Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x

First Published: 2015-02-01

Last Modified: 2024-02-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface includes the following sections:

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which you supply the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments that are separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments that are separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Convention	Description
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string includes the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information that you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Related Documentation for Cisco Nexus 9000 Series Switches

The entire Cisco Nexus 9000 Series switch documentation set is available at the following URL:

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

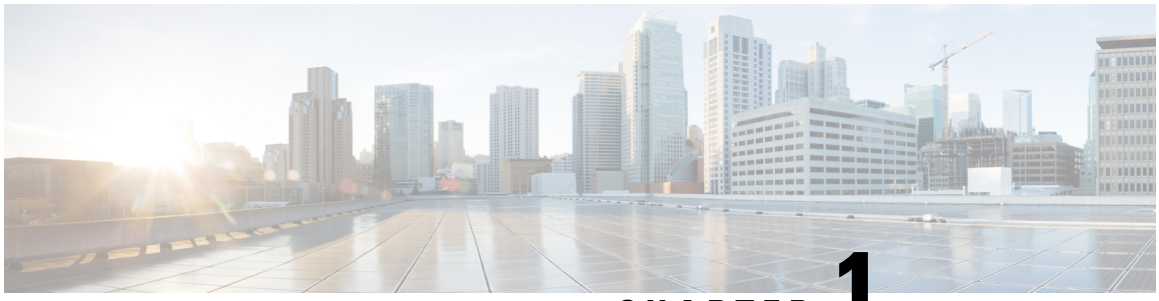
Communications, Services, and Additional Information

- 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.

Preface



CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x*.

New and Changed Information

This table summarizes the new and changed features for the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x* and tells you where they are documented.

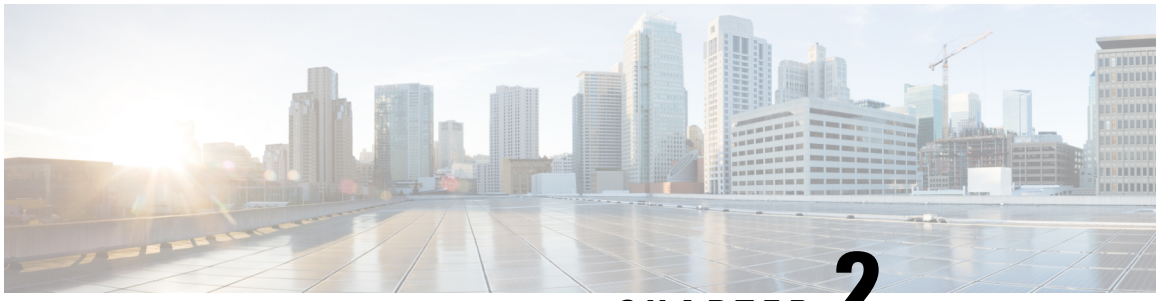
Table 1: New and Changed Features for Cisco NX-OS Release 7.x

Feature	Description	Changed in Release	Where Documented
Enhanced ISSU	Added support for the Cisco Nexus 9200 and 9300-EX platform switches.	7.0(3)I7(3)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5
ISSU	Added support for the Cisco Nexus 93180LC-EX switch.	7.0(3)I7(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5
ISSU	Added support for the Cisco Nexus 9200 platform switches, the Cisco Nexus 93108TC-EX and 93180YC-EX switches, and the Cisco Nexus 3132Q-V, 31108PC-V, 31108TC-V, 3232C, and 3264Q switches.	7.0(3)I6(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5

Feature	Description	Changed in Release	Where Documented
Enhanced ISSU	Introduced this feature for some Cisco Nexus 9300 platform switches and the Cisco Nexus 3164Q, 31128PQ, 3132Q-V, 31108PC-V, and 31108TC-V switches.	7.0(3)I5(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5
Fast reload	Removed support for this feature in the Cisco NX-OS 7.x software for the Cisco Nexus 3164Q switch.	7.0(3)I4(1)	Upgrading the Cisco NX-OS Software Using Fast Reload, on page 41
ISSU	Added ISSU support for FEX, NAT, segment routing, and VXLAN.	7.0(3)I4(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5
In-service software upgrade (ISSU)	Introduced this feature for some Cisco Nexus 9300 and 9500 platform switches and the Cisco Nexus 3164Q and 31128PQ switches.	7.0(3)I3(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5
Cisco NX-OS software image	Changed the image filename to start with "nxos" instead of "n9000."	7.0(3)I2(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5
Fast reload	Introduced this feature in the Cisco NX-OS 7.x software for the Cisco Nexus 3164Q switch.	7.0(3)I2(1)	Upgrading the Cisco NX-OS Software Using Fast Reload, on page 41
Software upgrade	Added the ability to perform a no-reload or non-interruptive software upgrade.	7.0(3)I2(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5
SHA256 algorithm to verify operating system integrity	Introduced this feature.	7.0(3)I2(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 5
Cisco NX-OS to ACI conversion	Added the ability to boot the ACI image from Cisco NX-OS mode (instead of from the loader> prompt) while converting a Cisco Nexus 9000 series switch from Cisco NX-OS to ACI boot mode.	7.0(3)I1(2)	Converting from Cisco NX-OS to ACI Boot Mode and from ACI Boot Mode Back to Cisco NX-OS, on page 47

Feature	Description	Changed in Release	Where Documented
Fast reload	Removed support for this feature, which was added in Cisco NX-OS Release 6.1(2)I3(4) for the Cisco Nexus 3164Q switch.	7.0(3)I1(1)	

New and Changed Information



CHAPTER 2

Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software

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

About the Software Image

Each device is shipped with the Cisco NX-OS software. The Cisco NX-OS software consists of one NXOS software image. The image filename begins with "nxos" [beginning with Cisco NX-OS Release 7.0(3)I2(1)] or "n9000" (for example, nxos.7.0.3.I2.1.bin or n9000-dk9.7.0.3.I1.1.bin).

Only this image is required to load the Cisco NX-OS operating system. This image runs on all Cisco Nexus 9000 Series switches, the Cisco Nexus 3164Q switch starting with Cisco NX-OS Release 6.1(2)I2(2a), the Cisco Nexus 31128PQ switch starting with Cisco NX-OS Release 7.0(3)I2(1), and the Cisco Nexus 3232C and 3264Q switches starting with Cisco NX-OS Release 7.0(3)I3(1).

Note Another type of binary file is the software maintenance upgrade (SMU) package file. SMUs contain fixes for specific defects. They are created to respond to immediate issues and do not include new features. SMU package files are available for download from Cisco.com and generally include the ID number of the resolved defect in the filename (for example, n9000-dk9.7.0.3.I1.1.**CSCab00001**.gbin). For more information on SMUs, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

Note Cisco also provides electronic programmable logic device (EPLD) image upgrades to enhance hardware functionality or to resolve known hardware issues. The EPLD image upgrades are independent from the Cisco NX-OS software upgrades. For more information on EPLD images and the upgrade process, see the Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes.

About ISSU

An ISSU allows you to upgrade the device software while the switch continues to forward traffic. ISSU reduces or eliminates the downtime typically caused by software upgrades. Beginning with Cisco NX-OS Release 7.0(3)I3(1), you can perform an in-service software upgrade (ISSU), also known as a nondisruptive upgrade, for some switches. (See Cisco NX-OS Software Upgrade Guidelines, on page 10 for a complete list of supported platforms.)

The default upgrade process is disruptive. Therefore, ISSU needs to be enabled using the command-line interface (CLI), as described in the configuration section of this document. Using the nondisruptive option helps ensure a nondisruptive upgrade. The guest shell is disabled during the ISSU process and it is later reactivated after the upgrade.

Enhanced ISSUs are supported for some Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3132Q-V, 31108PC-V, and 31108TC-V switches.

The following ISSU scenarios are supported on the Cisco Nexus 9000 Series switches:

- Performing standard ISSU on Top-of-Rack (ToR) switches with a single supervisor
- Performing standard ISSU on End-of-Row (EoR) switches with two supervisors
- Performing enhanced ISSU on Top-of-Rack (ToR) switches with a single supervisor

Performing Standard ISSU on Top-of-Rack (ToR) Switches with a Single Supervisor

The ToR Cisco Nexus 9300 platform switches and Cisco Nexus 3100 Series switches are the NX-OS switches with single supervisors. Performing ISSU on the Cisco Nexus 9000 and 3100 Series switches causes the supervisor CPU to reset and to load the new software version. After the CPU loads the updated version of the Cisco NX-OS software, the system restores the control plane to the previous known configuration and the runtime state and it gets in-sync with the data plane, thereby completing the ISSU process.

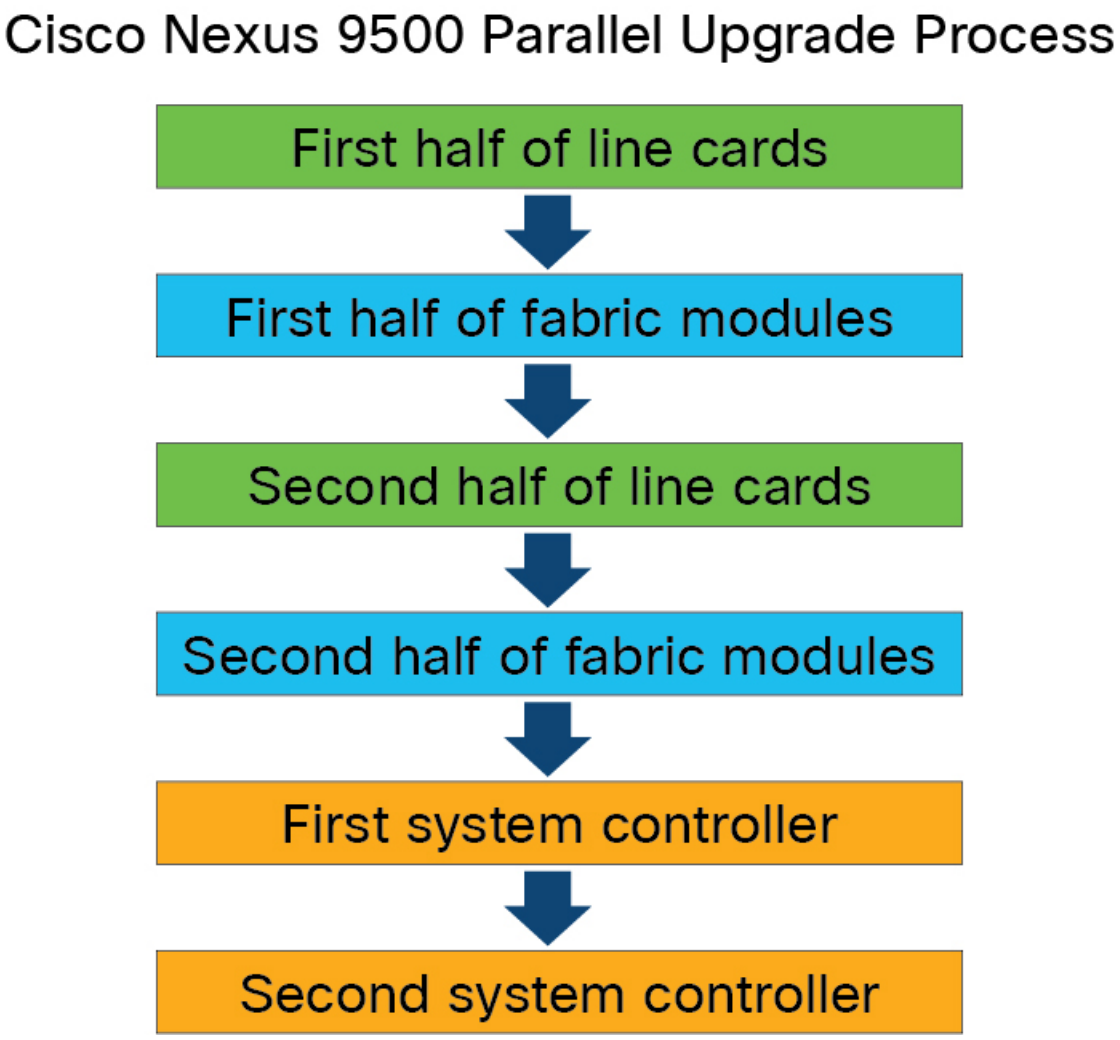
The data plane traffic is not disrupted during the ISSU process. In other words, the data plane forwards the packets while the control plane is being upgraded, any servers that are connected to the Cisco Nexus 9000 and 3100 Series switches do not see any traffic disruption. The control plane downtime during the ISSU process is approximately less than 120 seconds.

Performing Standard ISSU on End-of-Row (EoR) Switches with Two Supervisors

Cisco Nexus 9500 Series switches are the modular EoR switches that require two supervisors for ISSU. The minimum configuration required is two system controllers and two fabric modules.

Cisco Nexus 9500 Series switches support parallel upgrade as the default method. The parallel method upgrades the modules in the batches (as outlined in the following illustration) instead of upgrading the modules one after the other.

Figure 1: Parallel Upgrade Process for Cisco Nexus 9500 Series Switches



The steps for the parallel upgrade process on Cisco Nexus 9500 Series switches are:

- First the supervisors are upgraded (This procedure requires a switchover). Then the line cards, the fabric modules, the system controllers, and the FEX are upgraded.
- After the switchover is performed in a parallel upgrade, the secondary supervisor takes over. The installer determines the current line cards and the fabric modules.
- The installer then divides the components into the buckets. It places the first half of the line cards in the first bucket, the first half of the fabric modules in the second bucket, the second half of line cards in the

third bucket, the second half of the fabric modules in the fourth bucket, the first system controller in the fifth bucket, and the second system controller in the sixth bucket.

- Each bucket is upgraded successfully before an upgrade process starts for the next bucket.
- The console displays the modules with the bucket assignments and the status of the upgrade.

The user also has the option to choose a serial upgrade using the CLI.

While performing standard ISSU for the modular switches, the data plane traffic is not disrupted. The control plane downtime is approximately less than 6 Seconds.

Note The minimum requirement for a modular Cisco Nexus 9000 Series switch undergoing ISSU is two supervisors, two system controllers, and two fabric modules. The Cisco Nexus 9400 line cards can have a partially connected fabric module. In this case, if only two fabric modules are used with the Cisco Nexus 9400 line cards, the fabric modules should not be in slots 21 and 25. They should be in slots 22, 23, 24, or 26. This allows for the system to maintain high availability during ISSU.

Performing Enhanced ISSU on Top-of-Rack (ToR) Switches with a Single Supervisor

The Cisco NX-OS software normally runs directly on the hardware. However, configuring the enhanced or container based ISSU on single supervisor ToRs is accomplished by creating virtual instances of the supervisor modules and the line cards. With the enhanced ISSU, the software runs inside a separate Linux container (LXC) for the supervisors and the line cards. A third container is created as part of the ISSU procedure and it is brought up as a standby supervisor.

The virtual instances (or the Linux containers) communicate with each other using an emulated Ethernet connection. In the normal state, only two Linux containers are instantiated: vSup1 (a virtual SUP container in an active role) and vLC (a virtual linecard container). Enhanced ISSU requires 16G memory on the switch.

Note To enable booting in the enhanced ISSU (LXC) mode, use the **[no] boot mode lxc** command. This command is executed in the config mode. See the following sample configuration for more information:

```
switch(config)# boot mode lxc
Using LXC boot mode
Please save the configuration and reload system to switch into the LXC mode.
switch(config)# copy r s
[########################################] 100%
Copy complete.
```

Note When you are enabling enhanced ISSU for the first time, you have to reload the switch first.

During the software upgrade with enhanced ISSU, the supervisor control plane stays up with minimal switchover downtime disruption and the forwarding state of the network is maintained accurately during the upgrade. The supervisor is upgraded first and the line card is upgraded next.

The data plane traffic is not disrupted during the ISSU process. The control plane downtime is less than 6 seconds.

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

For information on ISSU and high availability, see the Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide.

Recommendations for Upgrading the Cisco NX-OS Software

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

Prerequisites for Upgrading the Cisco NX-OS Software

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

- For ISSU compatibility for all releases, see the Cisco NX-OS ISSU Support Matrix.
- Ensure that everyone who has access to the device or the network is not configuring the device or the network during this time. You cannot configure a device during an upgrade. Use the **show configuration session summary** command to verify that you have no active configuration sessions.
- Save, commit, or discard any active configuration sessions before upgrading or downgrading the Cisco NX-OS software image on your device. On a device with dual supervisors, the active supervisor module cannot switch over to the standby supervisor module during the Cisco NX-OS software upgrade if you have an active configuration session.
- To transfer NX-OS software images to the Nexus switch through a file transfer protocol (such as TFTP, FTP, SFTP, SCP, etc.), verify that the Nexus switch can connect to the remote file server where the NX-OS software images are stored. If you do not have a router to route traffic between subnets, ensure that the Nexus switch and the remote file server are on the same subnetwork. To verify connectivity to the remote server, transfer a test file using a file transfer protocol of your choice or use the ping command if the remote file server is configured to respond to ICMP Echo Request packets. An example of using the **ping** command to verify connectivity to a remote file server 192.0.2.100 is shown below:

```
switch# ping 192.0.2.100 vrf management
PING 192.0.2.100 (192.0.2.100): 56 data bytes
64 bytes from 192.0.2.100: icmp_seq=0 ttl=239 time=106.647 ms
64 bytes from 192.0.2.100: icmp_seq=1 ttl=239 time=76.807 ms
64 bytes from 192.0.2.100: icmp_seq=2 ttl=239 time=76.593 ms
64 bytes from 192.0.2.100: icmp_seq=3 ttl=239 time=81.679 ms
64 bytes from 192.0.2.100: icmp_seq=4 ttl=239 time=76.5 ms

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

For more information on configuration sessions, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide* specific to your release.

Prerequisites for Downgrading the Cisco NX-OS Software

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

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

Cisco NX-OS Software Upgrade Guidelines

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

- Schedule the upgrade when your network is stable and steady.
- Avoid any power interruption, which could corrupt the software image, during the installation procedure.
- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software upgrade. See the Hardware Installation Guide for your specific chassis.
- Perform the installation on the active supervisor module, not the standby supervisor module.
- The compressed image of Cisco Nexus 3000-series is hardware dependent and can only be used on the same device that it got compressed or downloaded from CCO. Do not use the Nexus 3000-series compressed image on Nexus 9000-series
- The following limitation applies to all Cisco Nexus 9200, 9300, and 9300-EX platform switches:

  A non-disruptive ISSU from Cisco NX-OS Release 7.0(3)I7(8) or 7.0(3)I7(9) to Cisco NX-OS Release 9.3(1) or 9.3(2) with NAT enabled is not supported. NAT must be disabled prior to the upgrade.
- If you are upgrading from any release to Cisco NX-OS Release 7.0(3)I7(6), 7.0(3)I7(7), or 7.0(3)I7(8) through LXC mode, it is disruptive.
- Performing a non-disruptive upgrade from Cisco NX-OS Release 7.0(3)I7(1) to 7.0(3)I7(3) (or a subsequent 7.x release) might un-configure the PBR policy. Possible workarounds are:
  - Disruptive upgrade
  - Remove all PBR policy configurations before a non-disruptive ISSU from Cisco NX-OS Release 7.0(3)I7(1) to 7.0(3)I7(3) (or a subsequent 7.x release). Perform the ISSU and re-apply the PBR configurations.
  - Perform the ISSU from Cisco NX-OS Release 7.0(3)I7(1) to 7.0(3)I7(3) (or a subsequent 7.x release) and reload the switch.
- When performing a PoAP upgrade from Cisco NX-OS Release 6.0(2)A8(11) to Cisco NX-OS Release 7.0(3)I7(8), the provisioning fails if the software image is not compacted. The PoAP script does not

support SCP compact in 6.0(2)A8(11), so a non-compacted image is copied instead, and this causes a bios upgrade failure.

To address this issue, use a pre-compacted image for PoAP from 6.0(2)A8(11). Perform a **copy scp**: *url***bootflash**: *destination-file-system* **compact** to the switch, then copy it back to the PoAP server. Start the provisioning. PoAP should pick-up the already compacted image and the provisioning should be successful.

- When upgrading from Cisco NX-OS Release 7.0(3)I6(1) or 7.0(3)I7(1) to Cisco NX-OS Release 7.0(3)I7(2) (or a subsequent 7.x release), if the Cisco Nexus 9000 Series switches are running vPC and they are connected to an IOS-based switch via Layer 2 vPC, there is a likelihood that the Layer 2 port channel on the IOS side will become error disabled. The workaround is to disable the **spanning-tree etherchannel guard misconfig** command on the IOS switch before starting the upgrade process. Once both the Cisco Nexus 9000 Series switches are upgraded, you can re-enable the command.
- If you are upgrading from Cisco NX-OS Release 7.0(3)I5(2) to Cisco NX-OS Release 7.0(3)I6(1) (or a subsequent 7.x release) using the **install all** command, BIOS will not be upgraded. When the upgrade to Cisco NX-OS Release 7.0(3)I6(1) (or a subsequent 7.x release) is complete, use the **install all** command again to complete the BIOS upgrade, if applicable.
- An upgrade performed via the **install all** command for Cisco NX-OS Release 7.0(3)I2(2b) to Release 7.0(3)I6(2) (or a subsequent 7.x release) might result in the VLANs being unable to be added to the existing FEX HIF trunk ports. To recover from this, the following steps should be performed after all FEXs have come online and the HIFs are operationally up:
  1. Enter the **copy run bootflash:fex_config_restore.cfg** command at the prompt.
  2. Enter the **copy bootflash:fex_config_restore.cfg running-config echo-commands** command at the prompt.
- In Cisco NX-OS Release 7.0(3)I6(1) and earlier, performing an ASCII replay or running the **copy file run** command on a FEX HIF configuration requires manually reapplying the FEX configuration after the FEX comes back up.
- When upgrading to Cisco NX-OS Release to 7.0(3)I7(1) (or a subsequent 7.x release) from 7.0(3)I2(x) or before and running EVPN VXLAN configuration, an intermediate upgrade to 7.0(3)I4(x) or 7.0(3)I5(x) or 7.0(3)I6(x) is required.
- When upgrading to Cisco NX-OS Release 7.0(3)I7(1) (or a subsequent 7.x release) running EVPN VXLAN and redistributing BGP EVPN into OSPF, match the route-type internal under the relevant route-map configured.
- When redistributing static routes, Cisco NX-OS requires the **default-information originate** command to successfully redistribute the default static route starting in 7.0(3)I7(6).
- Before enabling the FHS on the interface, we recommend that you carve the ifacl TCAM region on Cisco Nexus 9300 and 9500 platform switches. If you carved the ifacl TCAM region in a previous release, you must reload the system after upgrading to Cisco NX-OS Release 7.0(3)I7(1) (or a subsequent 7.x release). Uploading the system will create the required match qualifiers for the FHS TCAM region, ifacl.
- Before enabling the FHS, we recommend that you carve the ing-redirect TCAM region on Cisco Nexus 9200 and 9300-EX platform switches. If you carved the ing-redirect TCAM region in a previous release, you must reload the system after upgrading to Cisco NX-OS Release 7.0(3)I7(1) (or a subsequent 7.x release). Uploading the system will create the required match qualifiers for the FHS TCAM region, ing-redirect.

- An error occurs when you try to perform an ISSU if you changed the reserved VLAN without entering the **copy running-config save-config** and **reload** commands.
- On enhanced ISSUs from Cisco NX-OS Release 7.0(3)I5(1) or 7.0(3)I5(2) to Cisco NX-OS Release 7.0(3)I6(1) (or a subsequent 7.x release), ISSU completes, but you must reload the switch for tunnel enhancements to work. ToR ISSU does not require a reload.
- During an ISSU, there is a drop for all traffic to and from 100 Mb ports 65-66 on the Cisco Nexus 92304QC switch.
- The **install all** command is the recommended method for software upgrades and downgrades because it performs configuration compatibility checks and BIOS upgrades automatically. In contrast, changing the boot variables and reloading the device bypasses these checks and the BIOS upgrade and therefore it is not recommended.
- An enhanced ISSU can be performed only from a Cisco NX-OS Release 7.0(3)I5(1) to a later image. The upgrade will be disruptive.
- Upgrading from Cisco NX-OS Release 7.0(3)I1(2), Release 7.0(3)I1(3), or Release 7.0(3)I1(3a) requires installing a patch for Cisco Nexus 9500 platform switches only. For more information on the upgrade patch, see **Upgrade Patch Instructions**.
- When upgrading to Cisco NX-OS Release 7.0(3)I2(1) (or a subsequent 7.x release), Guest Shell automatically upgrades from 1.0 to 2.0. In the process, the contents of the guest shell 1.0 root filesystem are lost. To keep from losing important content, copy any needed files to /bootflash or an off-box location before upgrading to Cisco NX-OS Release 7.0(3)I2(1) (or a subsequent 7.x release).
- While performing an ISSU, VRRP and VRRPv3 displays the following messages:
  - If VRRPv3 is enabled:

```
2015 Dec 29 20:41:44 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR:
Service "vrrpv3" has sent the following message: Feature vrrpv3 is configured. User
 can
change vrrpv3 timers to 120 seconds or fine tune these timers based on upgrade time
 on all
Vrrp Peers to avoid Vrrp State transitions. - sysmgr
```

  - If VRRP is enabled:

```
2015 Dec 29 20:45:10 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR:
Service "vrrp-eng" has sent the following message: Feature vrrp is configured. User
 can
change vrrp timers to 120 seconds or fine tune these timers based on upgrade time
on all
Vrrp Peers to avoid Vrrp State transitions. - sysmgr
```

- Guest Shell is disabled during an ISSU and reactivated after the upgrade. Any application running in the Guest Shell will be affected.
- If you have ITD probes configured, you need to disable the ITD service (using the **shutdown** command) before upgrading to Cisco NX-OS Release 7.0(3)I3(1) (or a subsequent 7.x release). After the upgrade, enter the **feature sla sender** command to enable IP SLA for ITD probes and then the **no shutdown** command to re-enable the ITD service. (If you upgrade without shutting down the service, you can enter the **feature sla sender** command after the upgrade.)
- For Cisco Nexus 9500 platform switches with -R line cards, you must perform a write erase and reload the device to upgrade from any release prior to Cisco NX-OS Release 7.0(3)F3(4). To upgrade from

Cisco NX-OS Release 7.0(3)F3(4) or any later release, we recommend that you use the **install all** command, although we also support changing the boot variables and reloading the device.

- Detect a bad software image before performing an ISSU upgrade from an old release to a new release by checking the md5sum after downloading the new image (with seg6).
- When upgrading from Cisco Nexus 94xx, 95xx, and 96xx line cards to Cisco Nexus 9732C-EX line cards and their fabric modules, upgrade the Cisco NX-OS software before inserting the line cards and fabric modules. Failure to do so can cause a diagnostic failure on the line card and no TCAM space to be allocated. You must use the **write_erase** command followed by the **reload** command.
- If you upgrade from a Cisco NX-OS release that supports the CoPP feature to a Cisco NX-OS release that supports the CoPP feature with additional classes for new protocols, you must either run the setup utility using the **setup** command or use the **copp profile** command for the new CoPP classes to be available. For more information on these commands, see the "Configuring Control Plane Policing" chapter in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.
- For secure POAP, ensure that DHCP snooping is enabled and set firewall rules to block unintended or malicious DHCP servers. For more information on POAP, see the Cisco Nexus 9000 Series Fundamentals Configuration Guide.
- When you upgrade from an earlier release to a Cisco NX-OS release that supports switch profiles [beginning with Cisco NX-OS Release 7.0(3)I2(1)], you have the option to move some of the running-configuration commands to a switch profile. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.
- By default, the software upgrade process is disruptive.
- OpenFlow and LACP fast timer rate configurations are not supported for ISSU.
- Guest Shell is disabled during an ISSU and reactivated after the upgrade.
- ISSU supports only default hold timers for BGP peers.
- During an ISSU on a Cisco Nexus 3164Q, 31128PQ, or 9300 platform switch, all First-Hop Redundancy Protocols (FHRPs) will cause the other peer to become active if the node undergoing the ISSU is active.
- Make sure that both vPC peers are in the same mode (regular mode or enhanced mode) before performing a nondisruptive upgrade.

Note vPC peering between an enhanced ISSU mode (boot mode lxc) configured switch and a non-enhanced ISSU mode switch is not supported.

- During an ISSU, the software reload process on the first vPC device locks its vPC peer device by using CFS messaging over the vPC communications channel. Only one device at a time is upgraded. When the first device completes its upgrade, it unlocks its peer device. The second device then performs the upgrade process, locking the first device as it does so. During the upgrade, the two vPC devices temporarily run different releases of Cisco NX-OS; however, the system functions correctly because of its backward compatibility support.
- ISSU is not supported when onePK is enabled. You can run the **show feature | include onep** command to verify that this feature is disabled before performing an ISSU or enhanced ISSU.

- For Cisco Nexus 9500 platform switches with PTP enabled, we do not support non-disruptive ISSUs to Cisco NX-OS Release 7.0(3)I7(x) from any earlier release. This issue is resolved in Cisco NX-OS Release 7.0(3)I7(1), so these switches support non-disruptive ISSUs with PTP enabled from 7.0(3)I7(1) onwards.
- On performing a non-disruptive ISSU from Cisco NX-OS Release 7.0(3)I6(1) to any higher version, a traffic loss might occur based on the number of VLANs configured. To avoid traffic loss, it is recommended to increase the routing protocol's graceful restart timer to higher value. The recommended value of the graceful restart timer is 600 seconds. You can further increase or decrease this value based on the scale of the configuration.
- ISSUs are supported for the following:
  - From a major release to any associated maintenance release. For example, you can perform an ISSU from Cisco NX-OS Release 7.0(3)I6(1) to any future Cisco NX-OS Release 7.0(3)I6(x) release, where *x* is any maintenance release of the respective major release.
  - From the last two maintenance releases to the next two major releases. For example, you can perform an ISSU from Cisco NX-OS Release 7.0(3)I4(5) or 7.0(3)I4(6) to Cisco NX-OS Release 7.0(3)I5(2) or to 7.0(3)I6(1).
  - From an earlier maintenance release to the next two major releases. For example, you can perform an ISSU from Cisco NX-OS Release 7.0(3)I4(3) to Cisco NX-OS Release 7.0(3)I4(4) or 7.0(3)I4(5). However, to upgrade from Cisco NX-OS Release 7.0(3)I4(3) to 7.0(3)I6(1), you must perform two ISSUs, one from 7.0(3)I4(3) to 7.0(3)I4(4) or 4(5) and one from 7.0(3)I4(4) or 4(5) to 7.0(3)I6(1).

Note For a list of specific releases from which you can perform an ISSU, see the Cisco Nexus 9000 Series NX-OS Release Notes for your particular release.

- ISSUs are supported on the following platforms:

Series	Supported Platforms	Initial Release That Supports ISSU [1]	Features Not Supported with ISSU[2]
Cisco Nexus 9200	Standard and enhanced ISSU: Cisco Nexus 9236C, 9272Q, 92160YC-X, 92300YC, and 92304QC	Standard ISSU: 7.0(3)I6(1) Enhanced ISSU: 7.0(3)I7(3)	Segment routing, and Tetration

Series	Supported Platforms	Initial Release That Supports ISSU [1]	Features Not Supported with ISSU [2]
Cisco Nexus 9300	Standard and enhanced ISSU: Cisco Nexus 9332PQ, 9372PX, 9372PX-E, 9372TX, 9372TX-E, 9396PX, 9396TX, 93120TX, and 93128TX **Note** ISSU on one of these Cisco Nexus 9300 platform switches is supported when the switch is the spanning tree root. You can use the **show spanning-tree issu-impact** command to verify if the switch meets this criteria.	Standard ISSU: 7.0(3)I3(1) Enhanced ISSU: 7.0(3)I5(1)	Dual-homed FEX and segment routing **Note** Straight-through FEX is supported on Cisco Nexus 9372PX and 9396PX switches starting with Cisco NX-OS Release 7.0(3)I4(1).
Cisco Nexus 9300-EX	Standard and enhanced ISSU: Cisco Nexus 93108TC-EX, 93180LC-EX, and 93180YC-EX	Standard ISSU for Cisco Nexus 93108TC-EX and 93180YC-EX: 7.0(3)I6(1) Standard ISSU for Cisco Nexus 93180LC-EX: 7.0(3)I7(1) Enhanced ISSU: 7.0(3)I7(3)	Straight-through and dual-homed FEX, segment routing, and Tetration
Cisco Nexus 9300-FX	Standard ISSU: None Enhanced ISSU: None		
Cisco Nexus 9500	Standard ISSU: Cisco Nexus 9504, 9508, and 9516 with Cisco Nexus 9432PQ, 9464PX, 9464TX, 9536PQ, 9564PX, 9564TX, or 9636PQ line cards, dual supervisor modules, and a minimum of two system controllers and two fabric modules **Note** Cisco Nexus 9500 platform switches with -R, -EX, and -FX line cards do not support ISSU. Enhanced ISSU: None	Standard ISSU: 7.0(3)I3(1)	Dual-homed FEX, segment routing, and VXLAN **Note** Straight-through FEX is supported on Cisco Nexus 9500 platform switches with a Cisco Nexus 9464PX or 9564PX line card starting with Cisco NX-OS Release 7.0(3)I4(1).

Series	Supported Platforms	Initial Release That Supports ISSU [1]	Features Not Supported with ISSU[2]
Cisco Nexus 3000 that run Cisco Nexus 9000 NX-OS software	Standard ISSU: Cisco Nexus 3164Q, 31128PQ, 3132Q-V, 31108PC-V, 31108TC-V, 3232C, and 3264Q Enhanced ISSU: Cisco Nexus 3164Q, 31128PQ, 3132Q-V, 31108PC-V, and 31108TC-V	Standard ISSU for Cisco Nexus 3164Q and 31128PQ: 7.0(3)I3(1) Standard ISSU for Cisco Nexus 3132Q-V, 31108PC-V,31108TC-V, 3232C, and 3264Q: 7.0(3)I6(1) Enhanced ISSU for Cisco Nexus 3164Q, 31128PQ, 3132Q-V, 31108PC-V, and 31108TC-V: 7.0(3)I5(1)	Segment routing, and VXLAN for Cisco Nexus 3164Q and 31128PQ Segment routing for Cisco Nexus 3232C and 3264Q

[1] Enhanced ISSU is disruptive.
[2] ISSU is disruptive for these features.

Cisco NX-OS Software Downgrade Guidelines

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

- The only supported method of downgrading a Cisco Nexus 9000 Series switch is to utilize the **install all** command. Changing the boot variables, saving the configuration, and reloading the switch is not a supported method to downgrade the switch.
- Disable the Guest Shell if you need to downgrade from Cisco NX-OS Release 7.0(3)I7(7) to an earlier release.
- Software downgrades should be performed using the **install all** command. Changing the boot variables, saving the configuration, and reloading the switch is not a supported method to downgrade the switch.

Note For Cisco Nexus 9500 platform switches with -R line cards, software downgrades must be performed by doing a write erase and reloading the device.

- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software downgrade. See the Hardware Installation Guide for your specific chassis.

- Cisco NX-OS automatically installs and enables the guest shell by default. However, if the device is reloaded with a Cisco NX-OS image that does not provide guest shell support, the existing guest shell is automatically removed and a %VMAN-2-INVALID_PACKAGE message is issued. As a best practice, remove the guest shell with the **guestshell destroy** command before downgrading to an earlier Cisco NX-OS image.
- You must delete the switch profile (if configured) when downgrading from a Cisco NX-OS release that supports switch profiles to a release that does not. For more information, see the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.
- Software downgrades are disruptive. In-service software downgrades (ISSDs), also known as nondisruptive downgrades, are not supported.
- Downgrading with PVLANs (Private VLANs) configured is only supported with Cisco NX-OS 6.1(2)I3(4x) releases.
- For a boot-variable change and reload to Cisco NX-OS Release 7.0(3)I1(1x), the PVLAN process is not brought up, and the PVLAN ports are kept down. For a boot-variable change to the Cisco NX-OS Release 6.1(2)I3(3) and earlier, an ASCII replay will be tried, but feature PVLANs and other PVLAN configurations will fail.

ISSU Upgrade Compatibility

For ISSU compatibility for all releases, see the Cisco NX-OS ISSU Support Matrix.

Upgrade Patch Instructions

On Cisco Nexus 9500 series switches only, a software upgrade from Cisco NX-OS Release 7.0(3)I1(2), 7.0(3)I1(3), or 7.0(3)I1(3a) to any other Cisco NX-OS release requires installing two patches prior to upgrading using the **install all** command. These patches are available for each respective release and can be downloaded using the links below.

Caution Failing to follow this procedure could require console access in order to recover the switch after the upgrade.

Note These patches are only for upgrading. After the upgrade, the patch is automatically removed. If you decide not to upgrade after installing the patches, do not deactivate it. Deactivating the patch may cause a bios_daemon crash.

Cisco NX-OS Release 7.0(3)I1(2) Upgrade Patch

Cisco NX-OS Release 7.0(3)I1(3) Upgrade Patch

Cisco NX-OS Release 7.0(3)I1(3a) Upgrade Patch

To install these patches prior to upgrading using the install all command, follow the instructions shown below. An example is demonstrated below with an NX-OS software patch and upgrade from 7.0(3)I1(2) to 7.0(3)I7(1):

1. Add both patches with the **install add bootflash:**{*patch-file.bin*} command.

```
switch(config)# install add bootflash:n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 16 completed successfully at Thu Mar  3 04:24:13 2016
switch(config)# install add bootflash:n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 17 completed successfully at Thu Mar  3 04:24:43 2016
```

2. Activate both patches with the **install activate** {*patch-file.bin*} command.

```
switch(config)# install activate n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 18 completed successfully at Thu Mar  3 04:28:38 2016
switch (config)# install activate n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 19 completed successfully at Thu Mar  3 04:29:08 2016
```

3. Commit both patches with the **install commit** {*patch-file.bin*} command.

```
switch(config)# install commit n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 20 completed successfully at Thu Mar  3 04:30:38 2016
switch (config)# install commit n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 21 completed successfully at Thu Mar  3 04:31:16 2016
```

4. Proceed with an NX-OS software upgrade to the desired target release with the **install all** command.

```
switch (config)# install all nxos bootflash:nxos.7.0.3.I7.1.bin
Installer will perform compatibility check first. Please wait.
uri is: /nxos.7.0.3.I7.1.bin
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I7.1.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
```

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

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.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
     6       yes      disruptive         reset  Incompatible image
     8       yes      disruptive         reset  Incompatible image
     9       yes      disruptive         reset  Incompatible image
    10       yes      disruptive         reset  Incompatible image
    11       yes      disruptive         reset  Incompatible image
    14       yes      disruptive         reset  Incompatible image
    15       yes      disruptive         reset  Incompatible image
    16       yes      disruptive         reset  Incompatible image
    21       yes      disruptive         reset  Incompatible image
    22       yes      disruptive         reset  Incompatible image
    23       yes      disruptive         reset  Incompatible image
    24       yes      disruptive         reset  Incompatible image
    25       yes      disruptive         reset  Incompatible image
    26       yes      disruptive         reset  Incompatible image
    27       yes      disruptive         reset  Incompatible image
    28       yes      disruptive         reset  Incompatible image
    29       yes      disruptive         reset  Incompatible image
    30       yes      disruptive         reset  Incompatible image

Images will be upgraded according to following table:
Module  Image               Running-Version(pri:alt)         New-Version  Upg-Required
------  -----  ------------------------------------  ------------------  ------------
     1  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
     1   bios                v01.42(00:v01.42(00           v01.48(00           yes
     6  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
     6   bios                v01.48(00:v01.48(00           v01.48(00            no
     8  lcn9k                          7.0(3)I1(2)         7.0(3)I7(1)           yes
     8   bios                v01.48(00:v01.29(00           v01.48(00            no
```

```
     9  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
     9   bios                    v01.48(00:v01.35(00           v01.48(00            no
    10  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    10   bios                    v01.48(00:v01.42(00           v01.48(00            no
    11  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    11   bios                    v01.48(00:v01.52(00           v01.48(00            no
    14  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    14   bios                    v01.48(00:v01.48(00           v01.48(00            no
    15  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    15   bios                    v01.48(00:v01.40(00           v01.48(00            no
    16  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    16   bios                    v01.48(00:v01.42(00           v01.48(00            no
    21  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    21   bios                    v01.48(00:v01.42(00           v01.48(00            no
    22  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    22   bios                    v01.48(00:v01.40(00           v01.48(00            no
    23  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    23   bios                    v01.48(00:v01.40(00           v01.48(00            no
    24  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    24   bios                    v01.48(00:v01.40(00           v01.48(00            no
    25  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    25   bios                    v01.48(00:v01.40(00           v01.48(00            no
    26  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    26   bios                    v01.48(00:v01.40(00           v01.48(00            no
    27   nxos                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    27   bios  v08.06(09/10/2014):v08.18(08/11/2015)  v08.26(01/12/2016)           yes
    28   nxos                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    28   bios  v08.06(09/10/2014):v08.26(01/12/2016)  v08.26(01/12/2016)           yes
    29  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    29   bios                    v01.48(00:v01.35(00           v01.48(00            no
    30  lcn9k                          7.0(3)I1(2)          7.0(3)I7(1)           yes
    30   bios                    v01.48(00:v01.35(00           v01.48(00            no

Switch will be reloaded for disruptive upgrade.
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:/nxos.7.0.3.I7.1.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 6: 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.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 11: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 14: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 15: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 16: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 21: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 22: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 23: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 24: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 25: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 26: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 27: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 28: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 29: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 30: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS
Finishing the upgrade, switch will reboot in 10 seconds.
switch(config)#
User Access Verification
```

```
switch login:
[ 2644.917727] [1456980048]  writing reset reason 88,

CISCO SWITCH Ver 8.26

CISCO SWITCH Ver 8.26
Memory Size (Bytes): 0x0000000080000000 + 0x0000000380000000
 Relocated to memory
Time: 6/3/2016  4:41:8
Detected CISCO IOFPGA
Booting from Primary Bios
Code Signing Results: 0x0
Using Upgrade FPGA
FPGA Revision        : 0x27
FPGA ID             : 0x1168153
FPGA Date           : 0x20160111
Reset Cause Register: 0x22
Boot Ctrl Register  : 0x60ff
EventLog  Register1 : 0x2000000
EventLog  Register2 : 0xfbe77fff
Version 2.16.1240. Copyright (C) 2013 American Megatrends, Inc.
Board type  1
IOFPGA @ 0xe8000000
SLOT_ID @ 0x1b
Standalone chassis
check_bootmode: grub: Continue grub
Trying to read config file /boot/grub/menu.lst.local from (hd0,4)
 Filesystem type is ext2fs, partition type 0x83

Booting bootflash:/nxos.7.0.3.I7.1.bin ...
Booting bootflash:/nxos.7.0.3.I7.1.bin
Trying diskboot
 Filesystem type is ext2fs, partition type 0x83
IOFPGA ID: 1168153
Image valid


Image Signature verification was Successful.

Boot Time: 3/3/2016  4:41:44
INIT: version 2.88 booting
Unsquashing rootfs ...

Loading IGB driver ...
Installing SSE module ... done
Creating the sse device node ... done
Loading I2C driver ...
Installing CCTRL driver for card_type 3 ...
CCTRL driver for card_index 21000 ...
old data: 4000004 new data: 1
Not Micron SSD...

Checking all filesystems.......
Installing default sprom values ...
 done.Configuring network ...
Installing LC netdev ...
Installing psdev ...
Installing veobc ...
Installing OBFL driver ...
mounting plog for N9k!
tune2fs 1.42.1 (17-Feb-2012)
Setting reserved blocks percentage to 0% (0 blocks)
Starting portmap daemon...
```

```
creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Saving image for img-sync ...
Loading system software
Installing local RPMS
Patch Repository Setup completed successfully
dealing with default shell..
file /proc/cmdline found, look for shell
unset shelltype, nothing to do..
user add file found..edit it
Uncompressing system image: Thu Jun 3 04:42:11 UTC 2016
blogger: nothing to do.

..done Thu Mar 3 04:42:11 UTC 2016
Creating /dev/mcelog
Starting mcelog daemon
Overwriting dme stub lib
Replaced dme stub lib
INIT: Entering runlevel: 3
Running S93thirdparty-script...

2016 Mar  3 04:42:37 switch%$ VDC-1 %$  %USER-2-SYSTEM_MSG: <<%USBHSD-2-MOUNT>> logflash:
 online  - usbhsd
2016 Mar  3 04:42:37 switch%$ VDC-1 %$ Mar  3 04:42:37 %KERN-2-SYSTEM_MSG: [   12.509615]
 hwport mode=6 - kernel
2016 Mar  3 04:42:40 switch%$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Installing virtual service
 'guestshell+'
2016 Mar  3 04:42:40 switch%$ VDC-1 %$  %DAEMON-2-SYSTEM_MSG:
<<%ASCII-CFG-2-CONF_CONTROL>> Binary restore - ascii-cfg[13904]
2016 Mar  3 04:42:40 switch%$ VDC-1 %$  %DAEMON-2-SYSTEM_MSG:
<<%ASCII-CFG-2-CONF_CONTROL>> Restore DME database - ascii-cfg[13904]
2016 Mar  3 04:42:42 switch%$ VDC-1 %$ netstack: Registration with cli server complete
2016 Mar  3 04:43:00 switch%$ VDC-1 %$ %USER-2-SYSTEM_MSG: ssnmgr_app_init called on
ssnmgr up - aclmgr
2016 Mar  3 04:43:09 switch%$ VDC-1 %$ %USER-0-SYSTEM_MSG: end of default policer - copp
2016 Mar  3 04:43:10 switch%$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Install success virtual
service 'guestshell+'; Activating
2016 Mar  3 04:43:10 switch%$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Activating virtual
service 'guestshell+'
2016 Mar  3 04:43:13 switch%$ VDC-1 %$ %CARDCLIENT-2-FPGA_BOOT_PRIMARY: IOFPGA booted
from Primary
2016 Mar  3 04:43:18 switch%$ VDC-1 %$ %USER-2-SYSTEM_MSG: IPV6 Netlink thread init
successful  - icmpv6
2016 Mar  3 04:43:19 switch%$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come online


User Access Verification
switchlogin:
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 1
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 6
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 8
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 9
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 10
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 11
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 14
```

```
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 15
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 16
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 21
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 22
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 23
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 24
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 25
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 26
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 28
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 29
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 30
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 1 ok (Serial
number XYZ284014RR)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 1 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 2 ok (Serial
number XYZ285111TC)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 2 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 3 ok (Serial
number XYZ285111QQ)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 3 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 4 ok (Serial
number XYZ284014TI)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 4 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 5 ok (Serial
number XYZ284014TS)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 5 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 1
(Fan1(sys_fan1) fan) ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 2
(Fan2(sys_fan2) fan) ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 3
(Fan3(sys_fan3) fan) ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 30 detected (Serial
 number ABC1234DE56) Module-Type System Controller Model N9K-SC-A
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 30 powered up (Serial
 number ABC1234DE56)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 28 detected (Serial
 number :unavailable) Module-Type Supervisor Module Model :unavailable
2016 Mar  3 04:43:58 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 29 detected (Serial
 number ABC1234DEFG) Module-Type System Controller Model N9K-SC-A
2016 Mar  3 04:43:58 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 29 powered up (Serial
 number ABC1234DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 21 detected (Serial
 number ABC1213DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 22 detected (Serial
 number ABC1211DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 21 powered up (Serial
 number ABC1213DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 22 powered up (Serial
 number ABC1211DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 23 detected (Serial
 number ABC1234D5EF) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 23 powered up (Serial
```

```
 number ABC1234D5EF)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 24 detected (Serial
 number ABC1211DE3F) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 24 powered up (Serial
 number ABC1211DE3F)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 25 detected (Serial
 number ABC1213DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 25 powered up (Serial
 number ABC1213DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 26 detected (Serial
 number ABC1211DE34) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 26 powered up (Serial
 number ABC1211DE34)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 1. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 1 detected (Serial
 number ABC1217DEFG) Module-Type 32p 40G Ethernet Module Model N9K-X9432PQ
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 1 powered up (Serial
 number ABC1217DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 9. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 9 detected (Serial
 number ABC1236D4E5) Module-Type 48x1/10G-T 4x40G Ethernet Module Model N9K-X9564TX
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 9 powered up (Serial
 number ABC1236D4E5)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 10. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 10 detected (Serial
 number ABC1217EFGH) Module-Type 32p 40G Ethernet Module Model N9K-X9432PQ
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 10 powered up (Serial
 number ABC1217EFGH)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 11. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 11 detected (Serial
 number ABC123DEF4) Module-Type 36p 40G Ethernet Module Model N9K-X9536PQ
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 11 powered up (Serial
 number ABC123DEF4)
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 15. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 15 detected (Serial
 number ABC1212DEFG) Module-Type 36p 40G Ethernet Module Model N9K-X9536PQ
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 15 powered up (Serial
 number ABC1212DEFG)
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 16. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 16 detected (Serial
 number ABCD1235DEFG) Module-Type 48x1/10G SFP+ 4x40G Ethernet Module Model N9K-X9464PX
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 16 powered up (Serial
 number ABCD1235DEFG)
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 14. Ejector based shutdown enabled
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 14 detected (Serial
 number ABC9876DE5F) Module-Type 8p 100G Ethernet Module Model N9K-X9408PC-CFP2
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 14 powered up (Serial
 number ABC9876DE5F)
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 6. Ejector based shutdown enabled
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 6 detected (Serial
 number ABC9876DE3F) Module-Type 8p 100G Ethernet Module Model N9K-X9408PC-CFP2
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 6 powered up (Serial
 number ABC9876DE3F)
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 8. Ejector based shutdown enabled
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 8 detected (Serial
```

```
 number ABC3456D7E8) Module-Type 48x1/10G-T 4x40G Ethernet Module Model N9K-X9564TX
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 8 powered up (Serial
 number ABC3456D7E8)
2016 Mar  3 04:44:56 switch%$ VDC-1 %$ %USBHSD-STANDBY-2-MOUNT: logflash: online
2016 Mar  3 04:47:31 switch%$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL: System ready
2016 Mar  3 04:47:51 switch%$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully activated
 virtual service 'guestshell+'
2016 Mar  3 04:47:51 switch%$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED: The guest shell has
been enabled. The command 'guestshell' may be used to access it, 'guestshell destroy'
to remove it.

User Access Verification

switch#  show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2016, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.26
  NXOS: version 7.0(3)I7(1)
  BIOS compile time:  06/12/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I7.1.bin
  NXOS compile time:  2/8/2016 20:00:00 [02/09/2016 05:18:17]


Hardware
  cisco Nexus9000 C9516 (16 Slot) Chassis ("Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2403 0 @ 1.80GHz with 16401664 kB of memory.
  Processor Board ID SAL1745FTPW

  Device name: switch
  bootflash:   20971520 kB
Kernel uptime is 0 day(s), 0 hour(s), 8 minute(s), 13 second(s)

Last reset at 235176 usecs after  Thu Mar  3 04:40:48 2016

  Reason: Reset due to upgrade
  System version: 7.0(3)I1(2)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
switch#
```

Configuring Enhanced ISSU

Beginning with Cisco NX-OS Release 7.0(3)I5(1), you can enable or disable enhanced (LXC) ISSU.

Note After you upgrade to Cisco NX-OS Release 7.0(3)I5(1) from an earlier release, you can enable enhanced ISSU for use with future upgrades.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config#)`
		Enters global configuration mode.

Step 2	[**no**] **boot mode lxc**
	Example:
	`switch(config)# boot mode lxc`
	`Using LXC boot mode`
	Example:
	`switch(config)# no boot mode lxc`
	`Using normal native boot mode`
		Enables or disables enhanced (LXC) ISSU.

Step 3	(Optional) **show boot mode**
	Example:
	`switch(config)# show boot mode`
	`LXC boot mode is enabled`
	Example:
	`switch(config)# show boot mode`
	`LXC boot mode is disabled`
		Shows whether enhanced (LXC) ISSU is enabled or disabled.

Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the running configuration to the startup configuration.

Step 5	**reload**
	Example:
	`switch(config)# reload`
	`This command will reboot the system. (y/n)?  [n]`
	`Y`
	`loader>`
		Reloads the device. When prompted, press **Y** to confirm the reboot.

What to do next

Follow the instructions in Upgrading the Cisco NX-OS Software, on page 28. Make sure to choose the **non-disruptive** option if you want to perform an enhanced or regular ISSU.

Upgrading the Cisco NX-OS Software

Use this procedure to upgrade a Cisco Nexus 9000 Series switch to a Cisco NX-OS 7.x release.

Note The upgrade instructions are different for Cisco Nexus 9500 platform switches with an -R line card. See Upgrading the Cisco NX-OS Software for Cisco Nexus 9500 Platform Switches with -R Line Cards, on page 32.

Note If an error message appears during the upgrade, the upgrade will fail because of the reason indicated. See the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide for a list of possible causes and solutions.

Step 1 **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.

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

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

```
switch# dir bootflash:
49152    Dec 10 14:43:39 2015 lost+found/
80850712 Dec 10 15:57:44 2015 n9000-dk9.7.0.3.I1.1.bin
...

Usage for bootflash://sup-local
 4825743360 bytes used
16312102912 bytes free
21137846272 bytes total
```

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

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

```
switch# delete bootflash:n9000-dk9.7.0.3.I1.1.bin
```

Step 5 Verify that there is space available on the standby supervisor module.

```
switch# dir bootflash://sup-standby/
49152    Dec 10 14:43:39 2015 lost+found/
80850712 Dec 10 15:57:44 2015 n9000-dk9.7.0.3.I1.1.bin
...

Usage for bootflash://sup-standby
 4825743360 bytes used
16312102912 bytes free
```

```
21137846272 bytes total
```

Step 6 If you need more space on the standby supervisor module, delete any unnecessary files to make space available.

```
switch# delete bootflash://sup-standby/n9000-dk9.7.0.3.I1.1.bin
```

Step 7 Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Step 8 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/nxos.7.0.3.I2.1.bin
bootflash:nxos.7.0.3.I2.1.bin
```

Step 9 Display the SHA256 checksum for the file to verify the operating system integrity and ensure that the downloaded image is safe to install and use.

```
switch# show file bootflash://sup-1/nxos.7.0.3.I2.1.bin sha256sum
5214d563b7985ddad67d52658af573d6c64e5a9792b35c458f5296f954bc53be
```

Step 10 Check the impact of upgrading the software before actually performing the upgrade.

```
switch# show install all impact nxos bootflash:nxos.7.0.3.I2.1.bin
Installer will perform compatibility check first. Please wait.
uri is: /nxos.7.0.3.I2.1.bin
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I2.1.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I2.1.bin.
[####################] 100% -- SUCCESS
```

```
Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I2.1.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  Reset due to single supervisor
    21       yes      disruptive         reset  Reset due to single supervisor
    22       yes      disruptive         reset  Reset due to single supervisor
    23       yes      disruptive         reset  Reset due to single supervisor
    24       yes      disruptive         reset  Reset due to single supervisor
    25       yes      disruptive         reset  Reset due to single supervisor
    26       yes      disruptive         reset  Reset due to single supervisor
    27       yes      disruptive         reset  Reset due to single supervisor
    29       yes      disruptive         reset  Reset due to single supervisor
    30       yes      disruptive         reset  Reset due to single supervisor

Images will be upgraded according to following table:
Module    Image    Running-Version(pri:alt)           New-Version  Upg-Required
------  -------  -------------------------  --------------------  ------------
     1    lcn9k                7.0(3)I1(1)           7.0(3)I2(1)           yes
     1     bios         v01.42(00:v01.42(00             v01.42(00           no
    21    lcn9k                7.0(3)I1(1)           7.0(3)I2(1)           yes
    21     bios         v01.42(00:v01.42(00             v01.42(00           no
    22    lcn9k                7.0(3)I1(1)           7.0(3)I2(1)           yes
    22     bios         v01.42(00:v01.42(00             v01.42(00           no
    23    lcn9k                7.0(3)I1(1)           7.0(3)I2(1)           yes
    23     bios         v01.42(00:v01.42(00             v01.42(00           no
    24    lcn9k                7.0(3)I1(1)           7.0(3)I2(1)           yes
    24     bios         v01.42(00:v01.42(00             v01.42(00           no
    25    lcn9k                7.0(3)I1(1)           7.0(3)I2(1)           yes
    25     bios         v01.42(00:v01.42(00             v01.42(00           no
    26     nxos                7.0(3)I1(1)           7.0(3)I2(1)           no
    26     bios         v01.42(00:v01.42(00             v01.42(00           no
    27     nxos                7.0(3)I1(1)           7.0(3)I2(1)           no
    27     bios         v01.42(00:v01.42(00             v01.42(00           no
    29    lcn9k                7.0(3)I1(1)           7.0(3)I2(1)           yes
    29     bios         v01.42(00:v01.42(00             v01.42(00           no
    30    lcn9k                7.0(3)I1(1)           7.0(3)I2(1)           yes
    30     bios         v01.42(00:v01.42(00             v01.42(00           no
```

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

Reason Field Message — in Cisco NX-OS Release 7.0(3)I3(1)	Reason Field Message — in Cisco NX-OS Release 7.0(3)I4(1) or a Later Release	Description
Incompatible image	Incompatible image for ISSU	The Cisco NX-OS image to which you are attempting to upgrade does not support ISSU.

Reason Field Message — in Cisco NX-OS Release 7.0(3)I3(1)	Reason Field Message — in Cisco NX-OS Release 7.0(3)I4(1) or a Later Release	Description
Hitless upgrade is not supported	Default upgrade is not hitless	By default, the software upgrade process is disruptive. You must configure the **non-disruptive** option to perform an ISSU.

Step 11 Save the running configuration to the startup configuration.

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

Step 12 Upgrade the Cisco NX-OS software using the **install all nxos bootflash:***filename* [**no-reload** | **non-disruptive** | **non-interruptive** | **serial**] command.

```
switch# install all nxos bootflash:nxos.7.0.3.I2.1.bin
```

The following options are available:

- **no-reload**—Exits the software upgrade process before the device is reloaded.
- **non-disruptive**—Performs an in-service software upgrade (ISSU) to prevent the disruption of data traffic. (By default, the software upgrade process is disruptive.)
- **non-interruptive**—Upgrades the software without any prompts. This option skips all error and sanity checks.
- **serial**—Upgrades the I/O modules in Cisco Nexus 9500 Series switches one at a time. (By default, the I/O modules are upgraded in parallel, which reduces the overall upgrade time. Specifically, the I/O modules are upgraded in parallel in this order: the first half of the line cards and fabric modules, the second half of the line cards and fabric modules, the first system controller, the second system controller.)

Note If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.

Step 13 (Optional) Display the entire upgrade process.

```
switch# show install all status
```

Step 14 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```

Step 15 (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

Upgrading the Cisco NX-OS Software for Cisco Nexus 9500 Platform Switches with -R Line Cards

Use this procedure to upgrade a Cisco Nexus 9500 platform switch with an -R line card to a Cisco NX-OS 7.x release.

SUMMARY STEPS

1. **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.
2. Log in to the device on the console port connection.
3. Ensure that the required space is available for the image file to be copied.
4. If you need more space on the active supervisor module, delete unnecessary files to make space available.
5. Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.
6. Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.
7. Display the SHA256 checksum for the file to verify the operating system integrity and ensure that the downloaded image is safe to install and use.
8. Upgrade the Cisco NX-OS software using the **boot nxos bootflash:***filename* command.
9. Save the running configuration to the startup configuration.
10. Erase the startup configuration file.
11. Reload the switch.
12. (Optional) Log in and verify that the device is running the required software version.
13. (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

DETAILED STEPS

Step 1 **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 9 Save the running configuration to the startup configuration.

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

Step 10 Erase the startup configuration file.

```
switch# write erase
```

Step 11 Reload the switch.

```
switch# reload
```

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

```
switch# show version
```

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

Upgrade Process for vPCs

Upgrade Process for a vPC Topology on the Primary Switch

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

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

1. **The install all command issued on the vPC primary switch triggers the installation upgrade.**

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

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

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

Upgrade Process for a vPC Topology on the Secondary Switch

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

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

Downgrading to an Earlier Software Release

Use this procedure to downgrade a Cisco Nexus 9000 Series switch to a Cisco NX-OS 7.x release.

Note The downgrade instructions are different for Cisco Nexus 9500 platform switches with an -R line card. See Downgrading the Cisco NX-OS Software for Cisco Nexus 9500 Platform Switches with -R Line Cards, on page 37.

Note If an error message appears during the downgrade, the downgrade will fail because of the reason indicated. See the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide for a list of possible causes and solutions.

Step 1 **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.

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

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

```
switch# dir bootflash:
49152 Aug 01 14:43:39 2015 lost+found/
80850712 Aug 01 15:57:44 2015 nxos.7.0.3.I2.1.bin
...

Usage for bootflash://sup-local
 4825743360 bytes used
16312102912 bytes free
21137846272 bytes total
```

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

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

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

```
switch# copy scp://user@scpserver.cisco.com//download/n9000-dk9.7.0.3.I1.1.bin
bootflash:n9000-dk9.7.0.3.I1.1.bin
```

Step 6 Check for any software incompatibilities.

```
switch# show incompatibility-all nxos bootflash:n9000-dk9.7.0.3.I1.1.bin
Checking incompatible configuration(s)
No incompatible configurations
```

The resulting output displays any incompatibilities and remedies.

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

Step 8 Check for any hardware incompatibilities.

```
switch# show install all impact nxos bootflash:n9000-dk9.7.0.3.I1.1.bin
Installer will perform compatibility check first. Please wait.
uri is: /n9000-dk9.7.0.3.I1.1.bin
Installer is forced disruptive
```

```
Verifying image bootflash:/n9000-dk9.7.0.3.I1.1.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.7.0.3.I1.1.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  Reset due to single supervisor
    21       yes      disruptive         reset  Reset due to single supervisor
    22       yes      disruptive         reset  Reset due to single supervisor
    23       yes      disruptive         reset  Reset due to single supervisor
    24       yes      disruptive         reset  Reset due to single supervisor
    25       yes      disruptive         reset  Reset due to single supervisor
    26       yes      disruptive         reset  Reset due to single supervisor
    27       yes      disruptive         reset  Reset due to single supervisor
    29       yes      disruptive         reset  Reset due to single supervisor
    30       yes      disruptive         reset  Reset due to single supervisor

Images will be upgraded according to following table:
Module   Image              Running-Version(pri:alt)         New-Version  Upg-Required
------  ------  -----------------------------------  ------------------  ------------
     1   lcn9k                           7.0(3)I2(1)         7.0(3)I1(1)           yes
     1    bios                             v01.42(00 v01.42(00:v01.42(00           no
    21   lcn9k                           7.0(3)I2(1)         7.0(3)I1(1)           yes
    21    bios                             v01.42(00 v01.42(00:v01.42(00           no
```

```
22   lcn9k                          7.0(3)I2(1)          7.0(3)I1(1)           yes
22    bios                            v01.42(00 v01.42(00:v01.42(00           no
23   lcn9k                          7.0(3)I2(1)          7.0(3)I1(1)           yes
23    bios                            v01.42(00 v01.42(00:v01.42(00           no
24   lcn9k                          7.0(3)I2(1)          7.0(3)I1(1)           yes
24    bios                            v01.42(00 v01.42(00:v01.42(00           no
25   lcn9k                          7.0(3)I2(1)          7.0(3)I1(1)           yes
25    bios                            v01.42(00 v01.42(00:v01.42(00           no
26    nxos                           7.0(3)I2(1)          7.0(3)I1(1)           no
26    bios                            v01.42(00 v01.42(00:v01.42(00           no
27    nxos                           7.0(3)I2(1)          7.0(3)I1(1)           no
27    bios                            v01.42(00 v01.42(00:v01.42(00           no
29   lcn9k                          7.0(3)I2(1)          7.0(3)I1(1)           yes
29    bios                            v01.42(00 v01.42(00:v01.42(00           no
30   lcn9k                          7.0(3)I2(1)          7.0(3)I1(1)           yes
30    bios                            v01.42(00 v01.42(00:v01.42(00           no
```

Step 9 Power off any unsupported modules.

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

Step 10 Save the running configuration to the startup configuration.

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

Step 11 Downgrade the Cisco NX-OS software.

```
switch# install all nxos bootflash:n9000-dk9.7.0.3.I1.1.bin
```

Note If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.

Step 12 (Optional) Display the entire downgrade process.

Example:

```
switch# show install all status
```

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

```
switch# show version
```

Downgrading the Cisco NX-OS Software for Cisco Nexus 9500 Platform Switches with -R Line Cards

Use this procedure to downgrade a Cisco Nexus 9000 Series switch to a Cisco NX-OS 7.x release.

SUMMARY STEPS

1. **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.
2. Log in to the device on the console port connection.
3. Verify that the image file for the downgrade is present on the active supervisor module bootflash:.
4. If the software image file is not present, log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.
5. Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.
6. Check for any software incompatibilities.
7. Disable any features that are incompatible with the downgrade image.
8. Power off any unsupported modules.
9. Downgrade the Cisco NX-OS software.
10. Save the running configuration to the startup configuration.
11. Erase the startup configuration file.
12. Reload the switch.
13. (Optional) Log in and verify that the device is running the required software version.

DETAILED STEPS

Step 1 **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.

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

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

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

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

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

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

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

Step 6 Check for any software incompatibilities.

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

The resulting output displays any incompatibilities and remedies.

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

Step 8 Power off any unsupported modules.

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

Step 9 Downgrade the Cisco NX-OS software.

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

Step 10 Save the running configuration to the startup configuration.

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

Step 11 Erase the startup configuration file.

```
switch# write erase
```

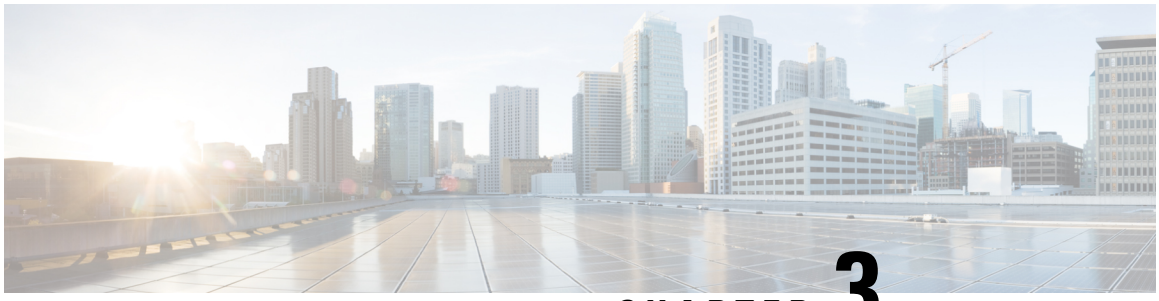
Step 12 Reload the switch.

Example:

```
switch# reload
```

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

```
switch# show version
```



CHAPTER 3

Upgrading the Cisco NX-OS Software Using Fast Reload

This chapter describes how to upgrade the Cisco NX-OS software on a Cisco Nexus 3164Q switch using fast reload. It contains the following sections:

About Fast Reload

Attention Starting with Cisco NX-OS Release 6.1(2)I3(4) and 7.0(3)I2(1), the Cisco Nexus 3164Q switch supports fast reload, but support is disabled starting with Cisco NX-OS Release 7.0(3)I4(1). The Cisco Nexus 9000 Series switches do not support this feature in any release.

The fast reload feature enables you to reboot the switch faster than with the **reload** command. You can also use fast reload to upgrade the software on the switch.

During a fast reload, the NXOS software image that runs on the CPU reloads the new image and runs it without a CPU or firmware reset. Although traffic is briefly disrupted during a fast reload, this feature enables the switch to reload faster than during a cold reboot.

You can use fast reload in a non-interruptive mode, which runs the installation process without any prompts, or with BGP graceful restart for BGP-compatible peers.

Fast Reload Sequence of Events

The following sequence of events occurs when you perform a fast reload using the **fast-reload** command:

1. The switch loads the NXOS software image and upgrades the kernel. All applications undergo a stateless cold reboot and are restarted through the startup configuration.

2. The control plane is disrupted. During this disruption, all control protocol communication stops. The control plane disruption is less than 90 seconds.
3. After the control plane disruption, all control plane applications undergo a stateless cold reboot and do not retain their state. The new configuration is applied when the switch reloads.
4. The data plane is disrupted. The data plane disruption is less than 30 seconds.
5. On the forwarding plane, all links become unavailable, and the data plane does not retain its state after reload. Traffic forwarding is resumed within 30 seconds.

Prerequisites for Fast Reload

Fast reload has the following prerequisites:

- Verify that sufficient space is available in the bootflash.
- To allow a fast reload, make sure that Link Aggregation Control Protocol (LACP) fast timers are not configured.

Guidelines and Limitations for Fast Reload

Fast reload has the following guidelines and limitations:

- Only the Cisco Nexus 3164Q switch supports fast reload. The Cisco Nexus 9000 Series switches and the Cisco Nexus 31128PQ switch do not support this feature.
- Using fast reload to downgrade the Cisco NX-OS software is not supported. To downgrade the software, use the **install all** command.
- Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. You cannot configure the switch during a fast reload. Use the **show configuration session summary** command to verify that you have no active configuration sessions.
- Save, commit, or discard any active configuration sessions before performing a fast reload. Any active configuration sessions will be deleted without warning.
- Make any topology changes (such as Spanning Tree Protocol changes) before you perform a fast reload. However, do not make changes to the Layer 2 and routing topologies.
- Do not insert or remove any fans or power supplies during a fast reload.
- Schedule the fast reload when your network is stable and steady.
- BIOS upgrades are not supported by fast reload.
- The CPU stops responding between control plane disruption and data plane disruption.
- The **copy** *configuration-file* **startup-config** command is supported with fast reload for a limited set of configurations.
- Ensure that the username is specified in the configuration file before you perform a **copy** *configuration-file* **startup-config** followed by the **fast-reload** or **reload** command. Otherwise, you will not be able to the access the switch and will need to complete the password recovery procedure to get the system back

online. For information on the password recovery procedure, see the "Power Cycling the Device to Recover the Administrator Password" section in the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide.

- Fast reload currently supports the following two configuration profiles:

  Fast-reload profile 1

  - 48 Layer 2 links
  - 1 VLAN and SVI
  - 16 Layer 3 ECMP links
  - 6000 IPv4 LPM routes, 3000 IPv6 LPM routes, 200 IPv4 VIPs, and 200 IPv6 VIPs
  - 2000 IPv4 ARPs and 2000 IPv6 neighbor discovery (ND)

  Fast-reload profile 2

  - 24 Layer 2 port channels with two members each
  - 24 VLANs and SVIs
  - 8 Layer 3 port-channel ECMPs with two members each
  - 6000 IPv4 LPM routes, 3000 IPv6 LPM routes, 50 IPv4 VIPs, and 50 IPv6 VIPs
  - 2000 IPv4 ARPs and 2000 IPv6 neighbor discovery (ND)

Performing a Fast Reload and Upgrading the Cisco NX-OS Software

You can use this procedure to reboot the device faster than during a cold reboot. If you specify a software image, the software on the switch is upgraded.

Before you begin

Ensure that you have a working software image and that you have analyzed the impact of the fast reload operation.

Step 1 Log in to the switch.

Step 2 Use the **fast-reload** [**save-config**] [**trigger-gr**] [**nxos bootflash:***nxos-image-name*] [**non-interruptive**] command to perform a fast reload.

Example:

```
switch# fast-reload nxos bootflash:nxos.7.0.3.I2.1.bin
```

The following options are available:

- **save-config**—Ensures that subsequent fast reload operations use the new NXOS software image as the boot variable. If you do not use the **save-config** option, this command does not save the boot variable, and subsequent fast reload operations use the old software image as the boot variable.
- **trigger-gr**—By default, the fast reload feature requires Border Gateway Protocol (BGP) peers to be graceful restart capable. The **trigger-gr** option adds support for restarts with aggressive timers.
- **nxos bootflash:***nxos-image-name*—Specifies the name of the NXOS software image. Make sure to specify a software version that supports the fast reload feature.
- **non-interruptive**—Performs a fast reload without any prompts. Before you choose this option, verify that fast reload works on your system because this option skips all error and sanity checks.

Example

This example shows how to use fast reload to upgrade the Cisco NX-OS software on the switch:

```
switch# fast-reload nxos bootflash:nxos.7.0.3.I2.1.bin
uri is: /nxos.7.0.3.I2.1.bin
..
..
Notifying services about fast-reload.

fast-reload can proceed!!

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

Install is in progress, please wait.
.....
[33492.924958] [1426413334]  writing reset reason 133, (null)
[33493.242369] [1426413334] Starting new kernel
INIT: version 2Loading IGB driver ...
Installing SSE module ... done
Creating the sse device node ... done
Installing CCTRL driver for card_type 11 ...
Checking SSD firmware ...
 Model=Micron_M550_MTFDDAT064MAY, FwRev=MU01, SerialNo=MSA182202S9

Checking all filesystems.......
Installing SPROM driver ...
Installing default sprom values ...
 done.Configuring network ...
Installing veobc ...
Installing OBFL driver ...
blogger: nothing to do.
..done Sun Aug 23 09:55:51 UTC 2015
tune2fs 1.35 (28-Feb-2004)
Setting reserved blocks percentage to 0 (0 blocks)
Starting portmap daemon...
creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Saving image for img-sync ...
Uncompressing system image: package:/isanboot/bin/images/sys Sun Aug 23 09:55:54 UTC 2015
blogger: nothing to do.

..done Sun Aug 23 09:55:56 UTC 2015
```

```
Load plugins that defined in image conf: /isan/plugin_img/img.conf
Initialize Patching Repository during load
Loading plugin 0: core_plugin...
num srgs 1
0: swid-core-inseor, swid-core-inseor
num srgs 1
0: swid-inseor-ks, swid-inseor-ks
Creating /dev/mcelog
Starting mcelog daemon
INIT: Entering runlevel: 3

Populating conf files for hybrid sysmgr ...
Starting hybrid sysmgr ...
```

Saving the Configuration with Fast Reload

This table shows the expected behavior for saving the configuration with different variations of the **fast-reload** command:

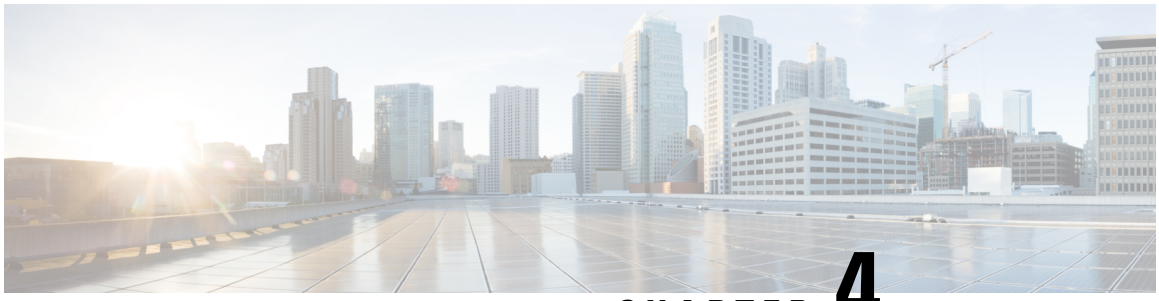
Command	Expected Behavior
fast-reload	Prompts you if there is a configuration change and performs a **copy running-config startup-config** based on your response.
fast-reload non-interruptive	No prompts appear, and the configuration is not saved. You need to save the configuration using the **save-config** option or the **copy running-config startup-config** command.
fast-reload nxos bootflash:*nxos-image-name* [**non-interruptive** | **trigger-gr**]	Implicitly performs a **copy running-config startup-config**, even if the image is the same image.
copy *configuration-file* **startup-config** **fast-reload**	After bootup, implicitly performs a **copy** *configuration-file* **startup-config** and sets the boot variable to the booted image.
copy *configuration-file* **startup-config** **fast-reload nxos bootflash:***nxos-image-name*	After bootup, implicitly sets the boot variable to the specified image and performs a **copy** *configuration-file* **startup-config**.

Note Ensure that the username is specified in the configuration file before you perform a **copy** *configuration-file* **startup-config** followed by the **fast-reload** or **reload** command. Otherwise, you will not be able to the access the switch and will need to complete the password recovery procedure to get the system back online. For information on the password recovery procedure, see the "Power Cycling the Device to Recover the Administrator Password" section in the Cisco Nexus 9000 Series NX-OS Troubleshooting Guide.

Additional References

Related Documents

Related Topic	Document Title
reload command	Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide



CHAPTER 4

Converting from Cisco NX-OS to ACI Boot Mode and from ACI Boot Mode Back to Cisco NX-OS

This chapter describes how to convert a Cisco Nexus 9000 Series switch from Cisco NX-OS to Cisco Application Centric Infrastructure (ACI) boot mode. It contains the following sections:

Converting to ACI Boot Mode

You can convert any Cisco Nexus 9000 Series switch from Cisco NX-OS to ACI boot mode.

Note You cannot convert a Cisco Nexus 3164Q or 31128PQ switch to ACI boot mode.

Note Use this procedure to convert a Cisco Nexus 9000 Series switch running Cisco NX-OS Release 7.0(3)I1(2) or later to ACI boot mode.

Before you begin

Verify whether your switch hardware is supported in ACI boot mode by checking the "Supported Hardware" section of the Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches. For example, line cards are not compatible between Cisco NX-OS and ACI boot mode.

Remove or turn off any unsupported modules (using the **poweroff module** *module* command). Otherwise, the software uses a recovery/retry mechanism before powering down the unsupported modules, which can cause delays in the conversion process.

For dual-supervisor systems, use the **show module** command to make sure that the standby supervisor module is in the ha-standby state.

Verify that the Application Policy Infrastructure Controller (APIC) is running Release 1.0(2j) or a later release.

Make sure that the ACI image is 11.0(2*x*) or a later release.

Use the **show install all impact epld** *epld-image-name* command to verify that the switch does not require any EPLD image upgrades. If any upgrades are required, follow the instructions in the Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes.

Step 1 Verify that the switch is running Cisco NX-OS Release 7.0(3)I1(2) or a later release.

Example:

```
switch(config)# show version
Software
BIOS: version 07.34
NXOS: version 7.0(3)I2(1)
BIOS compile time: 08/11/2015
NXOS image file name is: bootflash:///nxos.7.0.3.I1.2.bin
NXOS compile time: 08/13/2015 10:50:20 [08/13/2015 2:25]
```

Cisco NX-OS filenames begin with "nxos" [beginning with Cisco NX-OS Release 7.0(3)I2(1)] or "n9000" while ACI filenames begin with "aci-n9000."

Step 2 Follow these steps to copy the ACI image from the APIC:

a) Set the IP address on the mgmt0 interface of the switch to allow connectivity between this interface and the APIC.

b) Enable SCP services on the switch.

Example:

```
switch(config)# feature scp-server
```

c) From the APIC CLI, use SCP to copy the firmware image from the APIC to the active supervisor module on the switch.

Example:

```
admin@apic1:aci> scp -r /firmware/fwrepos/fwrepo/switch-image-name
admin@switch-ip-address:switch-image-name
```

d) For dual-supervisor systems, copy the ACI image to the standby supervisor module.

Example:

```
switch(config)# copy bootflash:aci-image bootflash://sup-standby/
```

Step 3 Follow these steps to boot to the ACI image:

a) Configure the switch to not boot from Cisco NX-OS.

Example:

```
switch(config)# no boot nxos
```

b) Save the configuration.

Example:

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

Note You must run the **copy running-config startup-config** command prior to booting the ACI image. Do not run it after you enter the **boot aci** command.

c) Boot the active and standby supervisor modules with the ACI image.

Example:

```
switch(config)# boot aci bootflash:aci-image-name
```

Caution Do not enter the **copy running-config startup-config** command after the **boot aci** command. If you do, the switch will go to the loader> prompt.

d) Verify the integrity of the file by displaying the MD5 checksum.

Example:

```
switch(config)# show file bootflash:aci-image-name md5sum
```

e) Reload the switch.

Example:

```
switch(config)# reload
```

f) Log in to the switch as an administrator.

Example:

```
Login: admin
```

Step 4 Verify whether you must install certificates for your device.

Example:

```
admin@apic1:aci> openssl asn1parse -in /securedata/ssl/server.crt
```

Look for PRINTABLESTRING in the command output. If "Cisco Manufacturing CA" is listed, the correct certificates are installed. If something else is listed, contact TAC to generate and install the correct certificates for your device.

Note You might need to install certificates for Cisco Nexus 9000 Series switches that were shipped prior to May 2014.

To run this command, contact TAC.

What to do next

See the ACI and APIC documentation to configure and operate your switch in ACI mode: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

Converting a Replacement Standby Supervisor to ACI Boot Mode

If you ever need to replace the standby supervisor module in a dual-supervisor system, you will need to copy and boot the ACI image for use with the replacement standby supervisor.

Before you begin

Copy the ACI image to a USB drive.

Step 1 Reload the switch.

Example:

```
switch# reload
```

Step 2 Enter a break sequence (Ctrl-C or Ctrl-]) during the initial boot sequence to access the loader> prompt.

Example:

```
Ctrl-C
loader>
```

Step 3 Plug the USB drive containing the ACI image into the standby supervisor USB slot.

Step 4 Boot the ACI image.

Example:

```
loader> boot usb#:aci-image-name
```

Note If you have two USB drives, enter the **dir** command to see which drive contains the ACI image. Then specify either **usb1** or **usb2** in the **boot** command.

Step 5 Log in to the switch as an administrator.

```
Login: admin
```

Step 6 Copy the ACI image from the USB drive to the switch.

Example:

```
switch# copy usb#:aci-image-name bootflash:aci-image-name
```

Converting Back to Cisco NX-OS

You can convert a Cisco Nexus 9000 Series switch from ACI boot mode back to Cisco NX-OS.

Step 1 Reload the switch.

Example:

```
switch# reload
```

Step 2 Enter a break sequence (Ctrl-C or Ctrl-]) during the initial boot sequence to access the loader> prompt.

Example:

```
Ctrl-C
loader>
```

Step 3 Configure the boot process to stop at the switch(boot)# prompt.

Example:

```
loader> cmdline recoverymode=1
```

Step 4 Boot the active supervisor module with the Cisco NX-OS image.

Example:

```
loader> boot nxos.7.0.3.I7.6.bin
```

Note If the Cisco NX-OS image mentioned in the bootvariable is not present in the bootflash, the system falls back to the loader prompt during the boot sequence. To recover the switch from the loader prompt, boot the system through a different image present in the bootflash, perform a **tftpboot**, or boot through a USB device.

Note For some Cisco NX-OS releases and Cisco Nexus 9000 Series switches, the following error message appears:

```
!!Fatal error!!
Can't reserve space for RPM repo
Please free up bootflash space and reboot
```

If you see this error message, start over from Step 1. After Step 3, enter the **cmdline init_system** command and then go to Step 4. The switch boots into the normal Cisco NX-OS prompt and skips the switch(boot)# prompt.

Step 5 Restores the switch's file system partitioning to the default settings. The bootflash filesystem is reset to Cisco NX-OS partitioning, and the Cisco NX-OS image is deleted.

Example:

```
switch(boot)# init system
```

Step 6 Completes the upload of the nx-os image file.

Example:

```
switch(boot)# load-nxos
```

Note For some Cisco Nexus 9000 Series switches, the device does not load with the normal Cisco NX-OS prompt (switch#) and instead comes up as "bash-4.2#". In this case, you must power cycle the device, jump to loader, and boot the NX-OS image using either TFTP or an USB method.

- For TFTP method - First assign a IP address and gateway to the device using the **set ip** *ip address subnet mask* and the **set gw** *gateway address* commands. This is required as the **init system** command in the above step erases all available configurations on the device

  Example

  ```
  loader> set ip 1.1.1.2 255.255.255.0
  loader>set gw 1.1.1.1
  ```

  Then use the **tftp** command to load the image.

  ```
  loader> boot tftp://<tftp server ip>/<nxos-image-name>
  ```

- For USB method - Mount the USB on the switch and execute the **dir** coammnd on the loader to see the contents of the bootflash folder and the USB device.

  Example

  ```
  loader > dir
  usb1::
  lost+found
  /nxos.7.0.3.I7.5.bin
  ```

  Then boot the NX-OS image using the following command:.

  ```
  loader> boot usb1:/nxos-image
  Example: boot usb1:/nxos.7.0.3.I7.5.bin
  ```

Once you boot the NX-OS image, the device will load as an NX-OS switch and you can continue with the remaining steps.

Step 7 Re-copy the Cisco NX-OS image into bootflash: and set the appropriate boot variables to ensure that the system boots the Cisco NX-OS image on the next reload.

Example:

TFTP example:

```
switch# copy tftp://tftp-server-ip/nxos-image-name bootflash:
switch# configure terminal
switch(config)# boot nxos bootflash:nxos-image-name
switch(config)# copy running-config startup-config
switch(config)# end
```

USB example:

```
switch# copy usb1:nxos-image-name bootflash:
switch# configure terminal
switch(config)# boot nxos bootflash:nxos-image-name
switch(config)# copy running-config startup-config
switch(config)# end
```

Step 8 Wait for the system controllers to come up, which could take approximately 15 to 20 minutes.

File system differences between ACI and Cisco NX-OS require a one-time reformatting change during the ACI to Cisco NX-OS conversion. Subsequent reloads with the Cisco NX-OS image will be faster.

Step 9 Verify that the active supervisor module and the system controllers are in the active state.

Example:

```
switch# show module
Mod  Ports  Module-Type                          Model              Status
---  -----  ------------------------------------ ------------------ ----------
27   0      Supervisor Module                    N9K-SUP-A          active
28   0      Supervisor Module                    N9K-SUP-A          ha-standby
29   0      System Controller                    N9K-SC-A           active
30   0      System Controller                    N9K-SC-A           active
```

Step 10 For dual-supervisor systems, follow Steps 3 through 6 on the standby supervisor.

Step 11 Log in to the switch and verify that it is running Cisco NX-OS software.

```
Software
BIOS: version 07.34
NXOS: version 7.0(3)I2(1)
BIOS compile time: 08/11/2015
NXOS image file name is: bootflash:///nxos.7.0.3.I1.2.bin
NXOS compile time: 08/13/2015 10:50:20 [08/13/2015 2:25]
```

Using SCP on the ACI Shell to Load NX-OS Image into Bootflash

Use this task if you have a switch in ACI mode and must convert it to NX-OS mode, but are unable to perform a TFTP boot and the USB option is not available. The following steps describe how to boot the switch on ACI mode, configure the management port, and copy the software image to the bootflash partition.

The leaf switch boots into ACI mode in fabric discovery state.

Step 1 Log in with the username "admin" and no password. The command prompt appears:

```
#
```

Step 2 **configure terminal**

Example:

```
# configure terminal
(config)#
```

Step 3 **interface mgmt 0**

Example:

```
(config)# interface mgmt 0
(config-if)#
```

Step 4 **ip address** *ipv4−address* { [*/length*] | [*subnet−mask*] }

Example:

```
(config-if)# ip address 10.1.1.20/24
(config-if)#
```

Step 5 **no shutdown**

Example:

```
(config-if)# no shutdown
(config-if)#
```

Step 6 **exit**

Example:

```
(config-if)# exit
(config)#
```

Step 7 **vrf context management**

Example:

```
(config)# vrf context management
(config-vrf)#
```

Step 8 **ip route** *ipv4−address* { [*/length*] | [*subnet−mask*] } *default-gw-ipv4−address* { [*/length*] | [*subnet−mask*] }

Example:

```
(config-vrf)# ip route 0.0.0.0/0 10.1.1.30/24
(config-vrf)#
```

Step 9 **end**

Example:

```
(config-vrf)# end
#
```

Step 10 **cd /bootflash**

Example:

```
# cd /bootflash
#
```

Step 11 **scp** *username* **@** *scp-server-ip-address* **:** *nxos-image*

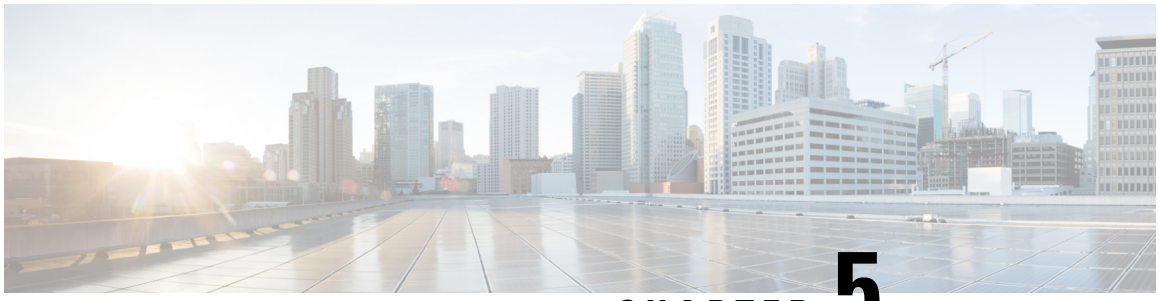
Example:

```
# scp user1@10.1.1.25:n9000-dk9.7.0.3.I1.1.bin
#
```

Step 12 Reload the switch, break into the loader prompt, and follow the steps to load the NX-OS image as shown in the previous Converting Back to Cisco NX-OS the procedure. The newly copied software image appears in the bootflash.

Example

```
# configure terminal
(config)# interface mgmt 0
(config-if)# ip address 10.1.1.20/24
(config-if)# no shutdown
(config-if)# exit
(config)# vrf context management
(config-vrf)# ip route 0.0.0.0/0 10.1.1.30/24
(config-vrf)#end
# cd /bootflash
# scp user1@10.1.1.25:n9000-dk9.7.0.3.I1.1.bin
```



CHAPTER 5

Migrating Switches in a vPC Topology

This chapter describes how to migrate from one pair of switches to another in a vPC topology. It contains the following sections:

vPC Forklift Upgrade

In a vPC topology, you can migrate from a pair of Cisco Nexus 9000 Series switches to a different pair of Cisco Nexus 9000 Series switches. For example, you might migrate from a pair of Cisco Nexus 9508 vPC peer nodes to a pair of Cisco Nexus 9516 switches. For more information, see the "vPC Forklift Upgrade Scenario" section in the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide .

INDEX