



Upgrading or Downgrading the Cisco Nexus 3000 Series NX-OS Software

This document describes how to upgrade or downgrade the Cisco NX-OS software on Cisco Nexus 3000 Series switches.

- [Information About Software Images, on page 1](#)
- [Supported Hardware, on page 2](#)
- [About ISSU, on page 2](#)
- [Compact Image for Cisco Nexus 3000, 3100, and 3500, on page 4](#)
- [Booting the Switch from the USB, on page 7](#)
- [Upgrading the BIOS and Power Sequencer Images, on page 7](#)
- [Guidelines for Upgrading in Fast-Reload Scenarios, on page 8](#)
- [Guidelines for Upgrading in Non-Fast Reload Scenarios, on page 9](#)
- [Upgrade Prerequisites, on page 9](#)
- [Pre-Installation Checks, on page 11](#)
- [Information About Fast Reboot, on page 12](#)
- [Using the Fast-Reload Command, on page 14](#)
- [Upgrading and Downgrading Using Fast Reboot, on page 17](#)
- [Upgrading Procedures, on page 18](#)
- [Upgrade Process for vPCs, on page 22](#)
- [Monitoring the Upgrade Status, on page 27](#)
- [NX-OS Upgrade History, on page 27](#)
- [Downgrading from a Higher Release, on page 28](#)
- [Troubleshooting Installations, on page 29](#)

Information About Software Images

Cisco Nexus 3000 Series switches are shipped with the Cisco NX-OS software preinstalled on the switches. Before upgrading or downgrading from an existing image, you should read through the information in this document to understand the guidelines, prerequisites, and procedures for upgrading the software. For updated information about the Cisco NX-OS software for Cisco Nexus 3000 Series switches, see the [Cisco Nexus 3000 Series Release Notes](#).

The Cisco NX-OS software consists of one Cisco NX-OS software image. The image filename begins with "nxos." Only this image is required to load the Cisco NX-OS operating system. This image runs on all the

Cisco Nexus 3000 and 3100 Series switches. Using the **install all** command is the only supported method of upgrading to new releases.



Note There is a single image for booting the Cisco Nexus 3000 Series switches. The kickstart and system images are not required. Due to a single image binary, the following commands are updated:

- **boot nxos** *single_image_binary*
- **install all nxos** *single_image_binary*

Supported Hardware

Cisco Nexus 3000 and 3100 Series switches are shipped with the Cisco NX-OS software preinstalled. Cisco NX-OS upgrades and downgrades are supported on the hardware listed in the following sections:

Cisco Nexus 3000 Series Switches

- Cisco Nexus 3016 switches
- Cisco Nexus 3048 switches
- Cisco Nexus 3064 switches

Cisco Nexus 3100 Series Switches

- Cisco Nexus 3132Q and 3132Q-XL switches
- Cisco Nexus 3172 switches



Note For software upgrade and downgrade information for Cisco Nexus 3000 Series switches that operate in N9K mode, see the [Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide](#).

About ISSU

An in-service software upgrade (ISSU) allows you to upgrade the device software while the switch continues to forward traffic. An ISSU reduces or eliminates the downtime typically caused by software upgrades. You can perform an ISSU, also known as a nondisruptive upgrade, for some switches. (See the "Guidelines and Limitations for ISSU" section for a list of supported platforms.)

ISSU Prerequisites

Follow the guidelines in the "Guidelines and Limitations for ISSU" section to ensure that the ISSU works smoothly.

Make sure that the network is stable and no changes are made while the ISSU is in progress.

Ensure feature compatibility between the current running release and the target release.

Make sure that interfaces are not in a spanning-tree designated forwarding state. Also, make sure that bridge assurance is not configured on any interface. The vPC peer-link is an exception to these requirements.

Verify that the current STP topology is consistent with the ISSU requirements. Use the **show spanning-tree issu-impact** command to display the STP configuration and whether or not there are potential STP issues.

Use the **show lacp issu-impact** command to display if a port or a peer switch is configured in the rate fast mode. The ISSU process is aborted if the system has any LACP fast timers configured.

Before performing an ISSU to Cisco NX-OS Release 9.3(1), you must configure the BGP graceful restart timer to 180 seconds for Cisco Nexus 3132Q-XL, 3172PQ-XL, and 3172TQ-XL platform switches.

Guidelines and Limitations for ISSU

The following is a list of important guidelines and limitations for ISSU:

- Non-disruptive standard ISSU on Cisco Nexus 3172PQ, 3172TQ, 3132Q, 3132Q-X, 3064, 3064-X, 3064-T, 3048, 3016 (4 GB low-memory platforms) is not supported to Cisco Nexus 9.3(1) and later releases.
- Cisco Nexus 3132Q-XL, 3172PQ-XL, and 3172TQ-XL switches support an ISSU to Cisco NX-OS Release 9.3(1) and later releases. For more information, see the [ISSU Support Matrix](#).
- Beginning with Cisco NX-OS Release 7.0(3)I5(1), Cisco Nexus 3000 series platforms with 16 GB or higher memory support enhanced ISSU. The upgrade will be disruptive.
- Enhanced ISSU in fallback mode from earlier releases to Cisco NX-OS Release 9.3(1) is not supported. Beginning with Cisco NX-OS Release 9.3(1), Cisco Nexus 3164Q, C31108PC-V, C31108TC-V, C3132Q-V support enhanced ISSU in fallback mode only. For more details, see the [ISSU Support Matrix](#).
- The Cisco Nexus 3264C-E switch does not support the enhanced ISSU mode fallback feature from Cisco NX-OS Release 9.3(1) to any future 9.3(x) releases.
- For any prior release version upgrading to 9.3(5) using ISSU, if the following logging level commands are configured, they are missing in the upgraded version and must be reconfigured:
 - **logging level evmc** *value*
 - **logging level mvsh** *value*
 - **logging level fs-daemon** *value*
- For any prior release version upgrading to Cisco NX-OS Release 9.3(6) using ISSU, if the following logging level commands are configured, they are missing in the upgraded version and must be reconfigured:
 - **logging level evmc** *value*
 - **logging level mvsh** *value*
- You can perform an ISSU for segment routing or VXLAN.
- The minimum free bootflash space required to perform an ISSU is 550 MB.
- The CLI and the SNMP configuration change requests are denied during ISSU operations.

- STP topology changes are not expected during an ISSU.
- The Guest Shell is disabled during an ISSU, and it is reactivated after the upgrade. During an ISSU, all First-Hop Redundancy Protocols (FHRPs) cause the other peer to become active if the node undergoing the ISSU is active.
- An ISSU is blocked if **boot poap enable** is configured.
- Upgrading from Cisco NX-OS Release 9.3(1), 9.3(2), or 9.3(3) to a higher release, with Embedded Event Manager (EEM) configurations saved to the running configuration, may cause a DME error to be presented. The error is in the output of the **show consistency-checker dme running-config enhanced** command, specifically, the event manager commands. If this occurs, delete all EEM applet configurations after completing the ISSU, then reapply the EEM configurations.
- Cisco Nexus 3048, 3064, 3132, and 3172 switches with a model number that does not end in **-XL** must run a compact NX-OS software image due to limited bootflash space. This compact image can be created using the NX-OS Compact Image procedure; alternatively, a compact NX-OS software image can be downloaded directly from [Cisco's Software Download website](#). This requirement does not apply to any other model of Nexus 3000 or 3100 series switch.
 - The MD5/SHA512 checksum published on [Cisco's Software Download website](#) for a compact NX-OS software image may not match the MD5/SHA512 checksum of a compact image created through the NX-OS Compact Image procedure.

Compact Image for Cisco Nexus 3000, 3100, and 3500

Early models of Cisco Nexus 3000, 3100, and 3500 Series switches with a model number that does not end in **-XL** have 1.4 to 1.6 gigabytes of storage space allocated to the bootflash. Over time, the file size of NX-OS software images has steadily increased to be over 1 gigabyte. As a result, it is difficult for Nexus 3000, 3100, and 3500 Series switches with a model number that does not end in **-XL** to simultaneously store more than one full NX-OS binary image at a time. Therefore, administrators cannot follow the standard NX-OS software upgrade procedure on Nexus 3000, 3100, and 3500 Series switches with a model number that does not end in **-XL** that is used for other Nexus platforms, such as Nexus 5000, 6000, 7000, and 9000 Series switches.

Starting with NX-OS software release 7.0(3)I3(1), the file size of NX-OS software images can be reduced through the NX-OS Compact Image procedure. This is a non-disruptive procedure that does not affect the switch's control plane or ability to forward data plane traffic.

Compact NX-OS Software Images on Cisco's Software Download Website

Compact NX-OS software images are available for download on [Cisco's Software Download website](#) for a few NX-OS software releases. These compact images have a published MD5/SHA512 checksum that can be used to verify the integrity of the NX-OS binary image file. The compact NX-OS software images can be downloaded from [Cisco's Software Download website](#) for the following NX-OS software releases:

- 9.3(4) and later
- 9.2(4)
- 7.0(3)I7(8) and later



Note The MD5/SHA512 checksum published on [Cisco's Software Download website](#) for a compact NX-OS software image may not match the MD5/SHA512 checksum of a compact image created through the NX-OS Compact Image procedure.

Compact Image to be Run for Different Switch Models

The following table describes the appropriate compact image to be run for each applicable model of switch, using NX-OS software release 9.3(6) as an example.

Table 1: Compact Image Table for Each Cisco Nexus 3000, 3100, and 3500 Series Platform

| Switch Model Number | Compact NX-OS Software Image Filename |
|---------------------|---------------------------------------|
| N3K-C3016Q-40GE | n3000-compact.9.3.6.bin |
| N3K-C3048TP-1GE | n3000-compact.9.3.6.bin |
| N3K-C3064PQ-10GX | n3000-compact.9.3.6.bin |
| N3K-C3064TQ-10GT | n3000-compact.9.3.6.bin |
| N3K-C3064TQ-32T | n3000-compact.9.3.6.bin |
| N3K-C3132Q-40GE | n3100-compact.9.3.6.bin |
| N3K-C3132Q-40GX | n3100-compact.9.3.6.bin |
| N3K-C3172PQ-10GE | n3100-compact.9.3.6.bin |
| N3K-C3172TQ-10GT | n3100-compact.9.3.6.bin |
| N3K-C3172TQ-32T | n3100-compact.9.3.6.bin |
| N3K-C3524P-10G | n3500-compact.9.3.6.bin |
| N3K-C3524P-10GX | n3500-compact.9.3.6.bin |
| N3K-C3548P-10G | n3500-compact.9.3.6.bin |
| N3K-C3548P-10GX | n3500-compact.9.3.6.bin |

NX-OS Compact Image Procedure

There are two ways to initiate the NX-OS Compact Image procedure. The following subsections describe each option in further detail.

NX-OS Compact Image Procedure on Bootflash/USB

Starting with NX-OS software release 7.0(3)I3(1), you can use the `install all` command with the `compact` option to initiate the NX-OS Compact Image procedure on an image stored in the switch's bootflash or an attached USB drive. This can also be performed on an NX-OS software image that the switch is currently

booted from - however, a minimum of 750MB of free space on the switch's bootflash is required to compact the currently booted image.

An example of how to initiate the NX-OS Compact Image procedure on an NX-OS software image stored on the switch's bootflash is as follows:

```
switch# install all nxos bootflash:nxos.7.0.3.I7.8.bin compact
```

NX-OS Compact Image Procedure Through SCP

Starting with NX-OS software release 7.0(3)I5(2), the NX-OS Compact Image procedure can be initiated while copying the image to the switch's bootflash or an attached USB drive with SCP (Secure Copy Protocol) using an additional option in the copy command. The compact option in the copy command overrides the bootflash space limitation as the image is compacted at the time of transferring the image to the switch's bootflash or an attached USB drive. This option is only supported with SCP - other protocols (such as SFTP [Secure File Transfer Protocol] and FTP [File Transfer Protocol]) are not supported.

An example of how to initiate the NX-OS Compact Image procedure while copying an NX-OS software image to the switch's bootflash through SCP is as follows:

```
switch# copy scp://username@192.0.2.100/nxos.7.0.3.I7.8.bin bootflash:nxos.7.0.3.I7.8.bin compact vrf management
```

NX-OS Compact Image Procedure Sequence

The sequence of compacting NX-OS software images is important. You cannot compact the currently loaded NX-OS software image if you have another NX-OS software image present on the bootflash due to the limited bootflash size of the switch.

First, you should compact the currently booted image on the bootflash using the NX-OS Compact Image Procedure on Bootflash/USB method previously described. Next, you should copy the desired NX-OS software image to the switch's bootflash using the NX-OS Compact Image Procedure through SCP method previously described, if possible. If this option is not possible, because you are upgrading to an NX-OS software release prior to 7.0(3)I5(2), you should copy the desired NX-OS software image to the switch's bootflash normally, then use the NX-OS Compact Image Procedure on Bootflash/USB method previously described to compact the image.

The minimum required free space to compact a non-booted image is 450MB of free space on the switch's bootflash. If the free space available on the switch's bootflash is less than 450MB after copying the target image, then the target image needs to be compacted using an attached USB drive or through the NX-OS Compact Image Procedure through SCP method previously described.

NX-OS Compact Image Platform Groups

The NX-OS Compact Image procedure described in this document is applicable to three separate platform groups:

- Nexus 3000 devices (N3K-C3048, N3K-C3064, and so on)
- Nexus 3100 devices (N3K-C3132, N3K-C3172, and so on)
- Nexus 3500 devices (N3K-C3524, N3K-C3548, and so on)

A compacted NX-OS binary image file can be re-used among other devices within the same platform group. However, a compact NX-OS binary image file cannot be used on devices that belong to a different platform group.

For example, consider a scenario where you have four Nexus 3000 devices of the following models:

- N3K-C3048TP-1GE
- N3K-C3064PQ-10GE
- N3K-C3172PQ-40GX
- N3K-C3548P-10G

An NX-OS binary image file compacted on the N3K-C3048TP-1GE can be transferred directly to the bootflash of the N3K-C3064PQ-10GE through a file transfer protocol of your choice (provided there is enough room on the N3K-C3064PQ-10GE). Furthermore, the N3K-C3064PQ-10GE can be upgraded with the use of this compact NX-OS binary image file through a supported method. However, the same compact NX-OS binary image file cannot be used to upgrade the N3K-C3172PQ-40GX and N3K-C3548P-10G devices. The NX-OS Compact Image procedure must be executed on both N3K-C3172PQ-40GX and N3K-C3548P-10G devices separately.

This compatibility between Nexus devices within the same platform group can be used to optimize the NX-OS software upgrade of a large number of devices. For example, if you have 100 N3K-C3048TP-1GE devices, you can use the NX-OS Compact Image procedure on a single device, then transfer the compact NX-OS binary image file to the resulting 99 devices. There is no need to perform the NX-OS Compact Image procedure on all 100 devices.

Booting the Switch from the USB

An option is provided to boot the switch from the USB using a loader prompt. For example:

```
loader> boot usb1:nxos.9.2.1.bin
```

Upgrading the BIOS and Power Sequencer Images

Changes to BIOS and power sequencers are rare; however, when they occur, they are included in the Cisco NX-OS image, and the BIOS and power sequencer are upgraded. The summary displayed by the installer during the installation process indicates the current version of the BIOS and power sequencer and the target version.



Note

After a successful power sequence upgrade, you must switch off the power to the system and then power it up.

BIOS Upgrade

See the following guidelines for the BIOS upgrade:

Cisco Nexus 3000 Series platforms require a BIOS upgrade to load Release 7.0(3)I2(1) or later images. Only BIOS versions 3.x.x are compatible with Release 7.0(3)I2(1) and later releases on all Cisco Nexus 3000 Series switches. This is taken care in the regular **install all** method of upgrade but it needs to be explicitly upgraded prior to the fast-reload upgrade.

Only after the BIOS upgrade is complete, it allows the system to perform fast-reload to the newer releases.

BIOS Versions for Each Cisco Nexus 3000 Series Platform

See the following BIOS versions for each Cisco Nexus 3000 Series platform.

Table 2: BIOS Versions Table for Each Cisco Nexus 3000 Series Platform

| Sr.No. | Switch Name | Switch Model | Latest BIOS version |
|--------|----------------------------|--------------|---------------------|
| 1. | Cisco Nexus 3132Q switch | C3132Q-40GE | 5.2.0 |
| 2. | Cisco Nexus 3132Q-X switch | C3132Q-40GX | 5.2.0 |
| 3. | Cisco Nexus 3172PQ switch | C3172PQ-10GE | 5.2.0 |
| 4. | Cisco Nexus 3172CR switch | C3172PQ-10GE | 5.2.0 |
| 5. | Cisco Nexus 3064-X switch | C3064PQ-10GX | 5.2.0 |
| 6. | Cisco Nexus 3064-TQ switch | C3064TQ-10GT | 5.0.0 |
| 7. | Cisco Nexus 3016Q switch | C3016Q-40GE | 5.0.0 |
| 8. | Cisco Nexus 3064-E switch | C3064PQ-10GE | 5.0.0 |
| 9. | Cisco Nexus 3064PQ switch | C3064PQ-FA | 5.0.0 |
| 10. | Cisco Nexus 3048TP switch | C3048TP-1GE | 5.0.0 |

Guidelines for Upgrading in Fast-Reload Scenarios

Procedure

Upgrade to a new release using fast-reload. Using fast-reload after the BIOS upgrade or using **install all** are the only supported methods of upgrading to a Cisco NX-OS 9.x release. For example:

```
switch#fast-reload nxos bootflash:nxos.9.2.1.bin
```

Example:

Note The configuration must be backed up prior to upgrading to a new release as the configuration is required for the downgrade later.

Guidelines for Upgrading in Non-Fast Reload Scenarios

Complete the following steps in the given sequence to upgrade to Cisco NX-OS Release 9.x when you are not using fast-reload:

Procedure

Perform **install all** to upgrade BIOS and also upgrade the NX-OS image to Cisco NX-OS Release 9.x. Upgrade the Cisco NX-OS software using the **install all nxos bootflash:filename [no-reload | non-disruptive | non-interruptive | serial]** command.

Example:

```
switch# install all nxos bootflash:nxos.9.2.1.bin
```

The following options are available:

- no-reload—Exits the software upgrade process before the device is reloaded.
- non-disruptive—Performs an in-service software upgrade (ISSU) to prevent the disruption of data traffic. (By default, the software upgrade process is disruptive.)
- non-interruptive—Upgrades the software without any prompts. This option skips all error and sanity checks.
- serial—Upgrades the line cards in the system one at a time. (By default, the line cards are upgraded in batches to save time.)

The configuration must be backed up prior to upgrading to a new release as the configuration is required for the downgrade later.

Upgrade Prerequisites

- Ensure that the network is stable and no changes are made while an upgrade is in progress.
- Ensure that you check for feature compatibility between the current running release and the target release.

Management Services After an Upgrade

Before the switch is reset for an upgrade, inband and management ports are brought down and are brought back up after the upgrade completes. Services that depend on the inband and management ports are impacted during this time.

Table 3: Inband and Management Ports Services Impacted During Upgrade Reset

| Service | Description |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet/SSH | When an upgrade resets the system to load the target Cisco NX-OS version, all Telnet/SSH sessions are disconnected and need to be reestablished after the upgrade completes. |
| AAA/RADIUS | Applications that leverage the AAA Service (such as login) are disabled during an upgrade, because all Network Management services are disabled during this time, this behavior is consistent. |
| HTTP | HTTP sessions to the switch are disconnected during an upgrade reboot. After the reboot, the HTTP is restarted and the switch will accept an HTTP sessions. |
| NTP | NTP sessions to and from the switch are disrupted during an upgrade reboot. After the reboot, NTP session are reestablished based on the saved startup configuration. |

Layer-2 Protocols Impact

The following table lists the upgrade impacts to Layer 2 protocols.

Table 4: Upgrade Impact to Layer 2 Protocols

| Protocol | Description |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LACP | IEEE 802.3ad provides for the default slow aging timers to be transmitted once every 30 seconds in steady state and to expire after 90 seconds. Upgrade should not impact peers that rely on LACP because the recovery time is less than 90 seconds. |
| IGMP | IGMP does not disrupt existing flows of multicast traffic that are already present, but new flows are not learned (and are dropped) until an upgrade completes. New router ports or changes to router ports are not detected during this time. |
| DCBX and LLDP | DCBX uses LLDP to exchange parameters between peer devices. Because DCBX is a link-local protocol, when the switch undergoes an upgrade, the age time is increased on all ports on the switches that are being upgraded. Manual configurations are ignored during this time. |
| CDP | During an upgrade, the time-to-live value is increased (180 seconds) if it is less than the recommended timeout value. The configuration is ignored if manually specified. |
| L2MP IS-IS | Before a switch reboots for an upgrade, the switch transmits L2 IS-IS hellos on all interfaces to prevent neighbor switches from marking routes to the upgrade switch as down. Any topology changes during this time are also not acted upon until the upgrade completes. |

Ethernet Interfaces on the Switch

To avoid link down to link up transitions during the control plane outage time, the laser is turned off for administratively up ports that are operationally down. This situation occurs during the upgrade reboot starting state. After the upgrade reboot and a stateful restart, the laser is turned back on. This action prevents the link state from transitioning from down to up during an upgrade.

Pre-Installation Checks

You should do certain sanity checks to ensure that the system is ready for an upgrade and to understand the impact of the upgrade:

- Enter the **show incompatibility** command to verify that the target image is feature-wise compatible with the current image.
- Enter the **show logging level** command to ensure that the severity level for all processes is set to 5 or below.
- Enter the **show install all impact** command to identify the upgrade impact.
- Enter the **install all** command to update to the latest Cisco NX-OS software.
- Review the installer impact analysis and choose to continue.



Note The switch might reload at this time and cause a traffic disruption.

- Monitor the installation progress.
- Verify the upgrade.
- Enter the **show install all status** command to verify the status of the installation

The following table lists the show commands that identify the impact or potential problems that may occur when performing an upgrade.

Table 5: Upgrade show Commands

| Command | Definition |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show incompatibility system | Displays incompatible configurations on the current system that will impact the upgrade version. |
| show logging level | Displays the facility logging severity level configuration. Logging levels for all processes must be set at 5 or below when performing an upgrade. Processes with a logging level greater than 5 are not displayed when you enter the show install all impact command. |
| show install all impact | Displays information that describes the impact of the upgrade. This command also displays if the upgrade is disruptive or not and if the switch needs to be rebooted and the reason why. |

You can also perform the following tasks to identify potential problems before they occur:

- Ensure that you have enough space to store the images on bootflash:
- Display incompatible configurations on the current system that will impact the upgrade version.

```
switch# show incompatibility system pccos  
No incompatible configurations
```

- Verify the impact of the upgrade.

```
switch# show install all impact nxos bootflash:nxos.9.2.1.bin
```

Information About Fast Reboot

During fast reboot, the image that runs on the CPU reloads the new image and runs it without a CPU or firmware reset. Although there is a brief disruption in traffic during fast reboot, it enables a switch to reload faster than during cold reboot.

Cisco NX-OS software allows you to use fast reboot in a non-interruptive mode. In this mode, fast reboot begins the installation process without any prompts. In this release, fast reboot also supports BGP graceful restart (GR) for compatible peers. You can trigger a fast reboot with graceful restart by using the **trigger-gr** option.

Fast Reboot Timing Requirements

Fast reboot has the following timing requirements for the configurations that it supports:

- Time taken to reset the ASIC and disrupt the data plane after control plane disruption—Less than 90 seconds, when the control plane is disrupted.
- Time taken to resume forwarding traffic—Less than 30 seconds from ASIC reset.

Fast Reboot Guidelines

Fast reboot is supported only with limited configurations and topologies. Some of supported configurations and guidelines are listed in this section. When reloading system software by using the **fast-reload** command, use the supported follow these guidelines:

- Configuration changes—You cannot enter configuration mode during a reload or an upgrade. You should save, commit, or discard any active configuration sessions before upgrading or downgrading the Cisco NX-OS software image. The active configuration session is deleted without a warning during a reload.

Use the **show configuration session summary** command to verify that there are no active configuration sessions.

```
switch# show configuration session summary  
There are no active configuration sessions
```

Ensure that you check the compatibility of configurations before using the **fast-reload** command.



Note Do not use the **fast-reload** command for upgrades that may lead to kernel or BIOS changes.

For more information on configuration sessions, see the [Cisco Nexus 3000 Series NX-OS System Management Configuration Guide](#).



Note The CLI and SNMP configuration change requests are denied.

- **Topology**—You should make topology changes such as Spanning Tree Protocol (STP) before you perform an upgrade. You should perform module installations or removals only before or after an upgrade. However, you should not make changes to the Layer 2 and routing topologies, and the default root bridge should not be configured.
- **Scheduling**—You should upgrade when your network is stable and steady. Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. You cannot configure a switch during an upgrade.
- **Space**—Verify that sufficient space is available in the location where you are copying the images. The internal bootflash requires approximately 650 MB of free space.
- **Hardware**—Avoid power interruptions during an installation procedure. Power interruptions can corrupt the software image.
- **Connectivity to remote servers**—Configure the IPv4 address or IPv6 address for the 10/100/1000 BASE-T Ethernet port connection (interface mgmt0). Ensure that the switch has a route to the remote server. The switch and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets.
- **Link Aggregation Control Protocol (LACP) fast timers**—To allow fast-reload, ensure that LACP fast timers are not configured.
- **Retrieve compatible images in one of two ways:**
 - **Locally**—Images are locally available on the switch.
 - **Remotely**—Images are in a remote location and you specify the destination using the remote server parameters and the filename to be used locally.
- **Command**—Use the following commands to prepare for and install the new software:
 - Use the **ping** command to verify connectivity to the remote server.
 - Use the **dir** command to verify the required space is available for the image files to be copied.
 - Use the **show install all impact** command to identify the upgrade impact. This command also displays whether the upgrade is disruptive or the reason why the upgrade is disruptive, whether the switch needs to be rebooted, and the reason why it needs to be rebooted.



Note We recommend that you log in to the console port to begin the upgrade process.

- Between control plane disruption and data plane disruption, the CPU stops responding.
- Configuration—Fast reboot currently supports the following configuration:
 - BGP v4 and v6
 - 16-way ECMP
 - 48 downlink L2 ports
 - 4 SVIs
 - Less than 10 VLANs
 - 2000 v4 routes and 2000 v6 routes
 - RACLs
 - ARPs
 - STP edge port configuration
- Repaved fast-reload also supports the change in configurations that earlier required a complete reload, for example, portmode profile, URPF enable/disable, and TCAM re-carving.
- Do not use the **fast-reload** option for upgrade to/from a version that has reached EOL.
- The fast reload feature also supports the change in the configurations that earlier required a complete reload, for example, portmode profile, URPF enable/disable, and TCAM re-carving.
- Fast reload does not upgrade the BIOS.
- If you upgrade from a Cisco NX-OS release that does not support the CoPP feature to a release that does support the CoPP feature, you must run the setup utility after the upgrade to enable CoPP on the device.
- Fast reload upgrades are supported from Cisco NX-OS Release 7.0(3)I7(4) or 7.0(3)I7(5) to a Cisco NX-OS 9.x release.
- Beginning with Cisco NX-OS Release 9.3(10), Fast Reload support is “hidden” in the NX-OS CLI, but still available if the command is executed. Fast Reload feature is not in the Release 9.3(x) train going forward.
- Cisco removes any public documentation claiming fast reload performance of under 30 seconds for the Cisco Nexus 3164Q switches.
- If you downgrade to a release lower than Cisco NXOS release 6.0(2)U2(1) using the **install-all** command, fast reload does not work.

Using the Fast-Reload Command

The **fast-reload** command reloads Cisco Nexus 3000 or Nexus 3100 Series switches faster than the **reload** command.

ASCII configuration based fast-reload is also supported in addition to the PSS/binary configuration based fast-reload. The Cisco Nexus 3000 Series switches do not go through a complete reset with fast reload. The boards of Cisco Nexus 3000 and 3100 Series switches have two reset domains. The reset domain 1 contains the CPU, the Platform Controller Hub (PCH), the Management Ethernet controller, the PCI bridge, the OBFL, the USB, and the Fan Controller. The reset domain 2 contains the ASIC, the PHY retimers, the SFP+ modules, and the QSFP modules. Fast reload resets only the reset domain 2 and there is no reset of CPU, reload of BIOS, and firmware.

After you run the **fast-reload** command, the following sequence of events take place:

1. The switch loads the NXOS software image and upgrades the kernel. All applications undergo a stateless cold reboot and they are restarted through the startup configuration.
2. The control plane is disrupted. During control plane disruption, all control protocol communication stops. Control plane disruption is always less than 90 seconds.
3. After the control plane disruption, all control plane applications undergo a stateless cold reboot and do not retain their state. The new configuration is applied when the switch reloads.
4. The data plane is disrupted. Data plane disruption is always less than 30 seconds.
5. On the forwarding plane, all links become unavailable and the data plane does not retain its state after reload. Traffic forwarding is resumed within less than 30 seconds.



Note Ensure that you have a working image and that you analyze the impact of the fast reboot operation before using this command.

Fast Reload in PSS/Binary Configuration

Procedure

-
- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Log in to the switch. |
| Step 2 | To perform fast reboot on Cisco Nexus 3000 and 3100 Series switches, use the following command: fast-reload [save-config] [trigger-gr] [nxos bootflash:nxos-image-name] [non-interruptive] command to perform a fast reload. |
-

Fast Reload In ASCII Configuration

ASCII configuration based fast-reload is also supported in addition to the PSS/binary configuration based fast-reload.



Note The copy file startup and fast reload are supported only for specific configurations, namely Layer 3 ports with port channels, eBGP, and a few physical l2 ports having SVI only towards the hosts.

To use ASCII-file based fast reload, use the following command:

copy *configuration-file* **startup-config**

fast-reload nxos bootflash:*nxos-image-name*

The *configuration-file* is an ASCII file that contains the system configurations that fast reload uses on upgrade or fast reload. It can be copied from the remote location also. If the NXOS software image is not specified, the image existing on the switch is reloaded. If the NXOS software image provided is a higher version than the existing version, an upgrade is triggered.



Note To ensure that subsequent fast reboot operations, use the NXOS software image as the boot variables, specify the save-config option while running the fast-reload command. If the save-config option is not specified, the fast-reload command does not save the boot variables.

Fast Reload Upgrade

You can perform a faster reload and upgrade to a newer release with minimal data downtime compared to install all command.

The feature is similar to existing fast-reload support on Cisco Nexus 3000 Series switches from Release 6.0(2)U2(1) onwards with a few additional steps to upgrade BIOS before upgrading to Release 7.0(3)I2(1) or later releases.



Caution The fast-reload to Release 7.0(3)I2(1) is supported only from Release 6.0(2)U6(3a) or later releases, after the BIOS has been upgraded. Using fast-reload from Release 6.0(2)U6(3a) to Release 7.0(3)I2(1) without upgrading the BIOS will result in the switch not booting up. See BIOS upgrade for more information.



Note If guest shell or any virtual-services are enabled, the **install all** command should be used. Use the **show virtual-service list** command to verify the presence or the state of the guest shell or any virtual services..

Enabling BGP Graceful Restart with Fast Reboot

Cisco NX-OS software allows you to enable BGP graceful restarts (GR) with fast reboot. You can now use the **fast-reload trigger-gr** command to enable BGP GR. Use this command only when all BGP peers are GR-capable.

To enable BGP GR with fast reboot on Cisco Nexus 3000 and 3100 Series switches, use the following command:

fast-reload [**save-config**] [**trigger-gr**] [**nxos bootflash:***nxos-image-name*] [**non-interruptive**] command to perform a fast reload.

```
switch# fast-reload trigger-gr nxos bootflash:nxos.9.2.1.bin non-interruptive
```


Upgrading and Downgrading Using Fast Reboot

Upgrading Using Fast Reboot

You can upgrade the software on a switch by using fast reboot. To upgrade, you must specify the NXOS software image.

Before You Begin

Ensure that the version of the NXOS software image specified in the fast-reload command is higher than the version of the image currently existing on the switch.

```
switch# fast-reload nxos bootflash:nxos.9.2.1.bin
```

Downgrading Using Fast Reboot

Downgrading the system software by using fast reboot is not supported. To downgrade the image software, use the **install all** command instead of fast reboot.

Using the Install All Command

The **install all** command triggers a disruptive software install on Cisco Nexus 3000 and Nexus 3100 Series switches. The following images are upgraded during the installation:

- The NXOS software image
- System BIOS
- Power sequencers on the system

The **install all** command provides the following benefits:

- You can upgrade the Cisco Nexus 3000 Series switches by using just one command.
- You can receive descriptive information about the intended changes to your system before you continue with the installation. For example, it identifies potential disruptive upgrades.
- You can continue or cancel the upgrade when you see this question (the default is no):

```
Do you want to continue (y/n) [n]: y
```
- You can also use the **install all non-interruptive** command to install a new image without any prompts.
- The command automatically checks the image integrity, which includes the NXOS software image.
- The command performs a platform validity check to verify that a wrong image is not used.
- Pressing Ctrl + C gracefully ends the **install all** command. The command sequence completes the update step in progress and returns to the EXEC prompt.
- After entering the **install all** command, if any step in the sequence fails, the upgrade ends.
- The following message appears to warn you about the impact of upgrading the power sequencer:

```
Warning: please do not remove or power off the module at this time.
```

Note: Power-seq upgrade needs a power-cycle to take into effect.



Note After a successful power sequence upgrade, you must switch off the power to the system and then power it up.

Using the Install All Non-Interruptive Command

Cisco NX-OS software supports the use of non-interruptive **install all** command. You can now use the **install all non-interruptive** command to install a new image without any prompts.

To perform a non-interruptive install all on Cisco Nexus 3000 and 3100 Series switches, use the following command:

install all nxos bootflash: *[nxos-image-name]* **[non-interruptive]**

```
switch# install all nxos bootflash:nxos.9.2.1.bin
```

Upgrading Procedures

The upgrade process is triggered when you enter the **install all** command. This section describes the sequence of events that occur when you upgrade a single Cisco Nexus 3000 Series switch.



Note If you have a release prior to Release 7.0(3)I2(1), upgrade to Cisco Nexus 3000 Release 6.0.2.U6(3a) first and then upgrade to Release 7.0(3)I2(1) or later releases.



Note During the compatibility check, the following ISSU-related messages might appear in the Reason field:

Table 6: ISSU- related messages

| Reason Field Message — in Cisco NX-OS Release 7.0(3)I3(1) | Reason Field Message — in Cisco NX-OS Release 7.0(3)I4(1) or a Later Release | Description |
|-----------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Incompatible image | Incompatible image for ISSU | The Cisco NX-OS image to which you are attempting to upgrade does not support ISSU. |
| Hitless upgrade is not supported | Default upgrade is not hitless | By default, the software upgrade process is disruptive. You must configure the non-disruptive option to perform an ISSU. |

Installation At-A-Glance

The following table shows an overview of the upgrade process.

Table 7: Upgrade Process At-A-Glance

| | |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrade Preparation | <ol style="list-style-type: none"> 1. Log into the first Cisco Nexus 3000 Series switch. We recommend that you log into the console port. In vPC topologies, the first upgrade can be performed on either the primary or secondary switch in the topology. 2. Log into Cisco.com to access the Software Download Center. To log into Cisco.com, go to https://www.cisco.com and click Log In at the top of the page. Enter your Cisco username and password. 3. Choose and download the software image to the server. 4. Verify that the required space is available in the bootflash: directory for the image file(s) to be copied. 5. If you need more space in the bootflash: directory, delete unnecessary files to make space available. 6. Copy the Cisco NX-OS software image to the bootflash using a transfer protocol such as ftp:, http:, https:, tftp:, scp:, or sftp. Example: <pre>switch# copy scp://user@scpserver.cisco.com/download/nxos.9.3.1.bin bootflash:nxos.9.3.1.bin</pre> <p>To reduce the software image size during the copy execution, use the compact keyword. You must use SCP, HTTP, or HTTPS as the source and bootflash or USB as the destination. The following example uses SCP and bootflash:</p> <pre>switch# copy scp://user@scpserver.cisco.com/download/nxos.9.3.5.bin bootflash:nxos.9.3.5.bin compact vrf management use-kstack</pre> <pre>user1@10.65.42.196's password: nxos.9.3.5.bin 100% 1887MB 6.6MB/s 04:47 Copy complete, now saving to disk (please wait)... Copy complete.</pre> <p>Note Software image compaction is only supported on SCP, HTTP, or HTTPS. If you attempt compaction with any other protocol, the system returns the following error:</p> <pre>Compact option is allowed only with source as scp/http/https and destination as bootflash or usb</pre> <p>Note Compacted images are not supported with LXC boot mode.</p> 7. Compare the file sizes of the images that were transferred using the dir bootflash command. The file sizes of the images obtained from https://www.cisco.com and the image sizes of the transferred files should be the same. 8. Complete these steps for each switch in the topology. |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pre-upgrade Checks | <ol style="list-style-type: none"> 1. Enter the show incompatibility command to verify that the target image is feature-wise compatible with the current image. 2. Enter the show install all impact command to identify the upgrade impact. |
| Upgrade Begins | <ol style="list-style-type: none"> 1. Enter the install all command to update to the latest Cisco NX-OS software. 2. Peruse the installer impact analysis and accept to proceed. 3. The installer upgrades the software. |
| Upgrade Verification | <ol style="list-style-type: none"> 1. Enter the show install all status command to verify the status of the installation. |

Copying the Running Configuration from an External Flash Memory Device

You can copy configuration files from an external flash memory device.

Before you begin

Insert the external flash memory device into the active supervisor module.

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | (Optional) dir {usb1: usb2:}[directory] Example: <pre>switch# dir usb1:</pre> | Displays the files on the external flash memory device. |
| Step 2 | copy {usb1: usb2:}[directory/]filename{bootflash:}[directory/]filename Example: <pre>switch# copy usb1:pcco.k bootflash:pcco.k</pre> | Copies the image from an external flash memory device into the bootflash. The filename argument is case sensitive. |
| Step 3 | copy {usb1: usb2:}[directory/]filename running-config Example: <pre>switch# copy usb1:dsn-config.cfg running-config</pre> | Copies the running configuration from an external flash memory device. The filename argument is case sensitive. |
| Step 4 | (Optional) show running-config Example: <pre>switch# show running-config</pre> | Displays the running configuration. |
| Step 5 | (Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre> | Copies the running configuration to the startup configuration. |

Copying the Startup Configuration from an External Flash Memory Device

You can recover the startup configuration on your Cisco NX-OS device by downloading a new startup configuration file saved on an external flash memory device.

Before you begin

Insert the external flash memory device into the active supervisor module.

Procedure

| | Command or Action | Purpose |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | (Optional) <code>dir {usb1: usb2:}[directory/]</code> Example: <code>switch# dir usb1:</code> | Displays the files on the external flash memory device. |
| Step 2 | <code>copy {usb1: usb2:}[directory/] filename {bootflash:}[directory/]filename</code> Example: <code>switch# copy usb1:pcco.k bootflash:pcco.k.</code> | Copies the image from an external flash memory device into the bootflash. The filename argument is case sensitive. |
| Step 3 | <code>copy {usb1: usb2:}[directory/] filename startup-config</code> Example: <code>switch# copy usb1:dsn-config.cfg startup-config</code> | Copies the startup configuration from an external flash memory device. The filename argument is case sensitive. |
| Step 4 | (Optional) <code>show startup-config</code> Example: <code>switch# show startup-config</code> | Displays the startup configuration. |
| Step 5 | (Optional) <code>copy running-config startup-config</code> Example: <code>switch# copy running-config startup-config</code> | Copies the running configuration to the startup configuration. |

Upgrade Process in a Non-vPC Topology

The following list summarizes the upgrade process in a non-vPC topology:

1. The **install all** command triggers the installation upgrade.
2. The compatibility checks display the impact of the upgrade.
3. The installation proceeds or not based on the upgrade impact.
4. The current state is saved.
5. The system unloads and runs the new image.

6. The stateful restart of the system software and application occurs.
7. The installer resumes with the new image.
8. The installation completes.

The following example displays the upgrade process:

```
switch# install all nxos bootflash:<nxos-image-name>
```

Upgrade Process for vPCs

Upgrade Process for a vPC Topology on the Primary Switch

The following list summarizes the upgrade process on a switch in a vPC topology that holds either the Primary or Operational Primary vPC roles. Steps that differ from a switch upgrade in a non-vPC topology are in bold.



Note In vPC topologies, the two peer switches must be upgraded individually. An upgrade on one peer switch does not automatically update the vPC peer switch.

1. **The install all command issued on the vPC primary switch triggers the installation upgrade.**
2. The compatibility checks display the impact of the upgrade.
3. The installation proceeds or not based on the upgrade impact.
4. **The configuration is locked on both vPC peer switches.**
5. The current state is saved.
6. The system unloads and runs the new image.
7. The stateful restart of the system software and application occurs.
8. The installer resumes with the new image.
9. The installation is complete.

When the installation is complete, the vPC primary switch is upgraded.



Note The vPC primary switch is running the upgraded version, and the vPC secondary switch is running the original software version.

Upgrade Process for a vPC Topology on the Secondary Switch

The following list summarizes the upgrade process on a switch in a vPC topology that holds either the Secondary or Operational Secondary vPC roles. Steps that differ from a switch upgrade in a non-vPC topology are in bold.

1. The **install all** command issued on the vPC secondary switch triggers the installation upgrade.
2. The compatibility checks display the impact of the upgrade.
3. The installation proceeds or not based on the upgrade impact.
4. The current state is saved.
5. The system unloads and runs the new image.
6. The stateful restart of the system software and application occurs.
7. The installer resumes with the new image.
8. **The configuration is unlocked on the primary and secondary switches.**
9. The installation is complete.

vPC Upgrade and Downgrade Procedure for Nexus 9000 -R series switches

In vPC topologies, the two peer switches usually must be upgraded individually. An upgrade on one peer switch does not automatically update the vPC peer switch.

However, Cisco NX-OS Releases 7.0(3)F3(3c) and 7.0(3)F3(4) are not compatible with Cisco NX-OS Release 9.2(x) for vPC peer switches. Both vPC peers must be upgraded simultaneously to Cisco NX-OS Release 9.2(x) to avoid one switch running a 7.0(3)F3(x) release and the other switch running 9.2(x). Optionally, if the switches are being upgraded from Cisco NX-OS Release 7.0(3)F3(4), you can use the following procedure to minimize the traffic impact during upgrade.



Note This procedure not to be used on Broadcom or Cloudscale-based switches.

1. Switch A and B are running a Cisco NX-OS release. Switch A is the primary switch, and switch B is the secondary switch. Use the **copy r s** command on both switches.

```
primary_switch# show vpc role
vPC Role status
-----
vPC role : primary
vPC system-mac : 00:23:04:ee:be:64
vPC system-priority : 32667
vPC local system-mac : 70:df:2f:eb:86:1f
vPC local role-priority : 90
vPC peer system-mac : 70:df:2f:eb:1c:ab
vPC peer role-priority : 100
primary_switch#
```

```
secondary_switch# show vpc role
vPC Role status
-----
vPC role : secondary
vPC system-mac : 00:23:04:ee:be:64
vPC system-priority : 32667
vPC local system-mac : 70:df:2f:eb:1c:ab
vPC local role-priority : 100
vPC peer system-mac : 70:df:2f:eb:86:1f
vPC peer role-priority : 90
```

```
secondary_switch#

primary_switch# copy r s v
[#####] 100%
Copy complete.

secondary_switch# copy r s v
[#####] 100%
Copy complete.
```

2. Bring down the peer link (PL) on the primary switch. The secondary switch brings down its vPC legs.

```
primary_switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
primary_switch(config)# int port-channel 100
primary_switch(config-if)# shutdown

Reload the secondary switch with Release 9.2.1 image (change bootvar /reload)

secondary_switch(config)# boot nxos nxos.9.2.1.bin
Performing image verification and compatibility check, please wait....
secondary_switch(config)#
secondary_switch(config)# copy r s v
[#####] 100%
Copy complete.

secondary_switch# reload
This command will reboot the system. (y/n)? [n] y
```

```
After reload
-----
secondary_switch# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer link is down
vPC keep-alive status : peer is alive
Configuration consistency status : failed
Per-vlan consistency status : success
Configuration inconsistency reason: Consistency Check Not Performed
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role : none established
Number of vPCs configured : 20
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Disabled (due to peer configuration)
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 90s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
vPC Peer-link status
-----
id Port Status Active vlans
-- --
1 Po100 down -

secondary_switch#

primary_switch(config-if)# show vpc
Legend:
```



```
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer link is down
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 20
Peer Gateway : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs and BDs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled, timer is off.(timeout = 240s)
Operational Layer3 Peer-router : Disabled
vPC Peer-link status
-----
id Port Status Active vlans
-- ---
1 Po100 down -
```

3. Configure vPC auto-recovery under the vPC domain on the secondary switch. Enable **vpc upgrade** (exec command).

```
secondary_switch(config)# vpc domain 100
secondary_switch(config-vpc-domain)# auto-recovery
secondary_switch(config-vpc-domain)# end

secondary_switch# show running-config vpc
!Command: show running-config vpc
!Running configuration last done at: Wed May 16 06:34:10 2018
!Time: Wed May 16 06:34:14 2018
version 9.2(1) Bios:version 01.11
feature vpc
vpc domain 100
peer-switch
role priority 100
peer-keepalive destination 10.1.31.30 source 10.1.31.29
delay restore 90
peer-gateway
auto-recovery
ipv6 nd synchronize
ip arp synchronize
interface port-channel100
vpc peer-link
interface port-channel2001
vpc 101

secondary_switch# show vpc upgrade
vPC upgrade : TRUE
SVI Timer : 0
Delay Restore Timer : 0
Delay Orphan Port Timer : 0
secondary_switch#

secondary_switch# show vpc upgrade >> Hidden command
vPC upgrade : FALSE
SVI Timer : 10
Delay Restore Timer : 90
Delay Orphan Port Timer : 0
```

```
secondary_switch# vpc upgrade    >> Hidden command
```

4. After Layer 3 routes are learned on the secondary switch, reload the primary switch with the new release image. The secondary switch takes over the primary role and brings up its vPC legs in approximately 5 seconds.

```
primary_switch(config)# show boot
Current Boot Variables:
sup-1
NXOS variable = bootflash:/nxos.9.2.1.bin
No module boot variable set
Boot Variables on next reload:
sup-1
NXOS variable = bootflash:/nxos.9.2.1.bin

No module boot variable set
primary_switch(config)# end

primary_switch# show boot
Current Boot Variables:
sup-1
NXOS variable = bootflash:/nxos.9.2.1.bin
No module boot variable set
Boot Variables on next reload:
sup-1
NXOS variable = bootflash:/nxos.9.2.1.bin

No module boot variable set
primary_switch# reload
This command will reboot the system. (y/n)? [n] y

secondary_switch# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer link is down
vPC keep-alive status : peer is not reachable through peer-keepalive
Configuration consistency status : failed
Per-vlan consistency status : success
Configuration inconsistency reason: Consistency Check Not Performed
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role : primary
Number of vPCs configured : 20
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Disabled (due to peer configuration)
Auto-recovery status : Enabled, timer is off.(timeout = 240s)
Delay-restore status : Timer is off.(timeout = 0s)
Delay-restore SVI status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
vPC Peer-link status
-----
id Port Status Active vlans
-- --
1 Po100 down -
vPC status
```

5. When the primary switch comes back up, the peer link on it is operationally up.

```

primary_switch# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary, operational secondary
Number of vPCs configured : 20
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 90s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
vPC Peer-link status
-----
id Port Status Active vlans
--
1 Po100 up 1,101-400

```

For downgrade, reload both switches at the same time.

Monitoring the Upgrade Status

The following table lists the **show** commands that are used to monitor installation upgrades.

| Command | Definition |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| show install all failure-reason | Displays the applications that failed during an installation and why the installation failed. |
| show install all status | Displays a high-level log of the installation. |
| show tech-support | Displays the system and configuration information that you can provide to the Cisco Technical Assistance Center when reporting a problem. |

NX-OS Upgrade History

During the life of a Cisco Nexus 3000 switch, many upgrade procedures can be performed. Upgrades can occur for maintenance purposes or to update the operating system to obtain new features. Over time, switches may be updated on numerous occasions. Viewing the types of upgrades and when they occurred can help in troubleshooting issues or simply understanding the history of the switch.

Beginning with Cisco NX-OS Release 9.3(5), Cisco Nexus 3000 switches log all upgrade activity performed over time providing a comprehensive history of these events. The stored upgrade history types are:

- Cisco NX-OS System Upgrades
- Electronic Programmable Logic Device (EPLD) Upgrades

- Software Maintenance Upgrade (SMU) Installations

View the Cisco NX-OS upgrade history by entering the **show upgrade history** command. The output displays any upgrade activity that previously occurred on the switch and defines the start and end times for each event. The following is an example output of the **show upgrade history** command:

```
switch# show upgrade history
TYPE                VERSION  DATE                STATUS
NXOS EPLD           n3000-   26 Apr 2020 11:37:16 EPLD Upgrade completed
                   epld.9.3.4.img
NXOS EPLD           n3000-   26 Apr 2020 11:32:41 EPLD Upgrade started
                   epld.9.3.4.img
NXOS system image   9.3(5)   24 Mar 2020 20:09:10 Installation End
NXOS system image   9.3(5)   24 Mar 2020 20:05:29 Installation started
NXOS SMU            9.3(5)   03 Mar 2020 23:34:15 Patch activation ended for
                   nxos.libnbproxyccli_patch-n3k_
                   ALL-1.0.0-9.3.5.lib32_n3000.rpm
NXOS SMU            9.3(5)   03 Mar 2020 23:34:03 Patch activation started for
                   nxos.libnbproxyccli_patch-n3k_
                   ALL-1.0.0-9.3.5.lib32_n3000.rpm
```

Downgrading from a Higher Release

The procedure for entering the **install all** command to downgrade the switch is identical to using the **install all** command for a switch upgrade, except that the image files to be loaded are for an earlier release than the image that is currently running on the switch. You can use the **show incompatibility system command** to ensure that there are no feature incompatibilities between the current release and the target release. Note that downgrades are disruptive.



Note Before you downgrade to a specific release, check the release notes for the current release installed on the switch, to ensure that your hardware is compatible with the specific release. See the Cisco [Nexus 3000 Series Switch Release Notes](#) for details.



Note The following limitation applies to Cisco Nexus platform switches that support Trust Anchor Module (TAM): The TACACS global key cannot be restored when downgrading from Cisco NX-OS Release 9.3(3) to an earlier version. TAM was updated to version-7 in 9.3(3), but earlier NX-OS versions used TAM version-3.

Downgrading from a Higher Release to a Lower Release

This section contains an example for downgrading from a higher release to a lower release.



Caution Make sure that you store the configuration file for later use.

Complete the following steps to downgrade:

Procedure

- Step 1** Enter the **write erase** command.
- Step 2** Enter the **write erase boot** command.
- Step 3** Enter the **copy Release 6.0(2)U6(3a)-config startup-config** command.
- switch# **copy downgrade startup-config**
- Step 4** Enter the **install all kickstart img.kick system img.sys no-save bios-force** command
- Step 5** To verify whether the boot variables exist, enter the **show boot** command. If the boot variables do not exist, enter the following set of commands to update the boot variables manually:

```
switch# configure t  
switch (config)# boot kickstart <img.kick>  
switch (config)# boot system <img.sys>  
switch (config)# write run start
```

Note If lockup occurs on the switch, do a tftp boot.

Troubleshooting Installations

Some common causes for upgrade failure are as follows:

- The bootflash: does not have enough space to accept the updated image.
- The hardware is installed or removed while the upgrade is in process.
- A power disruption occurs while an upgrade is in progress.
- The entire path for the remote server location is not specified accurately.

