



Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 8.x

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide	2
About Software Images	2
About In-Service Software Upgrades on Devices with Dual Supervisor Modules	2
Virtualization Support	3
Parallel Upgrade	3
Prerequisites for Upgrading the Cisco NX-OS Software	4
Cisco NX-OS Software Upgrade Guidelines	5
Cisco NX-OS Software Downgrade Guidelines	103
Upgrading a Device with Dual Supervisor Modules	104
Upgrading a Device with a Single Supervisor Module	108
Performing a Traditional Upgrade or Downgrade (Chassis Reload)	111
Example Outputs from Cisco NX-OS Software Upgrades	112
Communications, Services, and Additional Information	121
Feature History for Software Upgrade and Downgrade	121

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide

This document describes how to upgrade or downgrade the Cisco NX-OS software.

About Software Images

Each device is shipped with the Cisco NX-OS software. The Cisco NX-OS software consists of two images—the kickstart image and the system image.

The software image install procedure is dependent on the following factors:

- Software images—The kickstart and system image files reside in directories or folders that you can access from the Cisco NX-OS software prompt.
- Image version—Each image file has a version.
- Flash disks on the device—The bootflash: resides on the supervisor module and the CompactFlash disk is inserted into the slot0:, usb1, or usb2: device.
- Supervisor modules—There are single or dual supervisor modules.



Note On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during upgrades and downgrades. See the [Cisco Nexus 7000 Series Hardware Installation and Reference Guide](#).

About In-Service Software Upgrades on Devices with Dual Supervisor Modules

The Cisco NX-OS software supports in-service software upgrades (ISSUs) on devices with dual supervisor modules. An ISSU can update the software images on your device without disrupting data traffic. Only control traffic is disrupted. If an ISSU will cause a disruption of data traffic, the Cisco NX-OS software warns you before proceeding so that you can stop the upgrade and reschedule it to a time that minimizes the impact on your network.

An ISSU updates the following images:

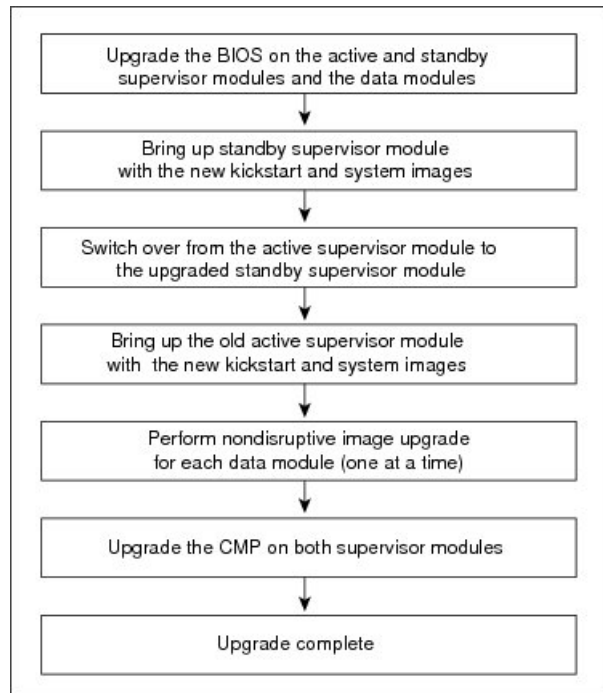
- Kickstart image
- System image
- Supervisor module BIOS
- Data module image
- Data module BIOS

- Connectivity management processor (CMP) image
- CMP BIOS



Note CMP is a Supervisor 1 only feature.

Figure 1: ISSU Process



This figure shows the ISSU process.



Note CMP is a Supervisor 1 only feature.

Virtualization Support

When you upgrade the Cisco NX-OS software, you upgrade the software for all virtual device contexts (VDCs) on the physical device. You cannot upgrade the Cisco NX-OS software for an individual VDC.

Parallel Upgrade

Parallel Upgrade with I/O Modules

Starting with Cisco NX-OS Release 5.2(1), multiple linecards can be simultaneously upgraded, and the infrastructure support is available. This decreases the ISSU time when compared with an ISSU upgrade that is done serially (one card at a time).

To start a parallel upgrade, use the following command: **install all kickstart image system image parallel**

Up to three linecards can be upgraded in parallel with this command. During the upgrade process, the upgrade of the linecards is displayed in the output as follows:

```
Non-disruptive upgrading.
[#           ] 0%
Module 5 upgrade completed successfully.
.

Module 3 upgrade completed successfully.
.

Module 6 upgrade completed successfully.
.

Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Non-disruptive upgrading.
[#           ] 0%
Module 9 upgrade completed successfully.
.

Non-disruptive upgrading.
[#####] 100% -- SUCCESS
```



Note This command will be ignored for a downgrade to a release below Cisco NX-OS Release 5.2.(1).

Parallel Upgrade with Fabric Extenders

Beginning with Cisco NX-OS Release 6.1(1), a parallel upgrade on the Fabric Extenders (FEX) is supported if the user types the parallel keyword in the command. You can perform a parallel upgrade of 10 FEXs at a time.

For releases prior to Cisco NX-OS Release 6.1(1), only a serial upgrade of FEXs is supported. The upgrade process switches to a serial upgrade even for the I/O modules present. Even if the user types the parallel keyword in the command, the upgrade will be a serial upgrade.

Prerequisites for Upgrading the Cisco NX-OS Software

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

For ISSU compatibility for all releases, see the [Cisco NX-OS ISSU Support Matrix](#).

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. On a device with a single supervisor module, the Cisco NX-OS software deletes the active configuration session without warning when you reload the device.

Use the **show configuration session summary** command to verify that you have no active configuration sessions.

For more information on configuration sessions, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

Cisco NX-OS Software Upgrade Guidelines



Note Cisco Nexus 7000 Series NX-OS Release Notes contain specific upgrade guidelines for each release. See the Release Notes document for the target upgrade release before starting the upgrade.

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

- Scheduling

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

- Space

Verify that sufficient space is available in the location where you are copying the images. This location includes the active and standby supervisor module bootflash: (internal to the device). Internal bootflash: has approximately 250 MB of free space available.

- Hardware

Avoid power interruption during any install procedure, which 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 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.

- Software images

- Ensure that the specified system and kickstart images are compatible with each other.
- If the kickstart image is not specified, the device uses the current running kickstart image.
- If you specify a different system image, ensure that it is compatible with the running kickstart image.
- Retrieve the 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.

- PowerOn Auto Provisioning (POAP)

- To support POAP to be more secure, ensure that DHCP snooping is enabled; and set the firewall rules to block unintended or malicious DHCP servers.

ISSU Paths for Cisco NX-OS Release 8.4(7)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(7).

Table 1: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(7))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(7)	8.4(6) 8.4(5) 8.4(4a) 8.4(4) 8.4(3) 8.4(2) 8.4(1) 8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(7)D1(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.4(6a)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(6a).

Table 2: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(6a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(6a)	8.4(5) 8.4(4a) 8.4(4) 8.4(3) 8.4(2) 8.4(1) 8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(9)D1(1) 7.3(8)D1(1) 7.3(7)D1(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.4(6)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(6).

Table 3: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(6))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(6)	8.4(5) 8.4(4a) 8.4(4) 8.4(3) 8.4(2) 8.4(1) 8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(7)D1(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.4(5)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(5).

Table 4: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(5))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(5)	8.4(4a) 8.4(4) 8.4(3) 8.4(2) 8.4(1) 8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(7)D1(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.4(4a)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(4a).

Table 5: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(4a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(4a)	8.4(4) 8.4(3) 8.4(2) 8.4(1) 8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.4(4)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(4).

Table 6: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(4))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(4)	8.4(3) 8.4(2) 8.4(1) 8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.4(3)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(3).

Table 7: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(3))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(3)	8.4(2) 8.4(1) 8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.4(2)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(2).

Table 8: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(2))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(2)	8.4(1) 8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.4(1)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.4(1).

Table 9: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.4(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.4(1)	8.3(2) 8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a.** ISSU from major release 8.1(1) to another major release 8.2(3).
- b.** ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c.** ISSU from major release 8.2(5) to another major release 8.4(5).
- d.** Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.3(2)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.3(2).

Table 10: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.3(2))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.3(2)	8.3(1) 8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.3(1)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.3(1).

Table 11: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.3(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.3(1)	8.2(10) 8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2)



Note ISSU from 8.2(8) to any higher releases like 8.3(1), 8.3(2), 8.4(1), 8.4(2), 8.4(3), 8.4(4), 8.4(4a) will be disruptive if M3 linecards are present.

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(10)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(10).

Table 12: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(10))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(10)	8.2(9) 8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(7)D1(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(9)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(9).

Table 13: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(9))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(9)	8.2(8) 8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(7)D1(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(8)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(8).

Table 14: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(8))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(8)	8.2(7a) 8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(7a)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(7a).

Table 15: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(7a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(7a)	8.2(7) 8.2(6) 8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(6)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(6).

Table 16: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(6))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(6)	8.2(5) 8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(6)D1(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(5)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(5).

Table 17: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(5))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(5)	8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(4)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(4).

Table 18: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(4))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(4)	8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(3)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(3).

Table 19: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(3))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(3)	8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(2)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(2).

Table 20: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(2))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(2)	8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note

1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

a. ISSU from major release 8.1(1) to another major release 8.2(3).

b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.

c. ISSU from major release 8.2(5) to another major release 8.4(5).

d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.1(2a)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.1(2a).

Table 21: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.1(2a))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.1(2a)	8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.
We recommend doing a binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.1(2)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.1(2).

Table 22: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.1(2))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.1(2)	8.1(1) 8.0(1) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.2(1)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.2(1).

Table 23: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.2(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.2(1)	8.1(1) 8.0(1) 7.3(2)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.
We recommend doing a binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.1(1)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.1(1).

Table 24: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.1(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.1(1)	8.0(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

- a. ISSU from major release 8.1(1) to another major release 8.2(3).
- b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.
- c. ISSU from major release 8.2(5) to another major release 8.4(5).
- d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.
We recommend doing a binary reload instead of upgrading.
Do you want to continue with the installation (y/n)? [n]
```

ISSU Paths for Cisco NX-OS Release 8.0(1)

See the below for the in-service software upgrade (ISSU) path to Cisco NX-OS Release 8.0(1).

Table 25: Supported ISSU Paths for the Cisco Nexus 7000 Series Platform (Cisco NX-OS Release 8.0(1))

Target Release	Current Release Supporting Direct ISSU Upgrade to Target Release
NX-OS Release 8.0(1)	7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1)

If you are doing ISSU from a release other than the non-disruptive upgrade releases listed in the above table, that ISSU is disruptive in quality and requires the switch to reload.

If two successive ISSUs are performed between major releases (Multi-hop ISSU), a switch reload is required before the second ISSU.



Note 1. Multi-hop ISSU term refers to two successive ISSUs between major releases.

2. A major release introduces significant new software features, hardware platforms.

The different major releases of Nexus 7000/7700 are 6.0.x, 6.1.x, 6.2.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x.

For example - Consider an upgrade from 8.1(1) TO 8.4(5).

The upgrade path - ISSU from 8.1(1) to 8.2(3) followed by ISSU from 8.2(3) to 8.2(5) and then followed by ISSU from 8.2(5) to 8.4(5) regardless of the timeframe.

The procedure for the ISSU upgrade path is as follows:

a. ISSU from major release 8.1(1) to another major release 8.2(3).

b. ISSU from 8.2(3) to 8.2(5) is within the same major release 8.2.x.

c. ISSU from major release 8.2(5) to another major release 8.4(5).

d. Step 1 and 3 are successive ISSUs between two different major releases. Hence before Step 3, a reload is required.

You will be prompted with the below information during the second ISSU. You must abort the ISSU, do a switch reload, and then proceed with the ISSU.

```
Multiple Major ISSU has been performed on this switch.  
We recommend doing a binary reload instead of upgrading.  
Do you want to continue with the installation (y/n)? [n]
```

In-Service Software Upgrade (ISSU)

To perform an ISSU upgrade to Cisco NX-OS Release 8.0(1) and later releases, follow these steps:

1. Enter the **show running-config aclmgr inactive-if-config** command for all VDCs.
2. Enter the **clear inactive-config acl** command for all VDCs.
3. If the configuration has any **mac packet-classify** configurations on any interfaces, remove all of the configurations by entering the **no mac packet-classify** command.
4. Start the ISSU procedure.

In-Service Software Upgrade (ISSU) Caveats

- When you perform ISSU to upgrade to a new Cisco NX-OS release, the default CoPP policy for the new release is not applied. Because you might have your own configured CoPP policy and want to continue using it, the policy for the earlier release continues to be applied. However, if you have not modified the default CoPP policy in earlier versions, it is recommended that when you install Cisco NX-OS Release 5.2 or later releases, you should apply the latest default CoPP policy for the upgrading version by using the **copp profile [strict | moderate | lenient]** command. This action removes the previous policy and applies a new CoPP policy. Note that reapplying copp profile configuration removes CoPP momentarily on the chassis for the new configuration to take into effect. Hence, this needs to be done in a maintained environment.
- ISSU upgrade from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1) with RISE configuration:

- RISE configuration must be removed prior to starting your upgrade to Cisco NX-OS Release 8.0(1). ISSU performs compatibility check and blocks the upgrade if RISE is configured.
 - If the RISE feature is not configured, there is no impact on the ISSU.
 - If the RISE feature is configured you will be prompted to remove this feature in order to proceed with the ISSU. You can proceed with the upgrade only after you disable this feature.
 - Sample CLI Output

```
"Running-config contains configuration that is incompatible with the new image (strict
incompatibility).
Please run 'show incompatibility-all system <image>' command to find out which feature needs to be
disabled.".
Pre-upgrade check failed. Return code 0x40930029 (Current running-config is not supported by new
image).
switch# show incompatibility-all system n7000-s2-dk9.8.0.1.bin

Checking incompatible configuration(s) for vdc 'switch':
-----
No incompatible configurations

Checking dynamic incompatibilities for vdc 'switch':
-----
Service : iscm , UUID: 1144 Description : Rise ISSU script Compatibility requirement: STRICT
Workaround:
ISSU from version < 8.0(1) not supported when Rise feature is enabled.
```

- ISSU upgrade from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1) with VXLAN configuration in a vPC setup: ISSU upgrade from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1) with VXLAN configuration in a vPC setup can result in a traffic loss when the second vPC peer is upgraded.

The following upgrade steps are recommended as the workaround for this issue:

- Shutdown vPC on the vPC secondary and reload with 8.0(1).
 - Perform no shut vpc after the system is operational.
 - Perform a vPC role change so that vPC secondary becomes a vPC primary.
 - Shutdown vPC on the other peer that is still running 7.3 release and reload with 8.0(1).
 - Perform no shut vpc after the system is operational.
 - Optionally, a vPC role change can be performed to get the latest peer back to vPC primary.
- If ISSU fails during a FEX module upgrade, you need to clear the flash as per the following steps and then proceed with the upgrade:
 - rlogin to the failing FEX—rlogin 192.0.2.<FEX-ID> -l root
 - umount /mnt/cfg
 - flash_eraseall /dev/mtd5
 - mount -t jffs2 -rw /dev/mtdblock5 /mnt/cfg

The **mount** command enables you to mount a file from a source folder to a destination folder.

- FCoE FEX

- Post ISSU you need to change port-channel load-balance for FEX, from default VDC, in order to apply load-balancing for SAN traffic.

Device(config)# **port-channel load-balance src-dst mac fex 101**

- You can revert back to default load-balance after changing the load-balance for FEX.
- When you perform an ISSU from Cisco NX-OS 7.3(2)D1(1) and earlier releases, and from Cisco NX-OS 8.0 release to Cisco NX-OS Release 8.1.x, then reload the FEXs after the ISSU to avoid any FCoE traffic loss.
- For details on ISSU for other earlier releases refer to the following: [Cisco Nexus 7000 Series NX-OS Release Notes, Release 7.2](#)
- For multi-hop ISSU scenario for releases earlier than Cisco NX-OS Release 7.2(0) refer to the following: [Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.2](#)

Non In-Service Software Upgrade (Non-ISSU)/Cold Boot Upgrade Steps

Cisco NX-OS Release 8.4(7) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
-----------------------	---

8.4(7)	
--------	--

8.4(6a)
8.4(6)
8.4(5)
8.4(4a)
8.4(4)
8.4(3)
8.4(2)
8.4(1)
8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(9)D1(1)
7.3(8)D1(1)
7.3(7)D1(1)
7.3(6)D1(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)

7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)
6.2(24a)
6.2(24)
6.2(22)
6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)
6.2(10)

Cisco NX-OS Release 8.4(6a) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.4(6a)	
---------	--

8.4(6)
8.4(5)
8.4(4a)
8.4(4)
8.4(3)
8.4(2)
8.4(1)
8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(9)D1(1)
7.3(8)D1(1)
7.3(7)D1(1)
7.3(6)D1(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)

7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)
6.2(24a)
6.2(24)
6.2(22)
6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)
6.2(10)

Cisco NX-OS Release 8.4(6) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.4(6)	
--------	--

8.4(5)
8.4(4a)
8.4(4)
8.4(3)
8.4(2)
8.4(1)
8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(7)D1(1)
7.3(6)D1(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)

	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(24a)
	6.2(24)
	6.2(22)
	6.2(20a)
	6.2(20)
	6.2(18)
	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)

Cisco NX-OS Release 8.4(5) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.4(5)	
--------	--

8.4(4a)
8.4(4)
8.4(3)
8.4(2)
8.4(1)
8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(6)D1(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)

7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)
6.2(24a)
6.2(24)
6.2(22)
6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)
6.2(10)

Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.4(4a) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
-----------------------	---

8.4(4a)	
---------	--

8.4(4)
8.4(3)
8.4(2)
8.4(1)
8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(6)D1(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)

7.2(1)D1(1)
7.2(0)D1(1)
6.2(24a)
6.2(24)
6.2(22)
6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)
6.2(10)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.4(4) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.4(4)	
--------	--

8.4(3)
8.4(2)
8.4(1)
8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(6)D1(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)

7.2(0)D1(1)
6.2(24a)
6.2(24)
6.2(22)
6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)
6.2(10)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.4(3) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.4(3)	
--------	--

8.4(2)
8.4(1)
8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(6)D1(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)

6.2(24a)
6.2(24)
6.2(22)
6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)
6.2(10)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.4(2) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.4(2)	
--------	--

8.4(1)
8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)
6.2(24)
6.2(22)

6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)
6.2(10)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.4(1) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.4(1)	
--------	--

8.3(2)
8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)
6.2(22)
6.2(20a)
6.2(20)
6.2(18)

	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)
	6.2(8b)
	6.2(8a)
	6.1(5a)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.3(2) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.3(2)	
--------	--

8.3(1)
8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)
6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)

	6.2(10)
	6.2(8b)
	6.2(8a)
	6.1(5a)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.3(1) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.3(1)	
--------	--

8.2(10)
8.2(9)
8.2(8)
8.2(7a)
8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(3)D1(1)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)
6.2(20)
6.2(18)
6.2(16)
6.2(14)
6.2(12)
6.2(10)
6.2(8b)
6.2(8a)

	6.1(5a)
--	---------



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.2(7a) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.2(7a)	
---------	--

8.2(7)
8.2(6)
8.2(5)
8.2(4)
8.2(3)
8.2(2)
8.2(1)
8.1(2a)
8.1(2)
8.1(1)
8.0(1)
7.3(6)D1(1)
7.3(5)D1(1)
7.3(4)D1(1)
7.3(3)D1(1)
7.3(2)D1(3a)
7.3(2)D1(3)
7.3(2)D1(2)
7.3(2)D1(1)
7.3(1)D1(1)
7.3(0)DX(1)
7.3(0)D1(1)
7.2(2)D1(2)
7.2(2)D1(1)
7.2(1)D1(1)
7.2(0)D1(1)
6.2(24a)
6.2(24)
6.2(22)
6.2(20a)
6.2(20)
6.2(18)
6.2(16)
6.2(14)

	6.2(12)
	6.2(10)

Cisco NX-OS Release 8.2(6) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
-----------------------	---

8.2(6)

8.2(5)

8.2(4)

8.2(3)

8.2(2)

8.2(1)

8.1(2a)

8.1(2)

8.1(1)

8.0(1)

7.3(6)D1(1)

7.3(5)D1(1)

7.3(4)D1(1)

7.3(3)D1(1)

7.3(2)D1(3a)

7.3(2)D1(3)

7.3(2)D1(2)

7.3(2)D1(1)

7.3(1)D1(1)

7.3(0)DX(1)

7.3(0)D1(1)

7.2(2)D1(2)

7.2(2)D1(1)

7.2(1)D1(1)

7.2(0)D1(1)

6.2(24a)

6.2(24)

6.2(22)

6.2(20a)

6.2(20)

6.2(18)

6.2(16)

6.2(14)

6.2(12)

6.2(10)

Cisco NX-OS Release 8.2(5) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.2(5)	8.2(4) 8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1) 6.2(22) 6.2(20a) 6.2(20) 6.2(18) 6.2(16) 6.2(14) 6.2(12) 6.2(10)

Cisco NX-OS Release 8.2(4) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.2(4)	8.2(3) 8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1) 6.2(22) 6.2(20a) 6.2(20) 6.2(18) 6.2(16) 6.2(14) 6.2(12) 6.2(10) 6.2(8b) 6.2(8a) 6.1(5a)

Cisco NX-OS Release 8.2(3) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.2(3)	8.2(2) 8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(3a) 7.3(2)D1(3) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1) 6.2(20a) 6.2(20) 6.2(18) 6.2(16) 6.2(14) 6.2(12) 6.2(10) 6.2(8b) 6.2(8a) 6.1(5a)

Cisco NX-OS Release 8.2(2) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
8.2(2)	8.2(1) 8.1(2a) 8.1(2) 8.1(1) 8.0(1) 7.3(5)D1(1) 7.3(4)D1(1) 7.3(3)D1(1) 7.3(2)D1(2) 7.3(2)D1(1) 7.3(1)D1(1) 7.3(0)DX(1) 7.3(0)D1(1) 7.2(2)D1(2) 7.2(2)D1(1) 7.2(1)D1(1) 7.2(0)D1(1) 6.2(20) 6.2(18) 6.2(16) 6.2(14) 6.2(12) 6.2(10) 6.2(8b) 6.2(8a) 6.1(5a)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.1(2a) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.1(2a)	8.1(2)
	8.1(1)
	8.0(1)
	7.3(5)D1(1)
	7.3(4)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(2)
	7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1)
	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(20)
	6.2(18)
	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)
	6.2(8b)
	6.2(8a)
	6.1(5a)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.1(2) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.1(2)	8.1(1)
	8.0(1)
	7.3(3)D1(1)
	7.3(3)D1(1)
	7.3(2)D1(2)
	7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1)
	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(20)
	6.2(18)
	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)
	6.2(8b)
	6.2(8a)
	6.1(5a)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.2(1) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.2(1)	8.1(1)
	8.0(1)
	7.3(3)D1(1)
	7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1)
	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(18)
	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)
	6.2(8b)
	6.2(8a)
	6.1(5a)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.1(1) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.1(1)	8.0(1)
	7.3(3)D1(1)
	7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1)
	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(18)
	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)
	6.2(8b)
	6.2(8a)
	6.1(5a)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

Cisco NX-OS Release 8.0(1) has the following cold boot support matrix:

Target Release	Current Release Supporting Cold-Boot Upgrade to Target Release
----------------	--

8.0(1)	7.3(3)D1(1)
	7.3(2)D1(1)
	7.3(1)D1(1)
	7.3(0)DX(1)
	7.3(0)D1(1)
	7.2(2)D1(2)
	7.2(2)D1(1)
	7.2(1)D1(1)
	7.2(0)D1(1)
	6.2(18)
	6.2(16)
	6.2(14)
	6.2(12)
	6.2(10)
	6.1(5a)



Note Non-ISSU upgrades are also referred to as cold boot upgrade.

To perform a non-ISSU upgrade (cold boot upgrade) to Cisco NX-OS Release 8.0(1) and later releases from any prior supported releases in the above table follow these steps:

1. Change the boot variable.

Example for Cisco NX-OS Release 8.2(1):

```
boot kickstart bootflash:/n7000-s2-kickstart.8.2.1.bin sup-1
boot system bootflash:/n7000-s2-dk9.8.2.1.bin sup-1
boot kickstart bootflash:/n7000-s2-kickstart.8.2.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.2.1.bin sup-2
```

Example for Cisco NX-OS Release 8.1(1):

```
boot kickstart bootflash:/n7000-s2-kickstart.8.1.1.bin sup-1
boot system bootflash:/n7000-s2-dk9.8.1.1.bin sup-1
boot kickstart bootflash:/n7000-s2-kickstart.8.1.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.1.1.bin sup-2
```

Example for Cisco NX-OS Release 8.0(1):

```
boot kickstart bootflash:/n7000-s2-kickstart.8.0.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.0.1.bin sup-1
boot kickstart bootflash:/n7000-s2-kickstart.8.0.1.bin sup-2
boot system bootflash:/n7000-s2-dk9.8.0.1.bin sup-2
```

2. Enter the **copy running-config startup-config vdc-all** command.

3. Enter the **reload** command to reload the switch.



Note Allow time after the reload for the configuration to be applied.

Reload based NXOS downgrades involve rebuilding the internal binary configuration from the text-based startup configuration. This is done to ensure compatibility between the binary configuration and the downgraded software version. As a result, certain specific configuration may be missing from the configuration, after downgrade, due to ASCII replay process. This would include FEX HIF port configuration and VTP database configuration. Furthermore, NX-OS configurations that require VDC or switch reload to take effect may require additional reload when applied during the downgrade process. Examples of this include URIB/MRIB shared memory tuning, custom reserved VLAN range and Fabricpath Transit Mode feature. In order to mitigate this during downgrade, you should copy your full configuration to bootflash/tftpserver.

Feature Support:

Any features introduced in a release must be disabled before downgrading to a release that does not support those features.

Unsupported Modules:

When manually downgrading from a Cisco NX-OS Release to an earlier release, first power down all modules that are unsupported in the downgrade image. Then, purge the configuration of the unsupported modules using the **purge module *module_number* running-config** command.

For complete instructions on upgrading your software, see the Cisco Nexus 7000 Series NX-OS Upgrade Downgrade Guide.

Non-In-Service Software Upgrade (Non-ISSU)/Cold Boot Upgrade Caveats

- When you perform a cold boot upgrade to a new Cisco NX-OS release, the default CoPP policy for the new release is not applied. Because you might have your own configured CoPP policy and want to continue using it, the policy for the earlier release continues to be applied. However, if you have not modified the default CoPP policy in earlier versions, it is recommended that when you install Cisco NX-OS Release 5.2 or later releases, you should apply the latest default CoPP policy for the upgrading version by using the **copp profile [strict | moderate | lenient]** command. This action removes the previous policy and applies a new CoPP policy. Note that reapplying copp profile configuration removes CoPP momentarily on the chassis for the new configuration to take into effect. Hence, this needs to be done in a maintained environment

Cold boot/Reload upgrades from Cisco NX-OS 7.3.x releases to Cisco NX-OS Release 8.0(1) and Cisco NX-OS Release 8.1(1) with RISE Configuration

- RISE configuration must be removed prior to starting your upgrade to Cisco NX-OS Release 8.0(1)/Cisco NX-OS Release 8.1(1). ISSU performs compatibility check and blocks the upgrade if RISE is configured. There is no warning displayed or prevention for the reload upgrade. Therefore make sure to remove RISE configuration before the reload upgrade.
 - There is no system check to block this upgrade path.
 - Ensure that the RISE feature is disabled before attempting to upgrade to Cisco NX-OS Release 8.0(1)/Cisco NX-OS Release 8.1(1). After upgrading to Cisco NX-OS Release 8.0(1)/Cisco NX-OS Release 8.1(1), configure RISE services as required. The RISE feature configuration can be verified by using the **show rise** and **show run services sc_engine** commands.
 - If you upgrade to Cisco NX-OS Release 8.0(1)/Cisco NX-OS Release 8.1(1) with the RISE configuration, RISE services will become unstable and unmanageable.
 - Steps to identify the error condition:

Even if the show feature command output shows RISE as enabled, no output will be displayed if you run the **show rise** and **show run services sc_engine** commands.
 - Steps to recover:

The only way to recover from this condition is to do a **reload ascii** on the switch.

ASCII Configuration Replay

Saving VLAN Configuration Information:

Because a VLAN configuration can be learned from the network while the VLAN Trunking Protocol (VTP) is in a server/client mode, the VLAN configuration is not stored in the running configuration. If you copy the running configuration to a file and apply this configuration at a later point, including after a switch reload, the VLANs will not be restored. However, the VLAN configuration will be erased if the switch is the only server in the VTP domain.

The following steps list the workaround for this limitation:

- Configure one of the clients as the server.
- Complete the following steps:
 - Copy the VTP data file to the bootflash: data file by entering the **copy vtp-datafile bootflash: vtp-datafile** command.
 - Copy the ASCII configuration to the startup configuration by entering the **copy ascii-cfg-file startup-config** command.
 - Reload the switch with Cisco NX-OS Release 6.2(2) or a later release

This limitation does not apply to a binary configuration, which is the recommended approach, but only to an ASCII configuration. In addition, this limitation applies to all Cisco NX-OS software releases for the Cisco Nexus 7000 series.

Rebind Interfaces command is not automatically executed when Replaying ASCII configuration in Cisco NX-OS Release 6.2(x):

The **rebind interfaces** command introduced in Cisco NX-OS Release 6.2(2) is needed to ensure the proper functionality of interfaces in certain circumstances. The command might be required when you change the module type of a VDC. However, because of the disruptive nature of the **rebind interfaces** command, for Cisco NX-OS Release 6.2(x) prior to Cisco NX-OS Release 6.2(8), this limitation applies only when all of the following conditions are met:

- The ASCII configuration file is replayed in the context of the default VDC or the admin VDC, and at least one VDC has an F2e Series or an F3 Series module listed as supported module types either before or after the replay.
- The limit-resource module-type commands listed in the ASCII configuration file requires that rebind interfaces command be executed.

The following steps list the workaround for this limitation:

- Manually enter the **rebind interfaces** command wherever needed to the ASCII configuration file for replay.
- Enter the **rebind interfaces** command immediately after you enter the **limit-resource module-type** command.
- Ensure that the ASCII replay properly applies all interface configurations for all interfaces in the relevant VDCs.



Note If you boot up the switch without any startup configuration, this limitation might apply to an ASCII replay. The reason is that without a startup configuration, the default VDC might still have certain interfaces automatically allocated. Because of this possibility, follow the approaches to work around the limitation.

Non In-Service Software Downgrade (non-ISSU)/Cold Boot Downgrade Steps

Instructions provided below list the steps for the cold boot (non-ISSU) downgrade. The example provided below is for a cold boot downgrade for the following:

- A switch that is running Cisco NX-OS Release 8.2(1) and needs to reload with Cisco NX-OSRelease 6.2(8a).
- A switch that is running Cisco NX-OS Release 8.1(1) and needs to reload with Cisco NX-OSRelease 6.2(8a).
- A switch that is running Cisco NX-OS Release 8.0(1) and needs to reload with Cisco NX-OSRelease 6.2(12).

Refer to the **ASCII Configuration Replay** caveats section for specific configuration caveats.

- Save the switch configuration.
 - Enter **copy running-config bootflash:<config.txt> vdc-all** command.
- Change the boot variable to boot the target release.
- Enter **copy running-config startup-config vdc-all** command to save the boot variable.
- Enter **write erase** command to erase running configuration on the switch.
- Enter **reload** command.

Once the switch and all the modules are up with the target image, do the following:

- Enter the **copy bootflash:<config.txt> running-config** command.
- Verify that the switch is configured correctly.
- Replay the configuration copy to check if fex interfaces exist.
 - Enter the **copy bootflash:<config.txt> running-config** command.

Terminology

This table summarizes the terms used in the **install all** command output for checking compatibility.

Table 26: install all Command Output Terminology

Term	Definition	
bootable	The module's ability to boot or not boot based on image compatibility.	
impact	The type of software upgrade mechanism—disruptive or nondisruptive.	
install-type	reset	Resets the module.
	sw-reset	Resets the module immediately after a switchover.
	rolling	Upgrades each module in sequence.
	copy-only	Updates the software for BIOS, loader, or bootrom.

Commands to use

- Verify connectivity to the remote server using the **ping** command.
- Ensure that the required space is available on both the active and standby supervisor modules for the image files to be copied using the **dir** command.
- Use the one-step **install all** command to upgrade your software. This command upgrades all modules in any Cisco NX-OS device.
- Run only one installation on a device at a time.



Note During vPC setup, the configuration is locked on the peer switch while ISSU is in progress.

- ISSU is not supported when the vPC peers are on a single physical device but are across VDCs.
- Do not enter another command while running the installation.
- Do the installation on the active supervisor module, not the standby supervisor module.



Note If the I/O modules are not compatible with the software image you install on the supervisor module, some traffic disruption might occur in those modules, depending on your configuration. The **install all** command output identifies these commands. You can choose to proceed with the upgrade or end at this point.

- The configuration is locked during the upgrade process.
- You can have only one instance of the **install all** command running.

Cisco NX-OS Software Downgrade Guidelines

- Any features introduced in a release must be disabled before downgrading to a release that does not support those features. See the release notes for information on the new features introduced in each release.
- In Cisco NX-OS Release 8.0(1), ISSD is not supported. You will have to perform a cold boot of the switch.
- VPC peers can only operate dissimilar versions of the Cisco NX-OS software during the upgrade or downgrade process. Operating VPC peers with dissimilar versions, after the upgrade or downgrade process is complete, is not supported.
- To determine incompatibility before you downgrade your software, use the following commands:
 - For hardware incompatibility—
sh install all impact system *system_name*
 - For software incompatibility—
show incompatibility-all system *image_filename*

Upgrading a Device with Dual Supervisor Modules

The **install all** command supports in-service software upgrades (ISSUs) on devices that have dual supervisor modules and performs the following actions:

- Determines whether the upgrade will be disruptive and asks if you want to continue.
- Ensure that you have enough space in the standby bootflash.
- Copies the kickstart and system images to the standby supervisor module.
- Sets the KICKSTART and SYSTEM boot variables.
- Reloads the standby supervisor module with the new Cisco NX-OS software.
- Reloads the active supervisor module with the new Cisco NX-OS software, which causes a switchover to the newly upgraded standby supervisor module.
- Upgrades the line cards.
- The Connectivity Management Processor (CMP) on both supervisors will get upgraded.

Benefits of Using the install all Command

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

- You can upgrade the entire device using just one command.
- You can receive descriptive information on the intended changes to your system before you continue with the installation.
- You have the option to cancel the command. You can continue or cancel when you see this question (the default is **no**):

```
Do you want to continue (y/n) [n] : y
```

- You can upgrade the entire device using the least disruptive procedure.
- You can see the progress of this command on the console, Telnet, and SSH screens:
 - Before a switchover process, you can only see the progress from the active supervisor module.
 - After a switchover process, you can see the progress from both the supervisor modules.
- The **install all** command automatically checks the image integrity, which includes the running kickstart and system images.
- The **install all** command performs a platform validity check to verify that a wrong image is not used—for example, to check if a Nexus 7000 device image is used inadvertently to upgrade a Nexus 5000 device.
- The **Ctrl-c** escape sequence gracefully ends the **install all** command. You are prompted to confirm your decision to abort the ISSU process. If you proceed, the command sequence completes the update step in progress and returns to the device prompt. (Other upgrade steps cannot be ended using **Ctrl-c**.)
- After entering the **install all** command, if any step in the sequence fails, the command completes the step in progress and ends. For example, if an I/O module fails to be updated for any reason (for example, due to an unstable network state), the command sequence disruptively updates that module and ends. In such cases, you can verify the problem on the affected switching module and upgrade the other I/O modules.

- The **show install all impact** *image-name* command runs pre-upgrade checks against a given image and informs the user if the images are compatible for an upgrade or a downgrade.



Note Refer to the "[Supported Upgrade and Downgrade Paths](#)" section of the Cisco Nexus 7000 Series NX-OS Release Notes to get details on the supported Cisco NX-OS release versions to which you can upgrade to or for the downgrade details.

ISSU Failure Conditions

The following situations cause the installation to fail to complete:

- If the standby supervisor module bootflash: file system does not have sufficient space to accept the updated image.
- If the specified system and kickstart images are not compatible.
- If the network or device is configured while the upgrade is in progress.
- If a Spanning Tree Protocol (STP) topology change occurs while the upgrade is in progress.
- If the **install all** command is entered on the standby supervisor module.
- If the **install all** command does not reference the default bootflash: in a dual supervisor module configuration.
- If a module is removed while the upgrade is in progress.
- If the device has any power disruption while the upgrade is in progress.
- If the entire path for the remote server location is not specified accurately.
- If some FEX ports are operating in LACP fast rate mode.
- If images are incompatible after an upgrade. For example, an I/O module image may be incompatible with the system image, or a kickstart image may be incompatible with a system image. This is also identified by the **show install all impact** command in the compatibility check section of the output (under the Bootable column).
- If a linecard is in failure state, the ISSU will abort.

The Cisco NX-OS software prevents most configuration changes while the **install all** command is in progress. However, the Cisco NX-OS software allows configuration changes from Cisco Fabric Services (CFS) and those changes may affect the ISSU.

Upgrade Procedure Summary

The following summary procedure describes how to upgrade a device that has dual supervisor modules to the latest Cisco NX-OS software.

Procedure

- Step 1** Log in to the console port on both of the active and standby supervisor modules.
- Step 2** Log in to Cisco.com and download the latest Cisco NX-OS kickstart and system images to a server.
- Step 3** Download the Cisco NX-OS kickstart and system images from the server to your device using the **copy** command.
- Step 4** Save the device configuration using the **copy running-config startup-config vdc-all** command.

Step 5 Enter the **install all** command at the active supervisor command prompt to upgrade the Cisco NX-OS software on your device.

Note A supervisor module switchover occurs during the software installation.

Detailed Upgrade Procedure

This section describes the detailed procedure to upgrade to the latest Cisco NX-OS software on a device with dual supervisor modules.

Procedure

Step 1 Log in to the device on the console port connection on both of the active and standby supervisor modules.

Step 2 Log in to Cisco.com to access the links provided in this document. To log in to Cisco.com, go to the URL <http://www.cisco.com/> and click **Log In** at the top of the page. Enter your Cisco username and password.

Note Unregistered Cisco.com users cannot access the links provided in this document.

Step 3 Access the Software Download Center using this URL: <http://www.cisco.com/public/sw-center/index.shtml>

Step 4 Navigate to the download site for your device.
You see links to the download images for your device.

Step 5 Select and download the kickstart and system software files to a server.

Step 6 Ensure that the required space is available for the image file(s) to be copied.

```
switch# dir bootflash:
 4096   Oct 24 18:06:54 2016  lost+found/
146701191 Aug 09 15:18:05 2016  n7000-s1-dk9.7.2.0.D1.1.bin.CCO
 30674944 Apr 25 15:51:13 2016  n7000-s1-kickstart.7.2.0.D1.1.bin.CCO

Usage for bootflash://sup-local
1260208128 bytes used
 579682304 bytes free
1839890432 bytes total
switch#
```

Tip We recommend that you have the kickstart and system image files for at least one previous release of the Cisco NX-OS software on the device to use if the new image files do not load successfully.

Step 7 If you need more space on the active supervisor module, delete unnecessary files to make space available.

```
switch# delete bootflash:n7000-s1-kickstart.7.2.0.D1.1.bin.CCO
switch# delete bootflash:n7000-s1-dk9.7.2.0.D1.1.bin.CCO
```

Step 8 Verify that there is space available on the standby supervisor module.

```
switch# dir bootflash://sup-standby/
 49152   Oct 16 14:43:39 2016  lost+found
 80850712 Oct 04 15:57:44 2016  n7000-s2-dk9.8.0.1.bin.CCO
```

```
22593024      Oct 04 15:52:56 2016  n7000-s2-kickstart.8.0.1.bin.CCO
```

```
Usage for bootflash://sup-standby
103492888 bytes used
800604904 bytes free
904097792 bytes total
```

Step 9 If you need more space on the standby supervisor module, delete any unnecessary files to make space available.

```
switch# delete bootflash://sup-standby/n7000-s2-kickstart.8.0.1.bin.CCO
switch# delete bootflash://sup-standby/n7000-s2-dk9.8.0.1.bin.CCO
```

Step 10 Copy the NX-OS kickstart and system images to the active supervisor module using a transfer protocol. You can use **ftp:**, **tftp:**, **scp:**, or **sftp:**. The examples in this procedure use **scp:**.

Note When you download an image file, change to your FTP environment IP address or DNS name and the path where the files are located.

```
switch# copy scp://user@scpserver.cisco.com/downloads/n7000-s2-kickstart.8.0.1.bin
n7000-s2-kickstart.8.0.1.bin
switch# copy scp://user@scpserver.cisco.com/downloads/n7000-s2-dk9.8.0.1.bin n7000-s2-dk9.8.0.1.bin
```

Step 11 Read the release notes for the related image file. See the *Cisco Nexus 7000 Series NX-OS Release Notes*.

Step 12 Save the running configuration to the startup configuration.

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

Step 13 Perform the upgrade using the **install all** command at the command prompt on the active supervisor module.

```
switch# install all kickstart n7000-s2-kickstart.8.0.1.bin system n7000-s2-dk9.8.0.1.bin
```

Note If the upgrade is disruptive, you can either resolve the issues that cause the disruption and repeat this step, or you can continue with the disruptive upgrade.

Step 14 After the installation operation completes, log in and verify that the device is running the required software version using the **show version** command.

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are owned by other third parties and
used and distributed under license.
Certain components of this software are licensed under the GNU General Public License (GPL) version
 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1.
A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

```
Software
  BIOS: version 3.1.0
  kickstart: version 8.0(1)
  system: version 8.0(1)
  BIOS compile time: 02/27/2016
  kickstart image file is: bootflash:///n7000-s2-kickstart.8.0.1.bin.S28
  kickstart compile time: 5/19/2016 11:00:00 [06/14/2016 21:46:24]
  system image file is: bootflash:///n7000-s2-dk9.8.0.1.bin.S28
  system compile time: 5/19/2016 11:00:00 [06/14/2016 23:40:21]
```

```
Hardware
  cisco Nexus7000 C7018 (18 Slot) Chassis ("Supervisor module-1X")
  Intel(R) Xeon(R) CPU with 8245320 kB of memory.
  Processor Board ID JAB1152011N

  Device name: switch bootflash: 2030616 kB
  slot0: 2044854 kB (expansion flash)

  Kernel uptime is 0 day(s), 0 hour(s), 18 minute(s), 3 second(s)
  Last reset at 507466 usecs after Mon Oct 24 21:12:39 2015
  Reason: Reset Requested by CLI command reload
  ...
```

Step 15 Reload both CMPs.

Note CMP is a Supervisor 1 only feature.

```
switch# reload cmp module 5
switch# reload cmp module 6
```

Step 16 Type the **show install all status** command.

The entire upgrade process is displayed.

Note Type **Ctrl + c** to exit the command.

Step 17 (Optional) Install licenses (if necessary) to ensure that the required features are available on the device. See the *Cisco NX-OS Licensing Guide*.

Upgrading a Device with a Single Supervisor Module

This section describes how to upgrade a Cisco NX-OS device with a single supervisor module.

Upgrade Procedure Summary

The following summary procedure describes how to upgrade a device that has a single supervisor module to the latest Cisco NX-OS software.

Procedure

- Step 1** Log in to the console port on the supervisor modules.
- Step 2** Log in to Cisco.com and download the latest Cisco NX-OS kickstart and system images.
- Step 3** Download the Cisco NX-OS kickstart and system images to your device using the **copy** command.
- Step 4** Update the KICKSTART and SYSTEM boot variables and module images using the **install all** command.

Detailed Upgrade Procedure

This section describes the detailed procedure to upgrade to the latest Cisco NX-OS software on a device with a single supervisor.

Procedure

- Step 1** Log in to the device on the console port connection.
- Step 2** Log in to Cisco.com to access the links provided in this document. To log in to Cisco.com, go to the URL <http://www.cisco.com/> and click **Log In** at the top of the page. Enter your Cisco username and password.

Note Unregistered Cisco.com users cannot access the links provided in this document.

- Step 3** Access the Software Download Center using this URL: <http://www.cisco.com/public/sw-center/index.shtml>
- Step 4** Navigate to the download site for your device.
You see links to the download images for your device.
- Step 5** Select and download the kickstart and system software files to a server.
- Step 6** Ensure that the required space is available in the bootflash: directory for the image file(s) to be copied.

```
switch# dir bootflash:
 4096   Oct 24 18:06:54 2016  lost+found/
146701191 Aug 09 15:18:05 2016  n7000-s2-dk9.8.0.1.bin.CCO
 30674944 Apr 25 15:51:13 2016  n7000-s2-kickstart.8.0.1.bin.CCO

Usage for bootflash://sup-local
1260208128 bytes used
 579682304 bytes free
1839890432 bytes total
switch#
```

Tip We recommend that you have the kickstart and system image files for at least one previous release of the Cisco NX-OS software on the device to use if the new image files do not load successfully.

- Step 7** If you need more space on the supervisor module bootflash, delete unnecessary files to make space available.

```
switch# delete bootflash:n7000-s1-kickstart.7.2.0.D1.1.bin.CCO
switch# delete bootflash:n7000-s1-dk9.7.2.0.D1.1.bin.CCO
```

- Step 8** Copy the NX-OS kickstart and system images to the active supervisor module bootflash using a transfer protocol. You can use **ftp:**, **tftp:**, **scp:**, or **sftp:**. The examples in this procedure use **scp:**.

Note When you download an image file, change to your FTP environment IP address or DNS name and the path where the files are located.

```
switch# copy scp://user@scpserver.cisco.com/downloads/n7000-s2-kickstart.8.0.1.bin
n7000-s2-kickstart.8.0.1.bin
switch# copy scp://user@scpserver.cisco.com/downloads/n7000-s2-dk9.8.0.1.bin n7000-s2-dk9.8.0.1.bin
```

Step 9 Read the release notes for the related image file. See the *Cisco Nexus 7000 Series NX-OS Release Notes*.

Step 10 Use the **install all** command to update the boot variables and module images on your device.

```
switch# install all kickstart n7000-s2-kickstart.8.0.1.bin system n7000-s2-dk9.8.0.1.bin
```

Note Beginning with Cisco NX-OS Release 5.2, you can save time by upgrading up to three line cards concurrently. To do so, add the **parallel** option at the end of the **install all** command (for example, **install all kickstart bootflash:n7000-s1-kickstart.5.2.1.bin system bootflash:n7000-s1-dk9.5.2.1.bin parallel**). The **parallel** option is available only when you are upgrading from Cisco NX-OS Release 5.2 to a later release.

Step 11 After the device completes the reload operation, log in and verify that the device is running the required software version.

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  BIOS:          version 3.1.0
  kickstart:    version 8.0(1)
  system:       version 8.0(1)
  BIOS compile time:      06/27/2016
  kickstart image file is: bootflash:///n7000-s2-kickstart.8.0.1.bin.S28
  kickstart compile time: 6/27/2016 11:00:00 [06/27/2016 21:46:24]
  system image file is:   bootflash:///n7000-s2-dk9.8.0.1.bin.S28
  system compile time:    6/27/2016 11:00:00 [06/27/2016 23:40:21]

Hardware
  cisco Nexus7000 C7018 (18 Slot) Chassis ("Supervisor module-1X")
  Intel(R) Xeon(R) CPU          with 8245320 kB of memory.
  Processor Board ID JAB1152011N

  Device name: switch
  bootflash:   2030616 kB
  slot0:       2044854 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 18 minute(s), 3 second(s)

Last reset at 507466 usecs after Mon Oct 24 21:12:39 2015
```

```
Reason: Reset Requested by CLI command reload
...
```

Step 12 Type the **show install all status** command.

The entire upgrade process is displayed.

Note Type **Ctrl + c** to exit the command.

Step 13 Reload the CMP modules.

Note CMP is a Supervisor 1 only feature.

```
switch# reload cmp module 5
switch# reload cmp module 6
```

Step 14 (Optional) Install licenses to ensure that the required features are available on the device. See the *Cisco NX-OS Licensing Guide*.

Performing a Traditional Upgrade or Downgrade (Chassis Reload)

This procedure is recommended for these specific scenarios:

- In lab environments where continuous uptime is not a requirement
- In production environments in the unlikely event that an upgrade needs to be downgraded in a timely manner
- In situations where ISSU or ISSD is not supported for the respective images

Before you begin

Save and back up all configurations before reloading the system to load the new software.

Power down unsupported line cards.

Procedure

Step 1 Configure the boot variable for the Cisco NX-OS software kickstart image.

```
switch(config)# boot kickstart bootflash:n7000-s2-kickstart.8.0.1.bin
```

Step 2 Configure the boot variable for the Cisco NX-OS software system image.

```
switch(config)# boot system bootflash:n7000-s2-dk9.8.0.1.bin
```

Step 3 Save the running configuration to the startup configuration.

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

Step 4 Verify that the "Current Boot Variables" and the "Boot Variables on the next reload" match the expected image.

```
Current Boot Variables:

sup-2
kickstart variable = bootflash:/n7000-s2-kickstart.8.0.1.bin system variable =
bootflash:/n7000-s2-dk9.8.0.1.bin
No module boot variable set
Boot Variables on next reload: sup-1
kickstart variable = bootflash:/n7000-s2-kickstart.8.0.1.bin system variable =
bootflash:/n7000-s2-dk9.8.0.1.bin
sup-2
kickstart variable = bootflash:/n7000-s2-kickstart.8.0.1.bin system variable =
bootflash:/n7000-s2-dk9.8.0.1.bin
No module boot variable set
```

Step 5 Verify that the image location and the image name match the above boot statements. In redundant supervisor chassis, the images auto-synchronize from to standby once the boot statements are set.

```
switch# show boot auto-copy list
switch# dir bootflash://sup-active/
 161980383   May 15 17:52:03 2016  n7000-s2-dk9.8.0.1.bin
 29471232   May 15 18:01:38 2016  n7000-s2-kickstart.8.0.1.bin

switch# dir bootflash://sup-standby/
 161980383   May 15 18:04:55 2016  n7000-s2-dk9.8.0.1.bin
 29471232   May 15 18:06:18 2016  n7000-s2-kickstart.8.0.1.bin
```

Step 6 After you verify the image location and statements, reload the Cisco NX-OS device.

```
switch# reload
```

Example Outputs from Cisco NX-OS Software Upgrades

This section includes example outputs from Cisco NX-OS software upgrades.

- The output of the **install all** command depends on the software image, especially the upgrade required (Upg-Required) field information in the upgrade table.
- Any time you perform a disruptive ISSU, the supervisor modules will be reloaded.

Example Nondisruptive Upgrade of a Device with Dual Supervisors

The following example has the console session output that shows a nondisruptive execution of the **install all** command on a device with dual supervisor modules:

```
switch# install all kickstart n7000-s2-kickstart.8.0.1.bin system n7000-s2-dk9.8.0.1.bin

Verifying image bootflash:/n7000-s2-kickstart.8.0.1.bin for boot variable "kickstart".
[#####] 100% -- SUCCESS

Verifying image bootflash:/n7000-s2-dk9.8.0.1.bin for boot variable "system".
[#####] 100% -- SUCCESS

Verifying image type.
[#####] 100% -- SUCCESS
```



```

Extracting "lc-m2-n7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "bios" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lc-f1-n7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lc-m2-n7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lc-m2-n7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:/n7000-s2-kickstart.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lc-m2-n7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lc-m2-n7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lc-f1-n7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lc-m2-n7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "fexth" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "fexth" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "fexth" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "cmp" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "cmp-bios" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Performing module support checks.
[#####] 100% -- SUCCESS

Notifying services about system upgrade.
[#####] 100% -- SUCCESS

```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	rolling	
2	yes	non-disruptive	rolling	
3	yes	non-disruptive	rolling	
8	yes	non-disruptive	rolling	
9	yes	non-disruptive	reset	
10	yes	non-disruptive	reset	

```

11      yes non-disruptive      rolling
14      yes non-disruptive      rolling
16      yes non-disruptive      rolling
18      yes non-disruptive      rolling
101     yes non-disruptive      rolling
102     yes non-disruptive      rolling
103     yes non-disruptive      rolling

```

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-Version	Upg-Required
1	lc-m1-n7k	7.3(1)	8.0(1)	yes
1	bios	v1.10.17(04/25/16): v1.10.17(04/25/15)		no
2	lc-f1-n7k	7.3(1)	8.0(1)	yes
2	bios	v1.10.17(04/25/16): v1.10.17(04/25/15)		no
3	lc-m1-n7k	7.3(1)	8.0(1)	yes
3	bios	v1.10.17(04/25/16): v1.10.17(04/25/15)		no
8	lc-m1-n7k	7.3(1)	8.0(1)	yes

Do you want to continue with the installation (y/n)? [n] **y**

Install is in progress, please wait.

Performing runtime checks.

[#####] 100% -- SUCCESS

Syncing image bootflash:/n7000-s2-kickstart.8.0.1.bin to standby.

[#####] 100% -- SUCCESS

Syncing image bootflash:/n7000-s2-dk9.8.0.1.bin to standby.

[#####] 100% -- SUCCESS

Setting boot variables.

[#####] 100% -- SUCCESS

Performing configuration copy.

[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom. Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Module 2: Refreshing compact flash and upgrading bios/loader/bootrom. Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Module 3: Refreshing compact flash and upgrading bios/loader/bootrom. Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Module 8: Refreshing compact flash and upgrading bios/loader/bootrom. Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Module 9: Refreshing compact flash and upgrading bios/loader/bootrom. Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Module 10: Refreshing compact flash and upgrading bios/loader/bootrom.


```

INIT:
Checking all filesystems..r.r.r..r done. Loading system software
/bootflash//n7000-s2-dk9.8.0.1.bin read done
Uncompressing system image: bootflash://n7000-s2-dk9.8.0.1.bin Mon May 24 10:00:07 PST 2016 blogger: nothing to
do.

..done Mon May 24 10:00:12 PST 2016
Load plugins that defined in image conf: /isan/plugin_img/img.conf Loading plugin 0: core_plugin...
num srgs 1
0: swid-core-supdc3, swid-core-supdc3
num srgs 1
0: swid-supdc3-ks, swid-supdc3-ks INIT: Entering runlevel: 3

Continuing with installation, please wait
2016 May 24 10:01:00 switch-B %$ VDC-1 %$ %IDEHSD-2-MOUNT: slot0: online 2016 May 24 10:01:39 switch-B %$ VDC-1
%$ %IDEHSD-2-MOUNT: logflash: online
2016 May 24 10:01:41 switch-B %$ VDC-1 %$ %CMPPROXY-2-LOG_CMP_UP: Connectivity Management processor(on module
10) is now UP

Module 10: Waiting for module online.
-- SUCCESS
2016 May 24 10:04:53 switch-B %$ VDC-1 %$ Oct 24 10:04:53 %KERN-2-SYSTEM_MSG: [ 480.115904] Switchover started
by redundancy driver - kernel
2016 May 24 10:04:53 switch-B %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming active
(pre-start phase).
2016 May 24 10:04:53 switch-B %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_START: Supervisor 10 is becoming active. 2016
May 24 10:04:55 switch-B %$ VDC-1 %$ %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2016 May 24 10:05:01 switch-B %$ VDC-1 %$ %CALLHOME-2-EVENT: HARDWARE_REMOVAL
2016 May 24 10:05:01 switch-B %$ VDC-1 %$ %PLATFORM-2-MOD_REMOVE: Module 6 removed (Serial number ) 2016 May
24 10:11:03 switch-B %$ VDC-1 %$ %IDEHSD-STANDBY-2-MOUNT: slot0: online
2016 May 24 10:11:12 switch-B %$ VDC-1 %$ %CMPPROXY-STANDBY-2-LOG_CMP_UP: Connectivity Management processor(on
module 9) is now UP
2016 May 24 10:11:15 switch-B %$ VDC-1 %$ %CALLHOME-2-EVENT: PERIODIC_CONFIGURATION
2016 May 24 10:12:02 switch-B %$ VDC-1 %$ %IDEHSD-STANDBY-2-MOUNT: logflash: online

Module 1: Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Module 2: Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Module 3: Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Module 8: Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Module 11: Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Module 14: Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Module 16: Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Module 18: Non-disruptive upgrading.
[#####] 100% -- SUCCESS

Module 10: Upgrading CMP image.
Warning: please do not reload or power cycle CMP module at this time.
[#####] 100% -- SUCCESS

```

```
Module 9: Upgrading CMP image.
Warning: please do not reload or power cycle CMP module at this time.
[#####] 100% -- SUCCESS
```

Recommended action::

```
"Please reload CMP(s) manually to have it run in the newer version.". Install has been successful.
User Access Verification
switch-B login: 2016 May 24 10:54:44 switch-B %$ VDC-1 %$ %COPP-2-COPP_PROFILE_DIFF:
CoPP Default Profile may have changed, please check the diffs using show copp diff profile <profile-type>
prior-ver profile <profile-type>
```

```
User Access Verification switch-B login: admin Password:<password>
Cisco Nexus Operating System (NX-OS) Software TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are owned by other third parties and used and
distributed under license.
Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the
GNU
Lesser General Public License (LGPL) Version 2.1.
A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```



Note A supervisor module switchover has occurred, and the active supervisor module is now the standby supervisor module.

Example Disruptive Upgrade of a Device with Dual Supervisors

The following console session example output shows a disruptive execution of the **install all** command on a device with dual supervisor modules:

```
switch# install all kickstart n7000-s2-kickstart.8.0.1.bin system n7000-s2-dk9.8.0.1.bin

Verifying image bootflash:/n7000-s2-kickstart.8.0.1.bin for boot variable "kickstart".
[#####] 100% -- SUCCESS

Verifying image bootflash:/n7000-s2-dk9.8.0.1.bin for boot variable "system".
[#####] 100% -- SUCCESS

Verifying image type.
[#####] 100% -- SUCCESS

Extracting "lcln7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "bios" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lcln7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "lcln7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:/n7000-s2-kickstart.8.0.1.bin.
[#####] 100% -- SUCCESS
```

```
Extracting "lcln7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS
```

```
Extracting "cmp" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS
```

```
Extracting "cmp-bios" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.
[#####] 100% -- SUCCESS
```

```
Performing module support checks.
[#####] 100% -- SUCCESS
```

```
Notifying services about system upgrade.
[#####] 100% -- SUCCESS
```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	Incompatible image
3	yes	disruptive	reset	Incompatible image
4	yes	disruptive	reset	Incompatible image
5	yes	disruptive	reset	Incompatible image
6	yes	disruptive	reset	Incompatible image
10	yes	disruptive	reset	Incompatible image

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-Version	Upg-Required
1	lcln7k	7.3(1)	8.0(1)	yes
1	bios	v1.10.17(04/25/16): v1.10.17(04/25/16)		no
3	lcln7k	7.3(1)	8.0(1)	yes
3	bios	v1.10.17(04/25/16): v1.10.17(04/25/16)		no
4	lcln7k	7.3(1)	8.0(1)	yes
4	bios	v1.10.17(04/25/16): v1.10.17(04/25/16)		no
5	system	7.3(1)	8.0(1)	yes
5	kickstart	7.3(1)	8.0(1)	yes

```
Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n] y
```



Note A supervisor module switchover has occurred and the active supervisor module is now the standby supervisor module.

The following example console session output from the standby supervisor module shows that the standby supervisor module switches over to become the active supervisor module:

```
switch(standby)#
NX7 SUP Ver 3.17.0
Serial Port Parameters from CMOS
PMCON_1: 0x20
PMCON_2: 0x0
```

PMCON_3: 0x3a
PM1_STS: 0x101
Performing Memory Detection and Testing
Testing 1 DRAM Patterns
Total mem found : 4096 MB
Memory test complete.
NumCpus = 2.
Status 61: PCI DEVICES Enumeration Started
Status 62: PCI DEVICES Enumeration Ended
Status 9F: Dispatching Drivers
Status 9E: IOFPGA Found
Status 9A: Booting From Primary ROM
Status 98: Found Cisco IDE
Status 98: Found Cisco IDE
Status 90: Loading Boot Loader

Reset Reason Registers: 0x10 0x0
Filesystem type is ext2fs, partition type 0x83

GNU GRUB version 0.97

Autobooting bootflash:/n7000-s1-kickstart.8.0.1a.bin bootflash:/n7000-s2-kickstart.8.0.1.bin...
Filesystem type is ext2fs, partition type 0x83
Booting kickstart image: bootflash:/n7000-s1-kickstart.8.0.1a.bin....
.....Image verification OK

Starting kernel...
INIT: version 2.85 booting
Checking all filesystems..r.r.r.. done.
n7000-s2-kickstart.8.0.1.bin read done
duplicate password entry

delete line `adminbackup:x:0:0::/var/home/adminbackup:/bin/bash'? **No**
duplicate password entry

delete line `adminbackup:x:2003:504::/var/home/adminbackup:/isan/bin/vsh_perm'? **No**
pwck: no changes

Setting kernel variables: sysctlnet.ipv4.ip_forward = 0
net.ipv4.ip_default_ttl = 64
net.ipv4.ip_no_pmtu_disc = 1
.

Setting the System Clock using the Hardware Clock as reference...System Clock set.
Local time: Fri Apr 18 02:33:42 UTC 2008
Loading system software
Uncompressing system image: n7000-s2-kickstart.8.0.1.bin

Load plugins that defined in image conf: /isan/plugin_img/img.conf
Loading plugin 0: core_plugin...
INIT: Entering runlevel: 3
Exporting directories for NFS kernel daemon...done.
Starting NFS kernel daemon:rpc.nfsd.
rpc.mountddone.

User Access Verification
switch login: **admin**
Password: <password>

Example Disruptive Upgrade of a Device with a Single Supervisor

The following console session example output shows a disruptive execution of the **install all** command on a device with a single supervisor module:

```
switch# install all kickstart n7000-s2-kickstart.8.0.1.bin system n7000-s2-dk9.8.0.1.bin
```

```
Verifying image bootflash:/n7000-s2-kickstart.8.0.1.bin for boot variable "kickstart".  
[#####] 100% -- SUCCESS
```

```
Verifying image bootflash:/n7000-s2-dk9.8.0.1.bin for boot variable "system".  
[#####] 100% -- SUCCESS
```

```
Verifying image type.  
[#####] 100% -- SUCCESS
```

```
Extracting "lcln7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Extracting "bios" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Extracting "lcln7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Extracting "lcln7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Extracting "system" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Extracting "kickstart" version from image bootflash:/n7000-s2-kickstart.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Extracting "lcln7k" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Extracting "cmp" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Extracting "cmp-bios" version from image bootflash:/n7000-s2-dk9.8.0.1.bin.  
[#####] 100% -- SUCCESS
```

```
Performing module support checks.  
[#####] 100% -- SUCCESS
```

```
Notifying services about system upgrade.  
[#####] 100% -- SUCCESS
```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	Incompatible image
3	yes	disruptive	reset	Incompatible image
4	yes	disruptive	reset	Incompatible image
5	yes	disruptive	reset	Incompatible image
6	yes	disruptive	reset	Incompatible image
10	yes	disruptive	reset	Incompatible image

Images will be upgraded according to following table:

Module	Image	Running-Version (pri:alt)	New-Version	Upg-Required
1	lcln7k	7.3(1)	8.0(1)	yes
1	bios	v1.10.17(04/25/16): v1.10.17(04/25/16)		no
3	lcln7k	7.3(1)	8.0(1)	yes
3	bios	v1.10.17(04/25/16): v1.10.17(04/25/16)		no
4	lcln7k	7.3(1)	8.0(1)	yes
4	bios	v1.10.17(04/25/16): v1.10.17(04/25/16)		no
5	system	7.3(1)	8.0(1)	yes
5	kickstart	7.3(1)	8.0(1)	yes
5	bios	v3.22.0(02/20/16): v3.22.0(02/20/16)		no
5	cmp	7.3(1)	8.0(1)	no
5	cmp-bios	02.01.05	02.01.05	no
6	system	7.3(1)	8.0(1)	yes
6	kickstart	7.3(1)	8.0(1)	yes
6	bios	v3.22.0(02/20/16): v3.22.0(02/20/16)		no
6	cmp	7.3(1)	8.0(1)	no
6	cmp-bios	02.01.05	02.01.05	no
10	lcln7k	7.3(1)	8.0(1)	yes
10	bios	v1.10.17(04/25/16): v1.10.17(04/25/16)		no

Switch will be reloaded for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] **y**

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Feature History for Software Upgrade and Downgrade

This table lists the release history for this feature.

Table 27: Feature History for Software Upgrade and Downgrade

Feature Name	Releases	Feature Information
Software upgrade/downgrade	8.2(10)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(10).

Feature Name	Releases	Feature Information
Software upgrade/downgrade	8.4(7)	Added guidelines for upgrading to Cisco NX-OS Release 8.4(7).
Software upgrade/downgrade	8.4(6a)	Added guidelines for upgrading to Cisco NX-OS Release 8.4(6a).
Software upgrade/downgrade	8.2(9)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(9).
Software upgrade/downgrade	8.4(6)	Added guidelines for upgrading to Cisco NX-OS Release 8.4(6).
Software upgrade/downgrade	8.4(5)	Added guidelines for upgrading to Cisco NX-OS Release 8.4(5).
Software upgrade/downgrade	8.4(4a)	Added guidelines for upgrading to Cisco NX-OS Release 8.4(4a).
Software upgrade/downgrade	8.2(7)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(7).
Software upgrade/downgrade	8.4(4)	Added guidelines for upgrading to Cisco NX-OS Release 8.4(4).
Software upgrade/downgrade	8.2(6)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(6).
Software upgrade/downgrade	8.4(2)	Added guidelines for upgrading to Cisco NX-OS Release 8.4(2).
Software upgrade/downgrade	8.2(5)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(5).
Software upgrade/downgrade	8.4(1)	Added guidelines for upgrading to Cisco NX-OS Release 8.4(1).
Software upgrade/downgrade	8.2(4)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(4).
Software upgrade/downgrade	8.2(3)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(3).
Software upgrade/downgrade	8.3(2)	Added guidelines for upgrading to Cisco NX-OS Release 8.3(2).
Software upgrade/downgrade	8.3(1)	Added guidelines for upgrading to Cisco NX-OS Release 8.3(1).
Software upgrade/downgrade	8.2(2)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(2).
Software upgrade/downgrade	8.1(2a)	Added guidelines for upgrading to Cisco NX-OS Release 8.1(2a).

Feature Name	Releases	Feature Information
Software upgrade/downgrade	8.2(1)	Added guidelines for upgrading to Cisco NX-OS Release 8.2(1).
Software upgrade/downgrade	8.1(1)	Added guidelines for upgrading to Cisco NX-OS Release 8.1(1).
Software upgrade/downgrade	8.0(1)	Added guidelines for upgrading to Cisco NX-OS Release 8.0(1).



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.