

Perform System Upgrade and Install Feature Packages

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

The topics covered in this chapter are:

- Upgrading the System, on page 1
- View supported software upgrade or downgrade versions, on page 4
- Restrictions for Cisco IOS XR software upgrades on NCS 5700 platforms, on page 8
- HTTPS copy and install operation requirements, on page 8
- Upgrading Features, on page 8
- Pre-upgrade consideration for configuration commit history, on page 10
- Upgrading Cisco IOS XR from 7.10.x/7.11.1 to 7.11.2 or later releases, on page 11
- Optional packages, on page 12
- Install Prepared Packages, on page 15
- Install Packages, on page 18
- Uninstall Packages, on page 25
- View Features and Capabilities Supported on a Platform, on page 28

Upgrading the System

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

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

Note If you insert a line card on a router that is running a lower version than the one the line card supports, the line card fails to boot. You must first upgrade the router to a software version that supports the line card, insert the line card and iPXE boot the line card.

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

Note

- Ensure that you have adequate disk space.
- Run the **fsck** command to check the status of the file system, for a successful IOS XR upgrade. You must run the **fsck** command in the System Admin EXEC mode to install a System Admin package, and in the XR EXEC mode to install the XR package.
- All install commands are applicable in both the System Admin EXEC mode and in XR EXEC mode. System Admin install operations are done from XR EXEC mode.

Perform a system upgrade by installing a base package–Cisco IOS XR Unicast Routing Core Bundle. To install this bundle, run the **install** command. The filename for the Cisco IOS XR Unicast Routing Core Bundle bundle is *ncs5500-mini-x.iso*.

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

Do not reload the router during an upgrade operation.

Note To enable hardware programming after upgrading the chassis from an older software version to IOS XR Release 7.6.x or later through ISSU, initiate a chassis reload. The chassis reload is mandatory, if you must enable a maximum transmission unit (MTU) value of 9646 on applicable interfaces.

Note Ensure that the system is on Cisco IOS XR Software Release 7.3.x, for a successful upgrade to Cisco IOS XR Software Release 7.6.x.

Note For a successful upgrade from Cisco IOS XR Release 7.2.2 to Cisco IOS XR Release 24.2.21, perform one of the following actions:

- Upgrade to the interim version, say, 7.3.2 and then to 24.2.21.
- Upgrade using USB boot.

Cisco IOS XR supports RPM signing and signature verification for Cisco IOS XR RPM packages in the ISO and upgrade images. All RPM packages in the Cisco IOS XR ISO and upgrade images are signed to ensure cryptographic integrity and authenticity. This guarantees that the RPM packages haven't been tampered with and the RPM packages are from Cisco IOS XR. The private key, which is used for signing the RPM packages, is created and securely maintained by Cisco.

Example partition layouts

The following table shows the partition layout across platforms for different Cisco IOS XR releases indicated below.

Release / Release Group	VM Type	Location	rootfs	log	config	disk0	harddisk
6.4.2	XR VM	0/0/CPU0	3.8G	469M	469M	968M	—
6.4.2	XR VM	0/RSP0/CPU0	3.8G	469M	469M	968M	23G
6.4.2	Sysadmin VM	0/0	2.4G	469M	469M	968M	—
6.4.2	Sysadmin VM	0/RSP0	2.4G	469M	469M	968M	31G
6.6.2 / 6.6.3 / 7.1.1 / 7.1.3 / 7.3.2	XR VM	0/0/CPU0	3.8G	1.9G	969M	3.8G	—
6.6.2 / 6.6.3 / 7.1.1 / 7.1.3 / 7.3.2	XR VM	0/RSP0/CPU0	3.8G	1.9G	969M	3.8G	23G
6.6.2 / 6.6.3 / 7.1.1 / 7.1.3 / 7.3.2	Sysadmin VM	0/0	2.4G	1.9G	969M	3.8G	—
6.6.2 / 6.6.3 / 7.1.1 / 7.1.3 / 7.3.2	Sysadmin VM	0/RSP0	2.4G	1.9G	969M	3.8G	31G
7.5.4 and later	XR VM	0/0/CPU0	7.6G	1.9G	969M	3.8G	—
7.5.4 and later	XR VM	0/RSP0/CPU0	7.6G	1.9G	969M	3.8G	45G
7.5.4 and later	Sysadmin VM	0/RSP0	7.6G	1.9G	969M	3.8G	62G
7.5.4 and later	Sysadmin VM	0/0	7.6G	1.9G	969M	3.8G	—

View supported software upgrade or downgrade versions

Cisco routers come preinstalled with Cisco IOS XR software. You can upgrade the software to access new features and fixes, or downgrade it if needed. To take advantage of the latest features and software improvements, we recommend that you keep your router updated with the current version.

Table 1: Feature History Table

Feature Name	Release Information	Description
Supported software upgrade or downgrade IOS XR versions	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.

Compatibility checks for Cisco IOS XR software upgrades and downgrades

The compatibility check feature for Cisco IOS XR software facilitates choosing a release that follows Cisco-certified upgrade and downgrade paths, asking critical questions such as:

- Which upgrade or downgrade releases are supported for my current release
- If I want to upgrade from Release X to Release Y, does my router support this upgrade
- Are there any bridging SMUs that must be installed before upgrading?

This feature checks whether your current release can upgrade or downgrade to a specified target release. This automatic validation occurs during the start of a software upgrade or downgrade using the **install replace** command. If the validation fails, the upgrade is blocked, and the system notifies you of the reason for the failure. This validation allows you to proactively determine upgrade or downgrade compatibility thus saving plannig effort.

The feature provides prerequisites and limitations for a specific upgrade or downgrade such as:

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

If needed, bypass automatic validation by including the **force** keyword with the **install replace** command. When you use this option, the system displays warning messages if the upgrade fails, but it does not stop the software upgrade. Explore **force ?** for any impacts beyond this.

Show commands for software upgrade and downgrade

You can view the software upgrade and downgrade information using the **show** commands in this table 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 **Note** From Cisco IOS XR Release 25.2.1, the **running** keyword is deprecated from the **show install upgrade-matrix iso** command. This is applicable for routers with Cisco IOS XR7 network operating systems.

Note If your running version is below Cisco IOS XR Release 7.5.1, upgrade the system to Cisco IOS XR Release 7.5.1. Then, use the **show install upgrade-matrix** command to check the required SMUs for your target version.

Supported software upgrade from running version

This example shows all supported releases for upgrade from the current version on the NCS 5500 router:

```
Router#show install upgrade-matrix running
Fri Jul 29 10:12:47.740 IST
This may take a while ...
```

```
The current software can be upgraded from and downgraded to the following releases:

================================================================================
From      To        Bridge SMUs Required        Caveats
================================================================================
7.0.2     7.5.1     None                        None
--------------------------------------------------------------------------------
7.5.1     7.0.2     None                        None
--------------------------------------------------------------------------------
7.5.1     7.4.1     None                        None
--------------------------------------------------------------------------------
7.5.1     7.1.3     None                        None
--------------------------------------------------------------------------------
7.5.1     7.1.2     None                        None
--------------------------------------------------------------------------------
7.5.1     7.2.1     None                        None
--------------------------------------------------------------------------------
7.5.1     7.2.2     None                        None
--------------------------------------------------------------------------------
7.5.1     7.3.1     None                        None
--------------------------------------------------------------------------------
7.5.1     7.3.2     None                        None
--------------------------------------------------------------------------------
7.4.1     7.5.1     None                        None
--------------------------------------------------------------------------------
7.1.3     7.5.1     None                        None
--------------------------------------------------------------------------------
7.1.2     7.5.1     None                        None
--------------------------------------------------------------------------------
7.2.1     7.5.1     None                        None
--------------------------------------------------------------------------------
7.2.2     7.5.1     None                        None
--------------------------------------------------------------------------------
7.3.1     7.5.1     None                        None
--------------------------------------------------------------------------------
7.3.2     7.5.1     None                        None
--------------------------------------------------------------------------------
```



Note To downgrade the system to a release earlier than Release 24.4.1, first deactivate the **ncs5500-healthcheck** package to prevent disk space issues during the downgrade.

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.

```
Router#show install upgrade-matrix iso /harddisk:/ncs5500-goldenk9-x-7.5.2-rev1.iso
Fri Jul 29 10:16:43.233 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.

Supported releases from current version to an ISO version

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

```
Router#show install upgrade-matrix iso /harddisk:/ncs5500-goldenk9-x-7.5.2-rev1.iso all
Fri Jul 29 10:17:02.826 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
--------------------------------------------------------------------------------
7.4.2     7.5.2     None                        None
--------------------------------------------------------------------------------
7.4.1     7.5.2     None                        None
--------------------------------------------------------------------------------
7.5.2     7.4.2     None                        None
--------------------------------------------------------------------------------
7.5.2     7.6.1     None                        None
--------------------------------------------------------------------------------
7.5.2     7.4.1     None                        None
--------------------------------------------------------------------------------
7.5.2     7.2.1     None                        None
--------------------------------------------------------------------------------
7.5.2     7.2.2     None                        None
--------------------------------------------------------------------------------
7.5.2     7.3.1     None                        None
--------------------------------------------------------------------------------
7.5.2     7.3.2     None                        None
--------------------------------------------------------------------------------
7.2.1     7.5.2     None                        None
--------------------------------------------------------------------------------
7.2.2     7.5.2     None                        None
--------------------------------------------------------------------------------
7.6.1     7.5.2     None                        None
--------------------------------------------------------------------------------
7.3.1     7.5.2     None                        None
--------------------------------------------------------------------------------
7.3.2     7.5.2     None                        None
--------------------------------------------------------------------------------
```

Supported releases from running version to an ISO version

This 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:

```
Router#show install upgrade-matrix iso /harddisk:/ncs5500-goldenk9-x-7.5.2-rev1.iso
from-running
Fri Jul 29 10:17:35.583 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
--------------------------------------------------------------------------------
```

Restrictions for Cisco IOS XR software upgrades on NCS 5700 platforms

Starting from Cisco IOS XR Release 25.3.1, these restrictions apply to the Cisco IOS XR software upgrades on NCS 5700 platforms.

- If the router reloads during the upgrade before executing the **install commit** command, it will boot the target image instead of the original image.
- The software does not support the **install package replace** command for installing ISO with control over reload timing. Do not attempt to use it as it results in an error.
- The software does not support rollbacks for release upgrades. Use the **install replace** command with the previous golden ISO instead.

HTTPS copy and install operation requirements

Starting with IOS XR Release 26.3.1, HTTPS copy and install operations require strict TLS session shutdown. If the remote HTTPS server closes the TCP connection without sending a TLS `close_notify` alert, the operation fails.

For a successful HTTPS copy and install operation, configure or update the remote HTTPS server to send a proper TLS `close_notify` alert prior to closing the connection.

Upgrading Features

Upgrading features is the process of deploying new features and software patches on the router. Perform a feature upgrade by installing packages. Perform a software patch installation by installing Software Maintenance Upgrade (SMU) files.

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

For example, the components of the routing package are split into individual RPMs such as BGP and OSPF. BGP is a part of the base software version and is a mandatory RPM, and hence can't be removed. However, you can add and remove optional RPMs such as OSPF as required.

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

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

Use the **install** commands to install packages and SMUs. For more information about the install process, see Install Packages, on page 18.

Note

- Ensure that you have adequate disk space.
- Run the **fsck** command to check the status of the file system, for a successful IOS XR upgrade. You must run the **fsck** command in the System Admin EXEC mode to install a System Admin package, and in the XR EXEC mode to install the XR package.
- All install commands are applicable in both the System Admin EXEC mode and in XR EXEC mode. System Admin install operations are done from XR EXEC mode.

There are separate packages and SMUs for the XR VM and the System Admin VM. They can be identified by their filenames.

The XR and System Admin packages and SMUs can be activated from XR and System Admin VMs.

You can alternatively perform a cross VM operation, by activating or deactivating the System Admin packages and SMUs from XR.

Third-Party SMUs

Consider these points while activating and deactivating third-party SMUs:

- To activate a third-party SMU, you should have a corresponding base package.
- When you activate a third-party SMU, the corresponding third-party base package state is inactive, this is an expected behavior.
- To deactivate a third-party SMU, ensure that you activate the corresponding third-party base package. Third-party SMUs deactivated explicitly might lead to triages to the install team.



Note All SMUs are bundled together with the base package in a TAR file



Note All Cisco RPMs have the platform name in the filename. For example, **ncs5500**-sysadmin.

Pre-upgrade consideration for configuration commit history

Before upgrading IOS XR software, keep in mind the following points about configuration commit history:

- The system stores configuration commit history in an internal binary database format, which uses a schema known as the configuration namespace version.
- This schema may change between software releases. If the namespace version changes, the upgraded software may not interpret commit records created on the previous release.
- Commands that reference pre-upgrade commits, such as **show configuration rollback changes** <*commit-id*>, may return the following error after upgrading:

  ```
  Configuration namespace version of one or more of the processed commits is not supported
  by the current software. The incompatible configuration will not be processed.
  ```

- This behavior is expected and does not indicate a system defect.

To preserve configuration commit history for audit or troubleshooting purposes, export commit details prior to the upgrade.

Example commands to export commit information:

- **show configuration commit list**
- **show configuration commit changes** <*commit-id*>

Save the output externally so it can be referenced after the upgrade.

After completing the upgrade, all commits created on the new software version will be fully accessible using standard rollback and commit history commands.

Upgrading Cisco IOS XR from 7.10.x/7.11.1 to 7.11.2 or later releases

Ensure that you follow these steps to avoid continuous process restarts affecting the SDR console. This issue is particularly common when base and VRF configurations are in place in Native mode, including setups for VRF, OSPF, BGP L3VPN, L2VPN xconnect, and MPLS OAM.

However, if the MDB profile is configured along with Native mode, you will not encounter this issue.

Before you begin

You don't need to follow these steps if you are upgrading from Cisco IOS XR Software Release 7.11.2 to Release 24.x.y and later releases.

Procedure

Step 1 Check that NPU Operating Mode is *native*, using the **show hw-module profile npu-operating-mode** command.

Example:

```
Router#show hw-module profile npu-operating-mode
NPU Operation Mode: Native
```

- If the NPU operation Mode is *Compatibility* mode or *Not Applicable*, you do not need to follow these steps.
- If the NPU operation mode is *Native*, follow further steps.

Step 2 Check if any hw-module is already configured for mdb-profile, using the **show running configuration** command.

Example:

```
Router#show running-config | i hw
hw-module profile mdb l3max-se <-- MDB profile configured
```

If mdb profile is not configured, please perform **Step 4.**

Step 3 Verify if mdb profile is already activated, using the **show hw-module profile mdb-scale** command.

Example:

```
Router#show hw-module profile mdb-scale
MDB scale profile: l3max-se
```

The MDB scale profile can be l3max, l3max-se, l2max, l2max-se.

If the profile is already configured and activated, no further steps are needed.

Step 4 If mdb profile is not configured, then check the default MDB Profile, using the **show hw-module profile mdb-scale** command.

Example:

```
Router#show hw-module profile mdb-scale
 MDB scale profile: l3max
```

The default mdb profile can be l3max or l3max-se. In the above example, the deafult mdb profile is l3max.

Step 5 Configure default MDB profile, using the **hw-module profile mdb***{mdb profile-name}* command.

Example:

```
Router#hw-module profile mdb l3max
In order to activate this new mdb profile, you must manually reload the chassis
Router(config)#commit
```

Step 6 Proceed with the upgrade, you don't need to manually reload the chassis at this point since we are in upgrade.

Optional packages

Cisco IOS XR software images are composed of a base image (ISO) that includes mandatory packages and optional packages (RPMs). Optional RPMs are software packages included in or available for the IOS XR image that provide additional features beyond the mandatory base functionality.

These optional RPMs can be included in the ISO image or provided separately for installation as needed. Optional RPMs enable specific features such as routing protocols such as OSPF, RIP, ISIS, and so on, security features such as k9sec for 802.1X, multicast, telemetry, and others.

Some optional RPMs are included in the base ISO image, while others are available as separate downloadable packages. Operators can add, upgrade, or remove optional RPMs using IOS XR software management commands, allowing flexible customization of the software features on the device.

Table 2: Feature History Table

Feature Name	Release Information	Description
Deprecated insecure protocols in optional RPMs	Release 26.2.1	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) This feature improves platform security and reduces the threat surface of the Cisco Networking products by restricting insecure protocols such as Telnet, FTP, TFTP, and RCP (deprecated in Cisco IOS XR Release 25.4.1) from Cisco IOS XR base package. In this release, Telnet is added to the optional RPM, `Telnet.rpm`, and FTP, TFTP, and RCP are added to the optional RPM, `IP-Insecure-Apps.rpm .` We recommend you to migrate to secure alternatives such as SSH, SCP, SFTP as Telnet, FTP, TFTP, and RCP protocols arenot supported anymore in the Cisco IOS XR base package.

Starting with Cisco IOS XR Release 26.2.1, the insecure protocols such as Telnet, FTP, TFTP, and RCP are no longer part of Cisco IOS XR base packages. Instead, install the new optional RPMs `Telnet.rpm` to use Telnet features and `IP-Insecure-Apps.rpm` to use FTP and TFTP features.

You must install these optional RPMs only if it is obsolutely required as deprecation warnings continue to be generated once every 30 days as long as Telnet, FTP, TFTP, and RCP configurations are used. The support for these optional RPMs will be completely removed from Cisco IOS XR in future releases such that Telnet, FTP, TFTP, and RCP will no longer be supported in Cisco IOS XR.

To avoid system failures or configuration inconsistencies, we strongly recommend you to migrate to secure protocols such as SSHv2, SFTP, and SCP.

Note Telnet to console is still supported and not impacted by this feature enhancement.

Limitations of optional packages

To improve system security, the absence of optional packages such as `Telnet.rpm` and `IP-Insecure-Apps.rpm` disables certain network management features and restricts insecure protocols.

Without the optional RPMs, `Telnet.rpm` and `IP-Insecure-Apps.rpm`:

- Telnet configuration and execution commands cannot be used.
- Telnet to Management ports is not supported.
- Configuration and execution commands using FTP, TFTP, and RCP are rejected.
- Copy, install, load, or any operations using FTP or TFTP will fail and report errors.
- Systems upgraded with existing insecure configurations may raise configuration inconsistency alarms.

  You must clear inconsistencies before committing any new configuration.

Commands and YANG data models supported using optional RPMs

In Cisco IOS XR Release 26.2.1, you can continue to use the commands and YANG data models for the deprecated Telnet, FTP, and TFTP protocols if you have installed the new `Telnet.rpm` and `IP-Insecure-Apps.rpm` respectively.

The following tables provide the supported configuration and execution commands and the YANG data models for Telnet, FTP, and TFTP in optional RPMs.

- Supported Telnet configuration and execution commands in optional RPMs
- Supported FTP and TFTP configuration and execution commands in optional RPMs
- Supported Telnet, TFTP, and FTP YANG models in optional RPMs

Table 3: Supported FTP and TFTP commands in optional RPMs

FTP config commands	TFTP config commands	FTP exec commands	TFTP exec commands
ip ftp client anonymous-password <>	**ip tftp client dscp** <>	**copy harddisk: ftp:**	**copy harddisk: tftp:**
ip ftp client passive	**ip tftp client dscp** <>	**copy ftp: harddisk:**	**copy tftp: harddisk:**
ip ftp client password *<WORD/clear/encrypted>*	**ip tftp client retries** <>	**copy running-config ftp:**	**copy running-config tftp:**
ip ftp client source-interface <>	**ip tftp client source-interface**<>	**copy ftp: running-config**	**copy tftp: running-config**
ip ftp client username <>	**ip tftp client timeout** <>	**copy xml-schema ftp:**	**copy xml-schema tftp:**
ip ftp client vrf <>	**ip tftp client vrf** *<WORD>*	**install source <ftp-path>**	**install source <tftp-path>**
ftp client anonymous-password <>	**ip tftp server homedir** <>	**install add source <ftp-path>**	**install add source <tftp-path>**

FTP config commands	TFTP config commands	FTP exec commands	TFTP exec commands
ftp client passive	**tftp client dscp** <>	**install replace <ftp-path>**	**install replace <tftp-path>**
ftp client password *<WORD/clear/encrypted>*	**tftp client retries** <>		
ftp client source-interface <>	**tftp client source-interface** <>		
ftp client username <>	**tftp client timeout** <>		
load ftp	**tftp client vrf** *<WORD>*		
	tftp ipv4 server homedir <>		
	tftp ipv6 server homedir <>		
	tftp vrf <WORD> ipv4 server homedir <>		
	tftp vrf *<WORD>***ipv6 server homedir** <>		
	load tftp		

Table 4: Supported Telnet, TFTP, and FTP YANG models in optional RPMs

Telnet YANG models	FTP and TFTP YANG models	FTP and TFTP YANG models for Install
`Cisco-IOS-XR-ipv4-telnet-cfg`	`Cisco-IOS-XR-um-ftp-tftp-cfg`	`Cisco-IOS-XR-spirit-install-act.yang`
`Cisco-IOS-XR-ipv4-telnet-mgmt-cfg`	`Cisco-IOS-XR-ip-tcp-cfg`	
`Cisco-IOS-XR-um-telnet-cfg`	`Cisco-IOS-XR-shellutil-copy-act`	
`Cisco-IOS-XR-openconfig-system-terminal-ext`		

Install Prepared Packages

A system upgrade or feature upgrade is performed by activating the ISO image file, packages, and SMUs. It is possible to prepare these installable files before activation. During the prepare phase, preactivation checks are made and the components of the installable files are loaded on to the router setup. The prepare process runs in the background and the router is fully usable during this time. When the prepare phase is over, all the prepared files can be activated instantaneously. The advantages of preparing before activation are:

- If the installable file is corrupted, the prepare process fails. This provides an early warning of the problem. If the corrupted file was activated directly, it might cause router malfunction.

- Directly activating an ISO image for system upgrade takes considerable time during which the router is not usable. However, if the image is prepared before activation, not only does the prepare process run asynchronously, but when the prepared image is subsequently activated, the activation process too takes less time. As a result, the router downtime is considerably reduced.
- It performs a disk-space check that is required for a successful operation. This quantifies the disk-space deficit, and provides you possible alternatives to free up space in the filesystem.
- It performs a package compatibility check. This ensures that all the required installation packages are available. For any package compatibility check error, details of the package and version are logged.

Complete this task to upgrade the system and install packages by making use of the prepare operation.

Note Depending on whether you are installing a System Admin package or a XR package, execute the **install** commands in the System Admin EXEC mode or XR EXEC mode respectively. All **install** commands are applicable in both these modes. System Admin install operations can be done from XR mode.

Procedure

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

For details, see Install Packages, on page 18.

Step 2 **show install repository**

Example:

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

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

Step 3 **show install request**

Example:

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

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

```
Install operation 8 is still in progress
```

Step 4 Execute one of these:

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

Example:

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

or

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

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

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

Step 5 **show install prepare**

Example:

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

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

Step 6 **install activate**

Example:

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

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

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

Activations of some SMUs require manual reload of the router. When such SMUs are activated, a warning message is displayed to perform reload. The components of the SMU get activated only after the reload is complete. Perform router reload immediately after the execution of the **install activate** command is completed.

Step 7 **show install active**

Example:

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

Displays packages that are active.

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

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

Step 8 **install commit**

Example:

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

Installing Packages: Related Commands

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

What to do next

- After performing a system upgrade, upgrade FPD by using the **upgrade hw-module location all fpd all** command from the System Admin EXEC mode. The progress of FPD upgrade process can be monitored using the **show hw-module fpd** command in the System Admin EXEC mode. Reload the router after the FPD upgrade is completed.
- Verify the installation using the **install verify packages** command.
- Uninstall the packages or SMUs if their installation causes any issues on the router. See Uninstall Packages.

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

Install Packages

Complete this task to upgrade the system or install a patch. The system upgrade is done using an ISO image file, while the patch installation is done using packages and SMUs. You can also include SMUs in an upgrade operation along with mini ISO.

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

Note

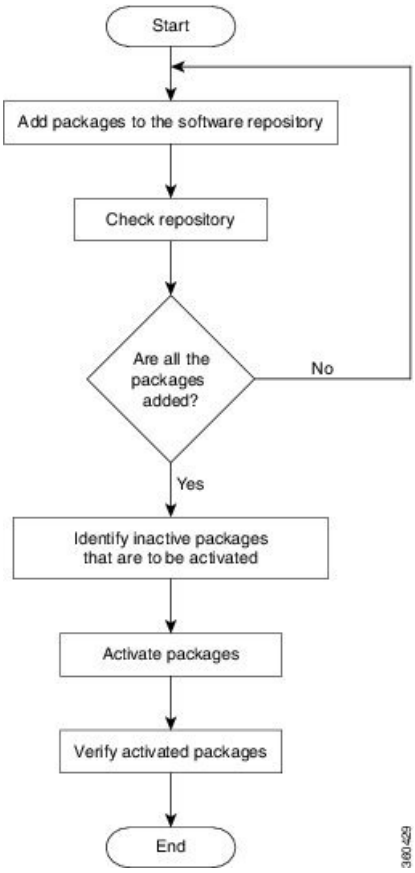
- Ensure that you have adequate disk space.
- Run the **fsck** command to check the status of the file system, for a successful IOS XR upgrade. You must run the **fsck** command in the System Admin EXEC mode to install a System Admin package, and in the XR EXEC mode to install the XR package.
- All install commands are applicable in both the System Admin EXEC mode and in XR EXEC mode. System Admin install operations are done from XR EXEC mode.

Note

- The system upgrade is supported only from XR EXEC mode.
- While the System Admin package can be executed using **install** commands in the System Admin EXEC mode and XR EXEC mode, the XR package can only be executed using the install commands in XR EXEC mode. All **install** commands are applicable in both these modes.
- While the System Admin SMUs can be installed in System Admin EXEC mode and XR EXEC mode, the XR SMUs can only be installed through the XR EXEC mode.
- Install operation over IPv6 is not supported.

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

Figure 1: Installing Packages Workflow



Before you begin

- You can add a package to the repository from a local disk in the router, from an inserted USB disk, or from a remote repository accessible through the management port or any data port.

  If the installable file is located on a USB in the router's USB port, use the **show media** or **show filesystem** commands. The installable file is labeled as either **usb:** or **disk2:** in the command outputs.

  If the installable file is located in a remote location that can be accessed through the management port, you must configure and bring up the management port to ensure reachability to the remote location. For more information, see the *Configure the Management Port* section in the *Bring-up the Router* chapter.

- Until Cisco IOS XR Release 7.11.21, after every user-triggered, ungraceful, or upgrade RP reload, you can check the sanity of the files from the install repository using the **run rpm -K --nosignature /install_repo/gl/xr/<package_name>** command in System Admin EXEC mode. This sanity check helps to detect the corrupt RPM files. Remove corrupt files, if detected and add valid files to avoid any file or file system corruption error that you may encounter during the installation or upgrade or post-upgrade process.

Procedure

Step 1 Execute one of these:

- **install add source** *<http or shttp transfer protocol>/package_path/ filename1 filename2 ...*
- **install add source** *<tftp transfer protocol>/package_path/ filename1 filename2 ...*
- **install add source** *<ftp or sftp transfer protocol>//user@server:/package_path/ filename1 filename2 ...*
- **install add source** *disk2: filename1 filename2 ...*

Example:

```
RP/0/RP0/CPU0:router#install add source /harddisk:/ ncs5500-mpls-1.0.0.0-r731.x86_64.rpm
ncs5500-mgbl-1.0.0.0-r732.x86_64.rpm
```

or

```
RP/0/RP0/CPU0:router#install add source sftp://root@8.33.5.15:/auto/ncs/package/
ncs55000-mcast-1.0.0.0-731.x86_64.rpm ncs5500-iosxr-mpls-1.0.0.0-732.x86_64.rpm
```

or

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

or

```
RP/0/RP0/CPU0:router#install add source sftp://root@8.33.5.15:/auto/ncs/package/
ncs55000-mcast-1.0.0.0-<release-number>.x86_64.rpm
ncs5500-iosxr-mpls-1.0.0.0-<release-number>.x86_64.rpm
```

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

The software files are unpacked from the package, validated, and then added to the software repository. This operation might take time depending on the size of the files being added. The operation is performed in asynchronous mode. The **install add** command runs in the background, and the EXEC prompt is returned when all files are unpacked.

Note
The repositories for the XR VM and the System Admin VM are different. The system automatically adds a routing package to the XR VM repository and a system administration package to the System Admin VM repository.

Important
Starting from Cisco IOS XR Release 7.11.21, if a file or file system corruption error is reported during the installation or upgrade or post-upgrade process, an alarm is raised to indicate that the RPM files are corrupted and a syslog is displayed. The alarm is automatically cleared once you replace the corrupt files with valid files.

Step 2 **show install request**

Example:

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

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

```
Install operation 8 is still in progress
```

Step 3 **show install repository**

Example:

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

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

Step 4 **show install inactive**

Example:

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

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

Step 5 Execute one of these:

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

Example:

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

or

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

The *operation_id* is that of the **install add** operation, see Install Packages, on page 18 Step Step 2, on page 21. This command can also be run from the Sys Admin mode.

The **install activate** operation makes the package configurations active on the router. Once activation begins, new features and software fixes take effect. By default, this operation runs in asynchronous mode, meaning the command executes in the background and the EXEC prompt is returned immediately. You can run the activate operation in synchronous mode by specifying the `sync` option from the CLI.

If you use an operation_id, all packages added as part of that operation are activated together. For example, if five packages were added under operation_id 8, running **install activate id 8** activates all five packages in a single step. You do not need to activate each package individually.

If an upgrade fails during activation, you can reuse the same operation_id to retry the activation after addressing the failure. Reusing the operation_id ensures that the same set of packages is activated consistently without re-adding them.

Activation does not occur instantaneously and may take some time to complete. Once activation is complete, the system reloads automatically. For restart SMU activation, the SMU takes effect when the processes impacted by the SMU are restarted.

Step 6 **show install active**

Example:

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

Displays packages that are active.

```
Node 0/RP0/CPU0 [RP]
Boot Partition: xr_lv70
Active Packages: 24
ncs5500-xr-<release-number> version=<release-number> [Boot image]
ncs5500-k9sec-1.0.0.0-<release-number>
ncs5500-mgbl-2.0.0.0-<release-number>
ncs5500-mpls-1.0.0.0-<release-number>
ncs5500-mpls-te-rsvp-1.0.0.0-<release-number>
```

```
ncs5500-infra-2.0.0.2-<release-number>.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.2-<release-number>.CSCxr22222
ncs5500-iosxr-fwding-2.0.0.5-<release-number>.CSCxr90016
ncs5500-iosxr-fwding-2.0.0.1-<release-number>.CSCxr55555
ncs5500-iosxr-fwding-2.0.0.6-<release-number>.CSCxr90017
ncs5500-dpa-1.0.0.1-<release-number>.CSCxr90002
ncs5500-dpa-1.0.0.2-<release-number>.CSCxr90004
ncs5500-dpa-fwding-1.0.0.1-<release-number>.CSCxr90005
ncs5500-k9sec-1.0.0.1-<release-number>.CSCxr80008
ncs5500-os-support-1.0.0.1-<release-number>.CSCxr90013
ncs5500-os-support-1.0.0.2-<release-number>.CSCxr90014
ncs5500-fwding-1.0.0.2-<release-number>.CSCxr90011
ncs5500-fwding-1.0.0.5-<release-number>.CSCxr90019
ncs5500-fwding-1.0.0.1-<release-number>.CSCxr90010
ncs5500-fwding-1.0.0.4-<release-number>.CSCxr90018
ncs5500-mgbl-2.0.0.2-<release-number>.CSCxr80009
ncs5500-mpls-1.0.0.1-<release-number>.CSCxr33333
ncs5500-mpls-te-rsvp-1.0.0.2-<release-number>.CSCxr33335
```

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

Table 5: Example: Installing Packages: Related Commands

Related Commands	Purpose
show install log	Displays the log information for the install process; this can be used for troubleshooting in case of install failure.
show install package	Displays the details of the packages that have been added to the repository. Use this command to identify individual components of a package.
install prepare	Makes pre-activation checks on an inactive package, to prepare it for activation.
show install prepare	Displays the list of package that have been prepared and are ready for activation.

Step 7 **install commit**

Example:

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

Commits the Host, XR, and System Admin newly active software.

Note
On Multi-SDR mode, you can use the **install commit sdr** to commit just the sdr from where the CLI is being triggered. For more information, see Secure Domain Router Commands.

What to do next

- After performing a system upgrade, upgrade FPD by using the **upgrade hw-module location all fpd all** command from the System Admin EXEC mode. The progress of FPD upgrade process can be monitored using the **show hw-module fpd** command in the System Admin EXEC mode. Reload the router after the FPD upgrade is completed.
- Verify the installation using the **install verify packages** command.

- Uninstall the packages or SMUs if their installation causes any issues on the router. See Uninstall PackagesUninstall Packages, on page 25.

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

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

Note During the installation process, on receiving a card reload request, the SDR manager destroys VMs sequentially one after the other. The SDR manager, in turn, requests the process manager for a graceful shutdown of the XR VMs within the 30-second timeout interval for each XR VM. If the shelf manager timer starts for chassis reload within the shutdown timeout interval of the associated XR VMs and if the reload request for any XR VM is queued, it causes a delay in processing the reload request for this XR VM. As a result, when you run the **show reboot history** command, you can see missing reboot information for the XR VM for which the reload request is delayed. Therefore, always check the reboot history of the admin VM (**show reboot-history admin-vm**) to obtain complete reboot information of the VMs associated with the card reload process.

This example provides the reboot history of the admin VM.

```
RP/0/RP0/CPU0:router# admin
Thu Jan 16 18:06:34.763 IST
Last login: Thu Jan 16 09:48:21 2025 from 192.0.0.4

test2 connected from 192.0.0.4 using ssh on sysadmin-vm:0_RP0
sysadmin-vm:0_RP0# show vm
Thu Jan  16 12:36:41.760 UTC+00:00

Location: 0/RP0
Id                Status        IP Address       HB Sent/Recv
--------------------------------------------------------------
sysadmin          running       192.0.0.1        NA/NA
default-sdr       running       192.0.0.4        4152882/4152882

sysadmin-vm:0_RP0# show reboot-history admin-vm
Thu Jan  16 12:40:10.814 UTC+00:00

Admin VM Reboot History for 0/0

Admin VM Reboot History for 0/1

Admin VM Reboot History for 0/2

Admin VM Reboot History for 0/3

Admin VM Reboot History for 0/RP0

Admin VM Reboot History for 0/FT0

Admin VM Reboot History for 0/FT1

Admin VM Reboot History for 0/FT2

Admin VM Reboot History for 0/PM1

Admin VM Reboot History for 0/SC0
sysadmin-vm:0_RP0#
```

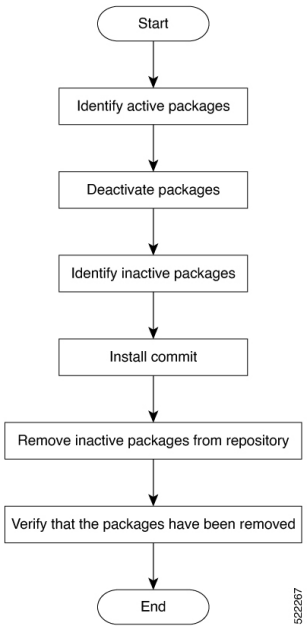
Uninstall Packages

Complete this task to uninstall a package. All router functionalities that are part of the uninstalled package are deactivated. Packages that are added in the XR VM cannot be uninstalled from the System Admin VM. However, the cross VM operation allows System Admin packages to be deactivated from XR as well.

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

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

Figure 2: Uninstalling Packages Workflow



This task uninstalls XR VM packages. If you need to uninstall System Admin packages, run the same commands from the System Admin EXEC mode.

Procedure

Step 1 **show install active**

Example:

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

Displays active packages. Only active packages can be deactivated.

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

```
ncs5500-iosxr-fwding-2.0.0.5-r600.CSCxr90016
ncs5500-iosxr-fwding-2.0.0.1-r600.CSCxr55555
ncs5500-iosxr-fwding-2.0.0.6-r600.CSCxr90017
ncs5500-dpa-1.0.0.1-r600.CSCxr90002
ncs5500-dpa-1.0.0.2-r600.CSCxr90004
ncs5500-dpa-fwding-1.0.0.1-r600.CSCxr90005
ncs5500-k9sec-1.0.0.1-r600.CSCxr80008
ncs5500-os-support-1.0.0.1-r600.CSCxr90013
ncs5500-os-support-1.0.0.2-r600.CSCxr90014
ncs5500-fwding-1.0.0.2-r600.CSCxr90011
ncs5500-fwding-1.0.0.5-r600.CSCxr90019
ncs5500-fwding-1.0.0.1-r600.CSCxr90010
ncs5500-fwding-1.0.0.4-r600.CSCxr90018
ncs5500-mgbl-2.0.0.2-r600.CSCxr80009
ncs5500-mpls-1.0.0.1-r600.CSCxr33333
ncs5500-mpls-te-rsvp-1.0.0.2-r600.CSCxr33335
```

Step 2 Execute one of these:

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

Example:

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

or

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

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

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

Step 3 **show install inactive**

Example:

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

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

Step 4 **install commit**

Step 5 **install remove** *package_name*

Example:

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

The inactive packages are removed from the repository.

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

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

Step 6 **show install repository**

Example:

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

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

What to do next

Install required packages. .

View Features and Capabilities Supported on a Platform

Table 6: Feature History Table

Feature Name	Release Information	Description
View Features and Capabilities Supported on a Platform	Release 7.5.2	This functionality displays a list of supported and unsupported features and their capabilities in a release for your router. With this feature, you are better equipped to plan your network configuration with features annotated for their support information. This feature introduces the **show features** command.

This feature provides an answer to the question `Is feature X supported on my router?`

You can determine whether a feature and their capabilities are supported on your router for the release. The support information is based on the release and platform-specific data such as platform variants, RP, or LC present on the router.

Note In Cisco IOS XR Software Release 7.5.2, only the capabilities for Access Control List (ACL) feature is supported.

The functionality to determine the capabilities information is enabled by default when the supported release is installed on the router.

Use the **show features** command to view the list of supported features and their capabilities. The feature capabilities are displayed in a tree structure with notations for the support information. For example, in ACL, the capability to use compression to accommodate a large number of Access Control Elements (ACEs) is supported, whereas IPv6 ACL BNG does not have support data in Cisco IOS XR Software Release 7.5.2. This support information about the feature is represented with the following key in the tree structure:

Key	Capability Support Information	Description
X	Unsupported	The feature capability is not supported on the platform for the release
-	Supported	The feature capability is supported on the platform for the release

Key	Capability Support Information	Description
?	Support unknown	The support for the feature capability is unknown on the platform for the release. This data could be because the optional package for the feature is not installed on the router.
*	Support data not available	The support for the feature capability is not available on the platform for the release. This data could be because the feature may be specific to a line card that is not present on the router.

View the List of Supported Features

In this example, the supported features on the router are displayed.

Note In Cisco IOS XR Software Release 7.5.2, only the feature capabilities for Access Control List (ACL) are supported.

```
Router#show features
Fri June 3 19:16:58.298 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Cisco IOS XR
|--[-] XR Protocols
|  |--[-] XR Base Protocols
|  |  |--[-] Services
|  |  |  |--[-] Access Control List (ACL)
|  |  |  |  |--[-]  IPv6 ACL Support
|  |  |  |  |  |--[*] IPv6 ACL ABF Track
|  |  |  |  |  |--[*] IPv6 ACL BNG
|  |  |  |  |  |--[*] IPv6 ACL Chaining (Meta ACL)
|  |  |  |  |  |--[-] IPv6 ACL Common ACL
|  |  |  |  |  |--[-] IPv6 ACL Compression
|  |  |  |  |  |--[*] IPv6 ACL Default ABF
|  |  |  |  |  |--[*] IPv6 ACL Fragment
|  |  |  |  |  |--[-] IPv6 ACL ICMP Off
|  |  |  |  |  |--[-] IPv6 ACL ICMP Protocol
|  |  |  |  |  |--[-] IPv6 ACL Interface Statistics
|  |  |  |  |  |--[-] IPv6 ACL Log Rate
|  |  |  |  |  |--[-] IPv6 ACL Log Threshold
|  |  |  |  |  |--[-] IPv6 ACL Logging
|  |  |  |  |  |--[-] IPv6 ACL MIB
|  |  |  |  |  |--[-] IPv6 ACL Object Groups (Scale)
|  |  |  |  |  |--[-] IPv6 ACL Police
|  |  |  |  |  |--[-] IPv6 ACL Priority
|  |  |  |  |  |--[*] IPv6 ACL Protocol Range
|  |  |  |  |  |--[-] IPv6 ACL Set Qos-Group
|  |  |  |  |  |--[-] IPv6 ACL Set TTL
|  |  |  |  |  |--[-] IPv6 ACL TCP Flags
|  |  |  |  |  |--[-] IPv6 ACL TTL Match
|  |  |  |  |  |--[-] IPv6 ACL UDF
|  |  |  |  |--[-] ES-ACL Support (L2 ACL)
```

```
|   |   |   |   |--[-] IPv4 ACL Support
|   |   |   |   |   |--[-] IPv4 ACL  Set Qos-group
|   |   |   |   |   |--[*] IPv4 ACL ABF Track
|   |   |   |   |   |--[*] IPv4 ACL BNG
|   |   |   |   |   |--[*] IPv4 ACL Chaining (Meta ACL)
|   |   |   |   |   |--[-] IPv4 ACL Common ACL
|   |   |   |   |   |--[-] IPv4 ACL Compression
|   |   |   |   |   |--[*] IPv4 ACL Default ABF
|   |   |   |   |   |--[*] IPv4 ACL Fragment
|   |   |   |   |   |--[-] IPv4 ACL Fragment Flags
|   |   |   |   |   |--[-] IPv4 ACL ICMP Off
|   |   |   |   |   |--[-] IPv4 ACL ICMP Protocol
|   |   |   |   |   |--[-] IPv4 ACL Interface Statistics
|   |   |   |   |   |--[-] IPv4 ACL Log Rate
|   |   |   |   |   |--[-] IPv4 ACL Log Threshold
|   |   |   |   |   |--[-] IPv4 ACL Logging
|   |   |   |   |   |--[-] IPv4 ACL MIB
|   |   |   |   |   |--[-] IPv4 ACL Object Groups (Scale)
|   |   |   |   |   |--[-] IPv4 ACL Police
|   |   |   |   |   |--[-] IPv4 ACL Priority
|   |   |   |   |   |--[*] IPv4 ACL Protocol Range
|   |   |   |   |   |--[-] IPv4 ACL Set TTL
|   |   |   |   |   |--[-] IPv4 ACL TCP Flags
|   |   |   |   |   |--[-] IPv4 ACL TTL
|   |   |   |   |   |--[-] IPv4 ACL UDF
|   |   |   |   |--[-] IPv4 Prefix-List
|   |   |   |   |--[-] IPv6 Prefix-List
```

View the List of Supported ACL Features

In this example, the capabilities for ACL features on the router are displayed.

```
Router#show features acl
Fri June 3 19:17:31.635 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Access Control List (ACL)
|--[-]  IPv6 ACL Support
|   |--[*] IPv6 ACL ABF Track
|   |--[*] IPv6 ACL BNG
|   |--[*] IPv6 ACL Chaining (Meta ACL)
|   |--[-] IPv6 ACL Common ACL
|   |--[-] IPv6 ACL Compression
|   |--[*] IPv6 ACL Default ABF
|   |--[*] IPv6 ACL Fragment
|   |--[-] IPv6 ACL ICMP Off
|   |--[-] IPv6 ACL ICMP Protocol
|   |--[-] IPv6 ACL Interface Statistics
|   |--[-] IPv6 ACL Log Rate
|   |--[-] IPv6 ACL Log Threshold
|   |--[-] IPv6 ACL Logging
|   |--[-] IPv6 ACL MIB
|   |--[-] IPv6 ACL Object Groups (Scale)
|   |--[-] IPv6 ACL Police
|   |--[-] IPv6 ACL Priority
|   |--[*] IPv6 ACL Protocol Range
|   |--[-] IPv6 ACL Set Qos-Group
|   |--[-] IPv6 ACL Set TTL
```

```
|  |--[-] IPv6 ACL TCP Flags
|  |--[-] IPv6 ACL TTL Match
|  |--[-] IPv6 ACL UDF
|--[-] ES-ACL Support (L2 ACL)
|--[-] IPv4 ACL Support
|  |--[-] IPv4 ACL  Set Qos-group
|  |--[*] IPv4 ACL ABF Track
|  |--[*] IPv4 ACL BNG
|  |--[*] IPv4 ACL Chaining (Meta ACL)
|  |--[-] IPv4 ACL Common ACL
|  |--[-] IPv4 ACL Compression
|  |--[*] IPv4 ACL Default ABF
|  |--[*] IPv4 ACL Fragment
|  |--[-] IPv4 ACL Fragment Flags
|  |--[-] IPv4 ACL ICMP Off
|  |--[-] IPv4 ACL ICMP Protocol
|  |--[-] IPv4 ACL Interface Statistics
|  |--[-] IPv4 ACL Log Rate
|  |--[-] IPv4 ACL Log Threshold
|  |--[-] IPv4 ACL Logging
|  |--[-] IPv4 ACL MIB
|  |--[-] IPv4 ACL Object Groups (Scale)
|  |--[-] IPv4 ACL Police
|  |--[-] IPv4 ACL Priority
|  |--[*] IPv4 ACL Protocol Range
|  |--[-] IPv4 ACL Set TTL
|  |--[-] IPv4 ACL TCP Flags
|  |--[-] IPv4 ACL TTL
|  |--[-] IPv4 ACL UDF
|--[-] IPv4 Prefix-List
|--[-] IPv6 Prefix-List
```

View the List of Supported ACL Features for Specific RP

In this example, the capabilities for ACL features on the RP location `0/RP0/CPU0` are displayed.

```
Router#show features acl detail location 0/RP0/CPU0
Fri June 3 19:15:49.889 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Access Control List (ACL)
    Cisco provides basic traffic filtering capabilities with access control
    lists (also referred to as access lists). User can configure access
    control lists (ACLs) for all routed network protocols to filter protocol
    packets when these packets pass through a device. User can configure
    access lists on your device to control access to a network, access lists
    can prevent certain traffic from entering or exiting a network.
|--[-]  IPv6 ACL Support
|      IPv6 based ACL is a list of source IPv6 addresses that use Layer 3 or
|      Layer 4 information to permit or deny access to traffic. IPv6 router
|      ACLs apply only to IPv6 packets that are routed.. A filter contains the
|      rules to match the packet matches, the rule also stipulates if the
|      packet should be permitted or denied.
|  |--[*] IPv6 ACL ABF Track
|  |      IPv6 ACL ABF Track allows the user to configure a rule with track as
|  |      nexthop inside the ACL rule . ACL Based Forwarding (ABF) denotes the
|  |      ability to forward packets to another next hop router based on the
|  |      criteria defined in the rule. Track takes precedence over VRF and
```

```
|   |      IP, if present in the nexthop
|   |--[*] IPv6 ACL BNG
|   |      IPv6 ACL BNG is an ACL subscriber BNG feature. It allows the use of
|   |      ACL on dynamic template.
|   |--[*] IPv6 ACL Chaining (Meta ACL)
|   |      IPv6 ACL Chaining (Meta ACL) allows the user to apply more than one
|   |      ACL on the interface.  is known as Meta ACL or ACL chaining.
|   |--[-] IPv6 ACL Common ACL
|   |      IPv6 ACL Common allows the user to apply the ACL on the interface
|   |      using the common keyword. Using this feature the ACL won't be
|   |      applied to the specific interface but it will be common to th entire
|   |      NPU to which the interface belongs.
|   |--[-] IPv6 ACL Compression
|   |      IPv6 ACL Compression allows the user to apply the ACL on the
|   |      interface using a compression level. This helps in reducing the
|   |      hardware resources needed to program the ACL.
|   |--[*] IPv6 ACL Default ABF
|   |      IPv6 ACL Default ABF allows the user to configure a rule with
|   |      default nexthop inside the ACL rule . ACL Based Forwarding (ABF)
|   |      denotes the ability to forward packets to another next hop router
|   |      based on the criteria defined in the rule
|   |--[*] IPv6 ACL Fragment
|   |      IPv6 ACL Fragment allows the user to configure a rule with fragment
|   |      inside the ACL rule and use it as a match criteria to filter traffic.
|   |--[-] IPv6 ACL ICMP Off
|   |      IPv6 ACL ICMP Off allows the user to not genearte the ICMP error
|   |      message on a deny action. When configured it will not send the
|   |      packet to FIB to generate ICMP error message.
-------------------------- Truncated for Brevity --------------------------
```