Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 6.x

First Published: 2014-03-15

Last Modified: 2020-12-11

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2014–2020 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface v

Audience v

Document Conventions v

Related Documentation for Cisco Nexus 9000 Series Switches vi

Documentation Feedback vi

Communications, Services, and Additional Information vi

Cisco Bug Search Tool vii

Documentation Feedback vii

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software 3

About the Software Image 3

Prerequisites for Upgrading the Cisco NX-OS Software 4

Prerequisites for Downgrading the Cisco NX-OS Software 4

Cisco NX-OS Software Upgrade Guidelines 5

Cisco NX-OS Software Downgrade Guidelines 5

Upgrading the Cisco NX-OS Software 6

Upgrade Process for vPCs 9

Upgrade Process for a vPC Topology on the Primary Switch 9

Upgrade Process for a vPC Topology on the Secondary Switch 10

Downgrading to an Earlier Software Release 10

CHAPTER 3

Upgrading the Cisco NX-OS Software Using Fast Reload 15

About Fast Reload 15

Fast Reload Sequence of Events 15
Prerequisites for Fast Reload 16
Guidelines and Limitations for Fast Reload 16
Performing a Fast Reload and Upgrading the Cisco NX-OS Software 17
Saving the Configuration with Fast Reload 19
Additional References 20
Related Documents 20

CHAPTER 4 **Converting from Cisco NX-OS to ACI Boot Mode and from ACI Boot Mode Back to Cisco NX-OS** 21
Converting to ACI Boot Mode 21
Converting a Replacement Standby Supervisor to ACI Boot Mode 24
Converting Back to Cisco NX-OS 25

CHAPTER 5 **Migrating Switches in a vPC Topology** 29
vPC Forklift Upgrade 29

Preface

This preface includes the following sections:

- Audience, on page v
- Document Conventions, on page v
- Related Documentation for Cisco Nexus 9000 Series Switches, on page vi
- Documentation Feedback, on page vi
- Communications, Services, and Additional Information, on page vi

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:

https://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

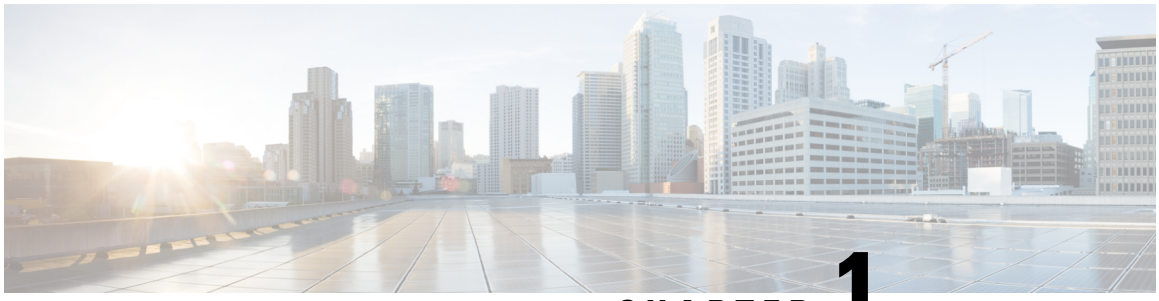
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



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 6.x*.

- New and Changed Information, on page 1

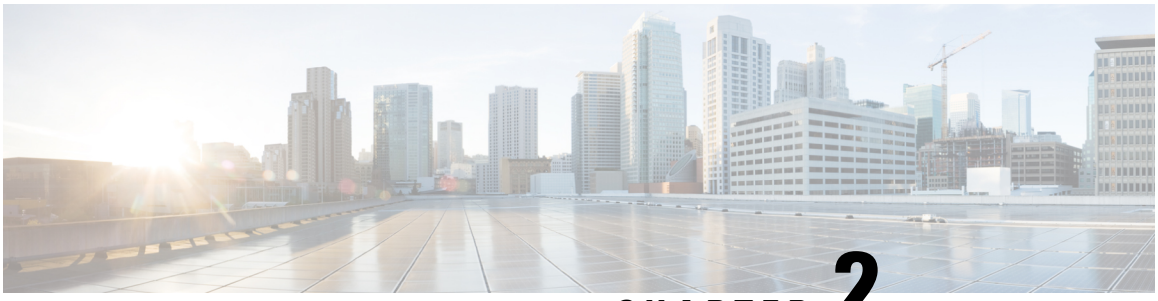
New and Changed Information

This table summarizes the new and changed features for the *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 6.x* and tells you where they are documented.

Table 1: New and Changed Features for Cisco NX-OS Release 6.x

Feature	Description	Changed in Release	Where Documented
Fast reload	Introduced this feature for the Cisco Nexus 3164Q switch.	6.1(2)I3(4)	Upgrading the Cisco NX-OS Software Using Fast Reload, on page 15
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.	6.1(2)I3(3)	Converting from Cisco NX-OS to ACI Boot Mode and from ACI Boot Mode Back to Cisco NX-OS, on page 21
Software upgrades and downgrades	Added the initial support to upgrade and downgrade Cisco NX-OS software on a Cisco Nexus 9000 series switch.	6.1(2)I2(1)	Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software, on page 3

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, on page 3
- Prerequisites for Upgrading the Cisco NX-OS Software, on page 4
- Prerequisites for Downgrading the Cisco NX-OS Software, on page 4
- Cisco NX-OS Software Upgrade Guidelines, on page 5
- Cisco NX-OS Software Downgrade Guidelines, on page 5
- Upgrading the Cisco NX-OS Software, on page 6
- Upgrade Process for vPCs, on page 9
- Downgrading to an Earlier Software Release, on page 10

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 (for example, n9000-dk9.6.1.2.I2.1.bin). Only this image is required to load the Cisco NX-OS operating system. This image runs on all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q switch starting with Cisco NX-OS Release 6.1(2)I2(2a).

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-dk9.6.1.2.I2.1.**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.

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 Nexus 9000 and 3000 Upgrade and ISSU 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 non-disruptive ISSU in spanning tree topology, before running the **show spanning-tree issu-impact** command, verify the following criteria:
  - No Topology change must be active in any STP instance
  - Bridge assurance(BA) should not be active on any port (except MCT and vPC peer link)
  - There should not be any Non-Edge Designated Forwarding port (except MCT and vPC peer link)
  - ISSU criteria must be met on the vPC peer switch

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
- 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 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).
- 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).
- 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.

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.
- 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.

Upgrading the Cisco NX-OS Software

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.

Procedure

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    May 10 14:43:39 2014 lost+found/
80850712 May 10 15:57:44 2014 n9000-dk9.6.1.2.I2.1.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-dk9.6.1.2.I2.1.bin
```

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

```
switch# dir bootflash://sup-standby/
49152    May 10 14:43:39 2014 lost+found/
80850712 May 10 15:57:44 2014 n9000-dk9.6.1.2.I2.1.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-dk9.6.1.2.I2.1.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/n9000-dk9.6.1.2.I2.2.bin
bootflash:n9000-dk9.6.1.2.I2.2.bin
```

Step 9 Check the impact of upgrading the software before actually performing the upgrade.

```
switch# show install all impact nxos bootflash:n9000-dk9.6.1.2.I2.2.bin
Installer will perform compatibility check first. Please wait.
uri is: /n9000-dk9.6.1.2.I2.2.bin
Installer is forced disruptive

Verifying image bootflash:/n9000-dk9.6.1.2.I2.2.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.2.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
------  --------  --------------  ------------  ------
     2       yes      disruptive         reset  Reset due to single supervisor
     4       yes      disruptive         reset  Reset due to single supervisor
     6       yes      disruptive         reset  Reset due to single supervisor
    22       yes      disruptive         reset  Reset due to single supervisor
    24       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
    28       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
------  -------  -------------------------  --------------------  ------------
     2    lcn9k                6.1(2)I2(1)           6.1(2)I2(2)           yes
     2     bios                  v01.35(00   v01.35(00:v01.27(00           no
     4    lcn9k                6.1(2)I2(1)           6.1(2)I2(2)           yes
     4     bios                  v01.35(00   v01.35(00:v01.23(00           no
     6    lcn9k                6.1(2)I2(1)           6.1(2)I2(2)           yes
     6     bios                  v01.35(00   v01.35(00:v01.24(00           no
    22    lcn9k                6.1(2)I2(1)           6.1(2)I2(2)           yes
    22     bios                  v01.35(00   v01.35(00:v01.24(00           no
    24    lcn9k                6.1(2)I2(1)           6.1(2)I2(2)           yes
    24     bios                  v01.35(00   v01.35(00:v01.24(00           no
    26    lcn9k                6.1(2)I2(1)           6.1(2)I2(2)           yes
    26     bios                  v01.35(00   v01.35(00:v01.24(00           no
    27     nxos                6.1(2)I2(1)           6.1(2)I2(2)           no
    27     bios                  v01.35(00   v01.35(00:v01.24(00           no
    28     nxos                6.1(2)I2(1)           6.1(2)I2(2)           no
    28     bios                  v01.35(00   v01.35(00:v01.24(00           no
    29    lcn9k                6.1(2)I2(1)           6.1(2)I2(2)           yes
    29     bios                  v01.35(00   v01.35(00:v01.24(00           no
    30    lcn9k                6.1(2)I2(1)           6.1(2)I2(2)           yes
    30     bios                  v01.35(00   v01.35(00:v01.24(00           no
```

Step 10 Save the running configuration to the startup configuration.

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

Step 11 Upgrade the Cisco NX-OS software.

```
switch# install all nxos bootflash:n9000-dk9.6.1.2.I2.2.bin
```

You can save time by upgrading up to three line cards concurrently. To do so, add the **parallel** option to the **install all** command (for example, **install all parallel nxos bootflash:n9000-dk9.6.1.2.I2.2.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 upgrade process.

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

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

```
switch# show version
```

Step 14 (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.

In a dual-homed non-vPC access network (either a triangle or Y shaped access network), with or without STP configured, with BFD enabled and with HSRP configured on the SVIs and with HSRP configured as BFD client, transient traffic may drop for both IPv4 native unicast and/or labeled traffic after performing an ND-ISSU n fallback mode.

To counter this, configure in all the HSRP IPv4 groups for all the HSRP enabled SVIs the **timer 2 120** on both HSRP peers prior to performing the ND-ISSU. The configuration of the **timer 3 120** may lead to traffic loss.

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

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.

Procedure

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 May 10 14:43:39 2014 lost+found/
80850712 May 10 15:57:44 2014 n9000-dk9.6.1.2.I2.2.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-dk9.6.1.2.I2.1.bin
bootflash:n9000-dk9.6.1.2.I2.1.bin
```

Step 6 Check for any software incompatibilities.

```
switch# show incompatibility-all nxos bootflash:n9000-dk9.6.1.2.I2.1.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-dk9.6.1.2.I2.1.bin
Installer will perform compatibility check first. Please wait.
uri is: /n9000-dk9.6.1.2.I2.1.bin
Installer is forced disruptive

Verifying image bootflash:/n9000-dk9.6.1.2.I2.1.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS
```

```
Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.I2.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/n9000-dk9.6.1.2.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
------  --------  --------------  ------------  ------
     2       yes      disruptive         reset  Reset due to single supervisor
     4       yes      disruptive         reset  Reset due to single supervisor
     6       yes      disruptive         reset  Reset due to single supervisor
    22       yes      disruptive         reset  Reset due to single supervisor
    24       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
    28       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
------  ------  ----------------------------------  ------------------  ------------
     2   lcn9k                          6.1(2)I2(2)         6.1(2)I2(1)           yes
     2    bios                v01.35(00:v01.27(00           v01.35(00           no
     4   lcn9k                          6.1(2)I2(2)         6.1(2)I2(1)           yes
     4    bios                v01.35(00:v01.23(00           v01.35(00           no
     6   lcn9k                          6.1(2)I2(2)         6.1(2)I2(1)           yes
     6    bios                v01.35(00:v01.24(00           v01.35(00           no
    22   lcn9k                          6.1(2)I2(2)         6.1(2)I2(1)           yes
    22    bios                v01.35(00:v01.24(00           v01.35(00           no
    24   lcn9k                          6.1(2)I2(2)         6.1(2)I2(1)           yes
    24    bios                v01.35(00:v01.24(00           v01.35(00           no
    26   lcn9k                          6.1(2)I2(2)         6.1(2)I2(1)           yes
    26    bios                v01.35(00:v01.24(00           v01.35(00           no
    27    nxos                          6.1(2)I2(2)         6.1(2)I2(1)           no
    27    bios v06.26(05/10/2014):v06.21(11/17/2013)  v06.26(05/10/2014)           no
    28    nxos                          6.1(2)I2(2)         6.1(2)I2(1)           no
    28    bios v06.26(05/10/2014):v06.21(11/17/2013)  v06.26(05/10/2014)           no
    29   lcn9k                          6.1(2)I2(2)         6.1(2)I2(1)           yes
    29    bios                v01.35(00:v01.24(00           v01.35(00           no
    30   lcn9k                          6.1(2)I2(2)         6.1(2)I2(1)           yes
    30    bios                v01.35(00:v01.24(00           v01.35(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-dk9.6.1.2.I2.1.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.

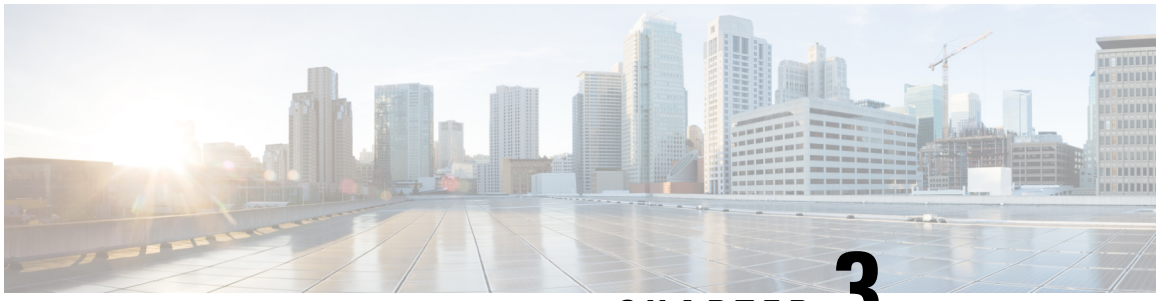
Step 12 (Optional) Display the entire downgrade process.

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
```



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, on page 15
- Prerequisites for Fast Reload, on page 16
- Guidelines and Limitations for Fast Reload, on page 16
- Performing a Fast Reload and Upgrading the Cisco NX-OS Software, on page 17
- Saving the Configuration with Fast Reload, on page 19
- Additional References, on page 20

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 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.

Procedure

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:n9000-dk9.6.1.2.I3.4.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:n9000-dk9.6.1.2.I3.4.bin
uri is: /n9000-dk9.6.1.2.I3.4.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 Mar 15 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 Mar 15 09:55:54 UTC 2015
blogger: nothing to do.

..done Sun Mar 15 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:

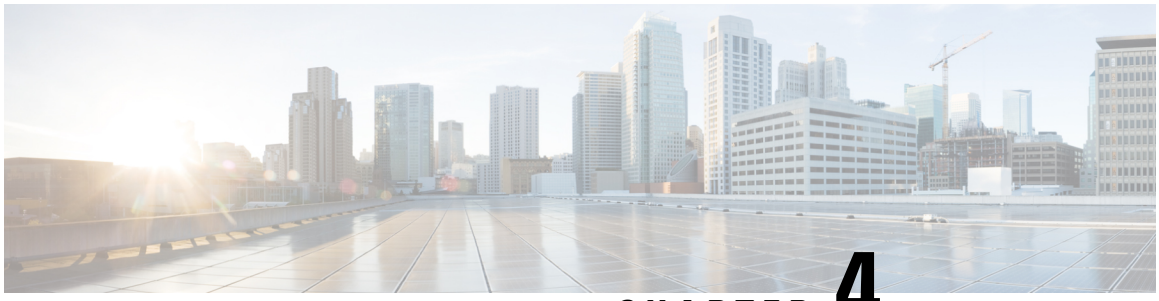
Command	Expected Behavior
fast-reload	Prompts you if there is a configuration change and performs a **copy running-config startup-config** based on your response.
fast-reload non-interruptive	No prompts appear, and the configuration is not saved. You need to save the configuration using the **save-config** 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, on page 21
- Converting a Replacement Standby Supervisor to ACI Boot Mode, on page 24
- Converting Back to Cisco NX-OS, on page 25

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 switch to ACI boot mode.

Note Use this procedure to convert a Cisco Nexus 9000 Series switch running Cisco NX-OS Release 6.1(2)I3(3) 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.

Procedure

Step 1 Verify that the switch is running Cisco NX-OS Release 6.1(2)I3(3) or a later release.

Example:

```
switch(config)# show version
Software
BIOS: version 08.06
NXOS: version 6.1(2)I3(3)
BIOS compile time: 12/03/2014
NXOS image file name is: bootflash:///n9000-dk9.6.1.2.I3.3.bin
NXOS compile time: 12/05/2014 10:50:20 [12/05/2014 2:25]
```

Cisco NX-OS filenames begin with "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
```

Note
Check the output of the **show boot** command to see if the bootvar is correctly set.

e) Reload the switch.

Example:

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

Note
If the switch goes into a bootloader prompt after following step 3e, manually execute the following commands in ACI mode, for example:

```
switch# dir /bootflash/aci-n9000*
switch# cat /mnt/cfg/0/boot/grub/menu.lst.local
switch# cat /mnt/cfg/1/boot/grub/menu.lst.local
switch# cd bootflash
switch# setup-bootvars.sh aci-n9000-VERSION.bin
```

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.

Procedure

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.

Procedure

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 n9000-dk9.6.1.2.I3.2.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
  /n9000-dk9.6.1.2.I3.3.bin
  ```

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

  ```
  loader> boot usb1:/nxos-image
  Example: boot usb1:/n9000-dk9.6.1.2.I3.3.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.

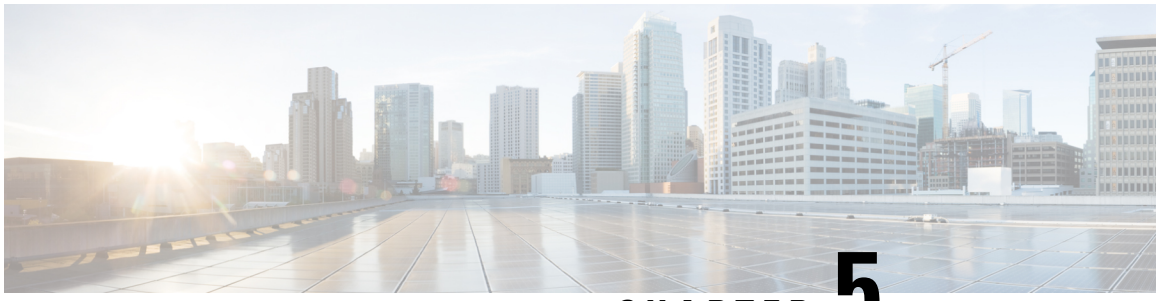
Example:

```
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 08.06
NXOS: version 6.1(2)I3(3)
BIOS compile time: 12/03/2014
NXOS image file name is: bootflash:///n9000-dk9.6.1.2.I3.3.bin
NXOS compile time: 12/05/2014 10:50:20 [12/05/2014 2:25]
```



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, on page 29

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.