Upgrading or Downgrading the Cisco Nexus 3600 Series NX-OS Software

This chapter describes how to upgrade or downgrade the Cisco NX-OS software. It contains the following sections:

About the Software Image

Each device is shipped with the Cisco NX-OS software. The Cisco NX-OS software consists of one NXOS software image. The image filename begins with "n3600" or "nxos," beginning with Cisco NX-OS Release 7.0(3)F3(4)] (for example, nxos.7.0.3.F3.4.bin).

Only this image is required to load the Cisco NX-OS operating system. This image runs on all Cisco Nexus 3600 Series switches.

Note Another type of binary file is the software maintenance upgrade (SMU) package file. SMUs contain fixes for specific defects. They are created to respond to immediate issues and do not include new features. SMU package files are available for download from Cisco.com and generally include the ID number of the resolved defect in the filename (for example, n9000-dk9.7.0.3.F3.4.**CSCab00001**.gbin). For more information on SMUs, see the Cisco Nexus 3600 NX-OS System Management Configuration Guide.

Recommendations for Upgrading the Cisco NX-OS Software

Cisco recommends performing a Nexus Health and Configuration Check before performing an upgrade. The benefits include identification of potential issues, susceptible Field Notices and Security Vulnerabilities, missing recommended configurations and so on. For more information about the procedure, see Perform Nexus Health and Configuration Check.

Prerequisites for Upgrading the Cisco NX-OS Software

Upgrading the Cisco NX-OS software has the following prerequisites:

- Ensure that everyone who has access to the device or the network is not configuring the device or the network during this time. You cannot configure a device during an upgrade. Use the **show configuration session summary** command to verify that you have no active configuration sessions.
- Save, commit, or discard any active configuration sessions before upgrading or downgrading the Cisco NX-OS software image on your device.

  On a device with dual supervisors, the active supervisor module cannot switch over to the standby supervisor module during the Cisco NX-OS software upgrade if you have an active configuration session.
- Ensure that the device has a route to the remote server. The device and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets. To verify connectivity to the remote server, use the **ping** command.

```
switch# ping 172.18.217.1 vrf management
PING 172.18.217.1 (172.18.217.1): 56 data bytes
64 bytes from 172.18.217.1: icmp_seq=0 ttl=239 time=106.647 ms
64 bytes from 172.18.217.1: icmp_seq=1 ttl=239 time=76.807 ms
64 bytes from 172.18.217.1: icmp_seq=2 ttl=239 time=76.593 ms
64 bytes from 172.18.217.1: icmp_seq=3 ttl=239 time=81.679 ms
64 bytes from 172.18.217.1: icmp_seq=4 ttl=239 time=76.5 ms

--- 172.18.217.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 76.5/83.645/106.647 ms
```

For more information on configuration sessions, see the *Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*.

Cisco NX-OS Software Upgrade Guidelines

Note The Cisco Nexus 3600 Series NX-OS Release Notes contain specific upgrade guidelines for each release. See the Release Notes for the target upgrade release before starting the upgrade.

Before attempting to upgrade to any software image, follow these guidelines:

- Schedule the upgrade when your network is stable and steady.

- Avoid any power interruption, which could corrupt the software image, during the installation procedure.
- Perform the installation on the active supervisor module, not the standby supervisor module.
- To upgrade from any release prior to Cisco NX-OS Release 7.0(3)F3(4), you must perform a write erase and reload the device. To upgrade from Cisco NX-OS Release 7.0(3)F3(4) to any later release, we recommend that you use the **install all** command, although we also support changing the boot variables and reloading the device.
- If you upgrade from a Cisco NX-OS release that supports the CoPP feature to a Cisco NX-OS release that supports the CoPP feature with additional classes for new protocols, you must either run the setup utility using the **setup** command or use the **copp profile** command for the new CoPP classes to be available. For more information on these commands, see the "Configuring Control Plane Policing" chapter in the Cisco Nexus 3600 Series NX-OS Security Configuration Guide.
- When you upgrade from an earlier release to a Cisco NX-OS release that supports switch profiles [beginning with Cisco NX-OS Release 7.0(3)F3(1)], you have the option to move some of the running-configuration commands to a switch profile. For more information, see the Cisco Nexus 3600 Series NX-OS System Management Configuration Guide.
- Make sure that both vPC peers are in the same mode (regular mode or enhanced mode) before performing a nondisruptive upgrade.

Note ISSU is not supported on Cisco Nexus 3600 platform switches.

- The fast reload feature is not supported on Cisco Nexus 3600 platform switches.

Upgrading the Cisco NX-OS Software

Use this procedure to upgrade from a Cisco NX-OS 7.x release to a later 7.x release.

Step 1 **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 3600 Series NX-OS Release Notes.

Step 2 Log in to the device on the console port connection.

Step 3 Ensure that the required space is available for the image file to be copied.

```
switch# dir bootflash:
 4096    May 21 14:49:07 2018  .rpmstore/
 4096    Aug 01 06:32:42 2017  .swtam/
 843257856    Feb 24 14:15:54 2018  nxos.7.0.3.F3.3.bin
```

Note We recommend that you have the image file for at least one previous release of the Cisco NX-OS software on the device to use if the new image file does not load successfully.

Step 4 If you need more space on the active supervisor module, delete unnecessary files to make space available.

```
switch# delete bootflash:nxos.7.0.3.F3.2.bin
```

Step 5 Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Step 6 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/nxos.7.0.3.F3.4.bin
bootflash:nxos.7.0.3.F3.4.bin
```

Step 7 Display the SHA256 checksum for the file to verify the operating system integrity and ensure that the downloaded image is safe to install and use.

```
switch# show file bootflash://sup-1/nxos.7.0.3.F3.4.bin sha256sum
5214d563b7985ddad67d52658af573d6c64e5a9792b35c458f5296f954bc53be
```

Step 8 Upgrade the Cisco NX-OS software using the **boot nxos bootflash:***filename* command.

```
switch# boot nxos bootflash:nxos.7.0.3.F3.4.bin
```

Step 9 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

Step 10 Erase the startup configuration file.

```
switch# write erase
```

Step 11 Reload the switch.

```
switch# reload
```

Step 12 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```

Step 13 (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

Prerequisites for Downgrading the Cisco NX-OS Software

Downgrading the Cisco NX-OS software has the following prerequisites:

- Before you downgrade from a Cisco NX-OS release that supports the Control Plane Policing (CoPP) feature to an earlier Cisco NX-OS release that does not support the CoPP feature, you should verify compatibility using the **show incompatibility nxos bootflash:***filename* command. If an incompatibility exists, disable any features that are incompatible with the downgrade image before downgrading the software.

Cisco NX-OS Software Downgrade Guidelines

Before attempting to downgrade to an earlier software release, follow these guidelines:

- Software downgrades must be performed by doing a write erase and reloading the device.
-
- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software downgrade. See the Hardware Installation Guide for your specific chassis.
- Cisco NX-OS automatically installs and enables the guest shell by default. However, if the device is reloaded with a Cisco NX-OS image that does not provide guest shell support, the existing guest shell is automatically removed and a %VMAN-2-INVALID_PACKAGE message is issued. As a best practice, remove the guest shell with the **guestshell destroy** command before downgrading to an earlier Cisco NX-OS image.
- You must delete the switch profile (if configured) when downgrading from a Cisco NX-OS release that supports switch profiles to a release that does not. For more information, see the Cisco Nexus 3600 Series NX-OS System Management Configuration Guide.

Note Software downgrades are disruptive. In-service software downgrades (ISSDs), also known as nondisruptive downgrades, are not supported.

Downgrading to an Earlier Software Release

Step 1 **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 3600 NX-OS Release Notes.

Step 2 Log in to the device on the console port connection.

Step 3 Verify that the image file for the downgrade is present on the active supervisor module bootflash:.

```
switch# dir bootflash:
4096    May 21 14:49:07 2018  .rpmstore/
4096    Aug 01 06:32:42 2017  .swtam/
843257856    Feb 24 14:15:54 2018  nxos.7.0.3.F3.4.bin
```

Step 4 If the software image file is not present, log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Note If you need more space on the active or standby supervisor module bootflash, use the **delete bootflash:** command to remove unnecessary files.

Step 5 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/bootflash:nxos.7.0.3.F3.3.bin
```

Step 6 Check for any software incompatibilities.

```
switch# show incompatibility-all nxos bootflash:nxos.7.0.3.F3.3.bin
Checking incompatible configuration(s)
No incompatible configurations
```

The resulting output displays any incompatibilities and remedies.

Step 7 Disable any features that are incompatible with the downgrade image.

Step 8 Power off any unsupported modules.

```
switch# poweroff module module-number
```

Step 9 Downgrade the Cisco NX-OS software.

```
switch# boot nxos bootflash:nxos.7.0.3.F3.3.bin
```

Step 10 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

Step 11 Erase the startup configuration file.

```
switch# write erase
```

Step 12 Reload the switch.

Example:

```
switch# reload
```

Step 13 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```