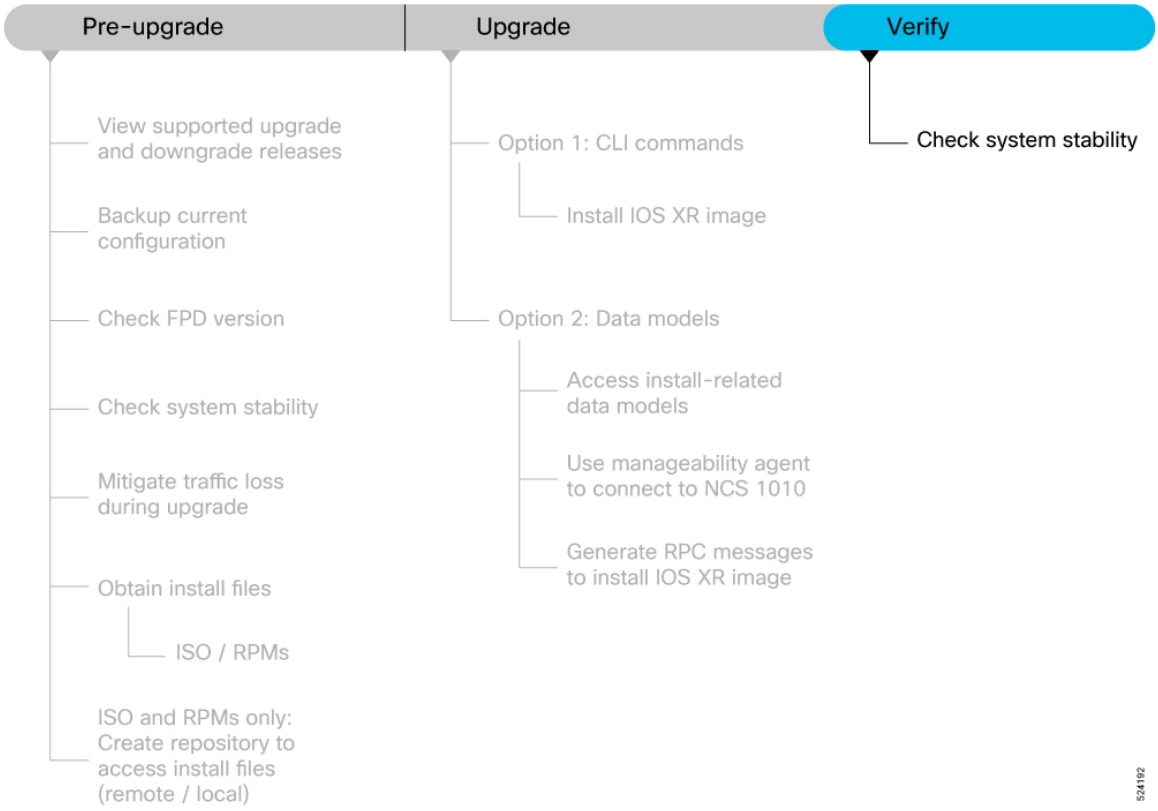
Perform preliminary checks to verify that NCS 1010 is upgraded successfully.

Software upgrade verification

Use this reference to review verify the software upgrade.

This section provides information about the processes involved in verifying the upgraded software on your NCS 1010.

- *Figure 3: Workflow to Verify the Software Upgrade*



- This section contains the following topics:

System stability checks before upgrade

System stability checks are essential to measure the efficiency and ability of an upgrade to function over an extended period.

Details

At the EXEC prompt, execute the following commands to assess basic system stability checks before and after the software upgrade.

Command	Reason	Workaround
show platform	Verify that all nodes are in `IOS XR RUN/OPERATIONAL` state	NA
show redundancy	Verify that a standby RP is available, and the system is in `NSR-ready` state	NA
show install active summary	Verify that the proper set of packages are active	NA

Command	Reason	Workaround
show install committed summary	Verify that the proper set of committed packages are same as active	Execute 'install commit' command
clear configuration inconsistency	Verify/fix configuration file system	NA
show hw-module fpd	Ensure all the FPD versions status are CURRENT	Execute `upgrade hw-module fpd` command
show media	Display the current state of the disk storage media	To free up space, remove older .iso image files and bug fix .tar files.
show inventory	Show chassis inventory information	NA