Cisco Nexus 5500 Series NX-OS Fundamentals Configuration Guide, Release 7.x

First Published: January 29, 2013

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

Text Part Number: OL-30890-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xi

Audience xi

Document Conventions xi

Related Documentation for Cisco Nexus 5500 Series NX-OS Software xiii

Documentation Feedback xiv

Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1

New and Changed Information for this Release 1

New and Changed Information for this Release 1

CHAPTER 2

Overview 3

Fibre Channel over Ethernet 3

Data Center I/O Consolidation 4

Virtual Interfaces 5

Ethernet Switching 5

FCoE and Fibre Channel Switching 5

QoS 6

Virtual Port Channels 6

Serviceability 6

Switched Port Analyzer 6

Ethanalyzer 6

Call Home 7

Online Diagnostics 7

Switch Management 7

Simple Network Management Protocol 7

Role-Based Access Control 7

Configuration Methods 7

Configuring with CLI, XML Management Interface, or SNMP 7
Configuring with Cisco Data Center Network Manager 8
Configuring with Cisco MDS Fabric Manager 8
Network Security Features 8
Virtual Device Contexts 8
Licensing 8
Typical Deployment Topologies 8
Ethernet TOR Switch Topology 8
Fabric Extender Deployment Topology 10
Data Center I/O Consolidation Topology 11
Supported Standards 11

CHAPTER 3 Using the Cisco NX-OS Setup Utility 13
Configuring the Switch 13
Image Files on the Switch 13
Starting the Switch 13
Boot Sequence 14
Console Settings 15
Upgrading the Switch Software 15
Downgrading from a Higher Release 19
Initial Configuration 20
Configuration Prerequisites 20
Initial Setup 21
Preparing to Configure the Switch 21
Default Login 22
Configuring the Switch 22
Changing the Initial Configuration 26
Management Interface Configuration 27
About the mgmt0 Interface 27
Configuring the Management Interface 27
Displaying Management Interface Configuration 28
Shutting Down the Management Interface 29

CHAPTER 4 Using PowerOn Auto Provisioning 31
Information About PowerOn Auto Provisioning 31

Network Requirements for POAP 32
POAP Configuration Script 32
POAP Process 33
Power-Up Phase 35
USB Discovery Phase 35
DHCP Discovery Phase 35
Script Execution Phase 37
Post-Installation Reload Phase 38
Configuration_File_Selection_Methods 38
Serial Number-Based Configuration File Selection 38
Hostname-Based Configuration File Selection 38
MAC-Based Configuration File Selection 38
Location-Based Configuration File Selection 39
Configuration Script Syslog Logging 39
Guidelines and Limitations for POAP 39
Setting Up the Network Environment To Use POAP 40
Configuring a Switch Using POAP 40
Verifying the Device Configuration 41

CHAPTER 5 **Understanding the Command-Line Interface 43**
Finding Feature Information 44
Information About the CLI Prompt 44
Command Modes 44
EXEC Command Mode 45
Global Configuration Command Mode 45
Interface Configuration Command Mode 45
Subinterface Configuration Command Mode 46
Saving and Restoring a Command Mode 47
Exiting a Configuration Command Mode 47
Command Mode Summary 48
Special Characters 49
Keystroke Shortcuts 49
Abbreviating Commands 52
Completing a Partial Command Name 52
Identifying Your Location in the Command Hierarchy 53

Using the no Form of a Command 53
Configuring CLI Variables 54
About CLI Variables 54
Configuring CLI Session-Only Variables 55
Configuring Persistent CLI Variables 55
Command Aliases 56
About Command Aliases 56
Defining Command Aliases 57
Configuring Command Aliases for a User Session 58
Command Scripts 58
Running a Command Script 58
Echoing Information to the Terminal 59
Delaying Command Action 60
Context-Sensitive Help 60
Understanding Regular Expressions 62
Special Characters 62
Multiple-Character Patterns 62
Anchoring 63
Searching and Filtering show Command Output 63
Filtering and Searching Keywords 64
diff Utility 65
grep and egrep Utilities 66
less Utility 67
sed Utility 67
sort Utility 67
Searching and Filtering from the --More-- Prompt 68
Using the Command History 69
Recalling a Command 69
Controlling CLI History Recall 70
Configuring the CLI Edit Mode 70
Displaying the Command History 70
Enabling or Disabling the CLI Confirmation Prompts 71
Setting CLI Display Colors 71
Sending Commands to Modules 72
BIOS Loader Prompt 73

Examples Using the CLI 73
Defining Command Aliases 73
Using CLI Session Variables 73
Using the System-Defined Timestamp Variable 74
Running a Command Script 74
Additional References for the CLI 75
Related Documents for the CLI 75

CHAPTER 6 Configuring Terminal Settings and Sessions 77
Information About Terminal Settings and Sessions 77
Terminal Session Settings 77
Console Port 78
COM1 Port 78
Virtual Terminals 79
Licensing Requirements for Terminal Settings and Sessions 79
Configuring the Console Port 79
Configuring the COM1 Port 81
Configuring Virtual Terminals 83
Configuring the Inactive Session Timeout 83
Configuring the Session Limit 84
Configuring Modem Connections 85
Enabling a Modem Connection 85
Downloading the Default Initialization String 87
Configuring and Downloading a User-Specified Initialization String 88
Initializing a Modem for a Powered-Up Cisco NX-OS Device 89
Clearing Terminal Sessions 90
Displaying Terminal and Session Information 90
Default Settings for File System Parameters 91
Additional References for Terminal Settings and Sessions 91
Related Documents for Terminal Settings and Sessions 91

CHAPTER 7 Basic Device Management 93
Finding Feature Information 93
Information About Basic Device Management 94
Device Hostname 94

Message-of-the-Day Banner 94
EXEC Banner 94
Device Clock 94
Clock Manager 94
Time Zone and Summer Time (Daylight Saving Time) 94
User Sessions 95
Licensing Requirements for Basic Device Management 95
Changing the Device Hostname 95
Configuring the MOTD Banner 96
Configuring the EXEC Banner 97
Configuring the Time Zone 98
Configuring Summer Time (Daylight Saving Time) 99
Manually Setting the Device Clock 101
Setting the Clock Manager 101
Managing Users 102
Displaying Information about the User Sessions 102
Sending a Message to Users 103
Verifying the Device Configuration 103
Default Settings for Basic Device Parameters 104
Additional References for Basic Device Management 104
Related Documents for Basic Device Management 104

CHAPTER 8 **Using the Device File Systems, Directories, and Files 105**
Information about the External Storage Devices, Device File Systems, Directories, and Files 105
File Systems 105
Directories 106
Files 106
Licensing Requirements for File Systems, Directories, and Files 107
Working with Directories 107
Identifying the Current Directory 107
Changing the Current Directory 107
Creating a Directory 108
Displaying Directory Contents 109
Deleting a Directory 109

Accessing Directories on the Standby Supervisor Module 110
Working with Files 110
Moving Files 110
Copying Files 111
Deleting Files 112
Displaying File Contents 112
Displaying File Checksums 113
Compressing and Uncompressing Files 113
Displaying the Last Lines in a File 114
Redirecting show Command Output to a File 114
Finding Files 115
Working with Archive Files 115
Creating an Archive Files 116
Appending Files to an Archive File 117
Extracting Files from an Archive File 117
Displaying the Filenames in an Archive File 118
Examples of Using the File System 118
Accessing Directories on Standby Supervisor Modules 118
Moving Files 119
Copying Files 119
Deleting a Directory 119
Displaying File Contents 120
Displaying File Checksums 120
Compressing and Uncompressing Files 121
Redirecting show Command Output 121
Finding Files 121
Default Settings for File System Parameters 122
Additional References for File Systems 122
Related Documents for File Systems 122

CHAPTER 9 **Working with Configuration Files 123**

Information About Configuration Files 123
Types of Configuration Files 123
Licensing Requirements for Configuration Files 124
Managing Configuration Files 124

Saving the Running Configuration to the Startup Configuration 124
Copying a Configuration File to a Remote Server 125
Downloading the Running Configuration From a Remote Server 126
Downloading the Startup Configuration From a Remote Server 127
Copying Configuration Files to an External Flash Memory Device 128
Copying the Running Configuration from an External Flash Memory Device 129
Copying the Startup Configuration from an External Flash Memory Device 130
Copying Configuration Files to an Internal File System 131
Rolling Back to a Previous Configuration 132
Removing the Configuration for a Missing Module 133
Erasing a Configuration 134
Clearing Inactive Configurations 135
Verifying the Device Configuration 136
Examples of Working with Configuration Files 136
Copying Configuration Files 136
Backing Up Configuration Files 136
Rolling Back to a Previous Configuration 137
Additional References for Configuration Files 137
Related Documents for Configuration Files 137

Preface

The Preface contains the following sections:

- Audience, page xi
- Document Conventions, page xi
- Related Documentation for Cisco Nexus 5500 Series NX-OS Software, page xiii
- Documentation Feedback, page xiv
- Obtaining Documentation and Submitting a Service Request, page xv

Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices and Cisco Nexus 2000 Series Fabric Extenders.

Document Conventions

Note As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.

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 the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).

Convention	Description
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments 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.
`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 will include 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 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.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation for Cisco Nexus 5500 Series NX-OS Software

The entire Cisco NX-OS 5500 Series documentation set is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/tsd-products-support-series-home.html

Release Notes

The release notes are available at the following URL:

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

Configuration Guides

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

The documents in this category include:

- *Cisco Nexus 5500 Series NX-OS Adapter-FEX Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS FabricPath Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS FCoE Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS Fundamentals Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS Interfaces Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS Layer 2 Switching Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS Multicast Routing Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS Quality of Service Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS SAN Switching Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS Security Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS System Management Configuration Guide*
- *Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide*

Installation and Upgrade Guides

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9670/prod_installation_guides_list.html

The document in this category include:

- *Cisco Nexus 5500 Series NX-OS Software Upgrade and Downgrade Guides*

Licensing Guide

The *License and Copyright Information for Cisco NX-OS Software* is available at http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html.

Command References

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

The documents in this category include:

- *Cisco Nexus 5500 Series NX-OS Fabric Extender Command Reference*
- *Cisco Nexus 5500 Series NX-OS FabricPath Command Reference*
- *Cisco Nexus 5500 Series NX-OS Fundamentals Command Reference*
- *Cisco Nexus 5500 Series NX-OS Interfaces Command Reference*
- *Cisco Nexus 5500 Series NX-OS Layer 2 Interfaces Command Reference*
- *Cisco Nexus 5500 Series NX-OS Multicast Routing Command Reference*
- *Cisco Nexus 5500 Series NX-OS Quality of Service Command Reference*
- *Cisco Nexus 5500 Series NX-OS Security Command Reference*
- *Cisco Nexus 5500 Series NX-OS System Management Command Reference*
- *Cisco Nexus 5500 Series NX-OS TrustSec Command Reference*
- *Cisco Nexus 5500 Series NX-OS Unicast Routing Command Reference*
- *Cisco Nexus 5500 Series NX-OS Virtual Port Channel Command Reference*

Technical References

The *Cisco Nexus 5500 Series NX-OS MIB Reference* is available at http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/mib/reference/NX5500_MIBRef.html.

Error and System Messages

The *Cisco Nexus 5500 Series NX-OS System Message Guide* is available at http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/system_messages/reference/sl_nxos_book.html.

Troubleshooting Guide

The *Cisco Nexus 5500 Series NX-OS Troubleshooting Guide* is available at http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html.

Documentation Feedback

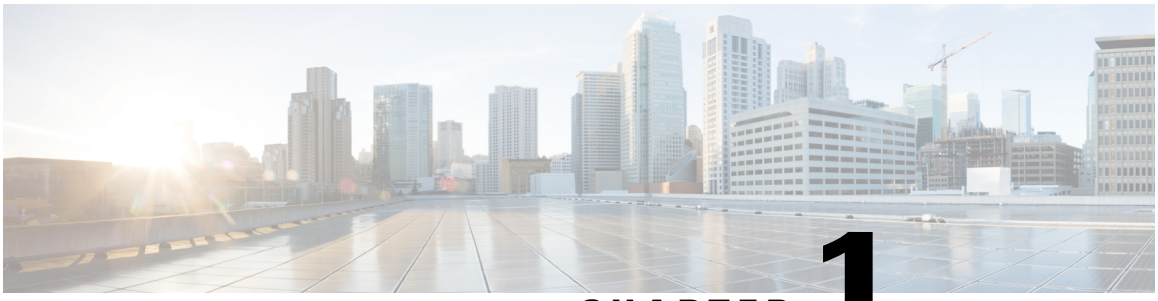
To provide technical feedback on this document, or to report an error or omission, please send your comments to: ciscodfa-docfeedback@cisco.com.

We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

New and Changed Information for this Release

There are no new or changed features in this release.

- New and Changed Information for this Release, page 1

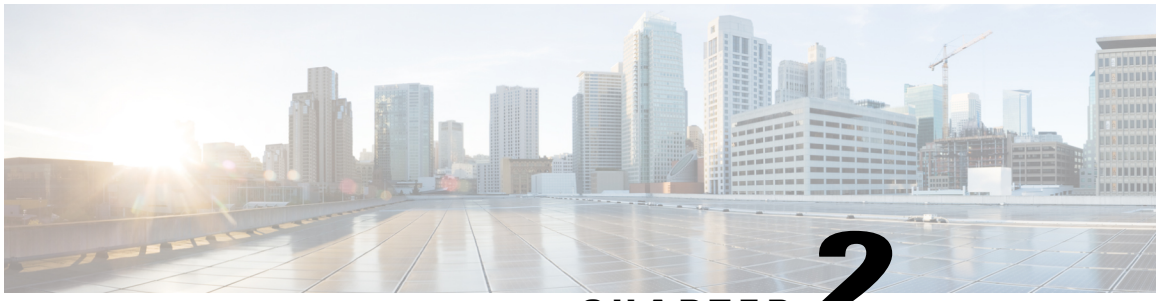
New and Changed Information for this Release

The following table provides an overview of the significant changes made to this configuration guide. The table does not provide an exhaustive list of all changes made to this guide or all new features in a particular release.

Table 1: New and Changed Information

Feature	Description	Release	Where Documented
EXEC banner	Added the support for the EXEC banner feature.	7.3(0)N1(1)	Basic Device Management
63 character hostname and switchname	Added support for 63 characters for hostname and switchname.	7.3(0)N1(1)	Basic Device Management

New and Changed Information for this Release



CHAPTER 2

Overview

This chapter contains the following sections:

- Fibre Channel over Ethernet, page 3
- Data Center I/O Consolidation, page 4
- Virtual Interfaces, page 5
- Ethernet Switching, page 5
- FCoE and Fibre Channel Switching, page 5
- QoS , page 6
- Virtual Port Channels, page 6
- Serviceability, page 6
- Switch Management, page 7
- Network Security Features, page 8
- Virtual Device Contexts , page 8
- Licensing, page 8
- Typical Deployment Topologies, page 8
- Supported Standards, page 11

Fibre Channel over Ethernet

Fibre Channel over Ethernet (FCoE) allows Fibre Channel traffic to be encapsulated over a physical Ethernet link. FCoE frames use a unique EtherType so that FCoE traffic and standard Ethernet traffic can be carried on the same link.

Classic Ethernet is a best-effort protocol; in the event of congestion, Ethernet will discard packets, relying on higher level protocols to provide retransmission and other reliability mechanisms. Fibre Channel traffic requires a lossless transport layer; as a data storage protocol, it is unacceptable to lose a single data packet. Native Fibre Channel implements a lossless service at the transport layer using a buffer-to-buffer credit system.

For FCoE traffic, the Ethernet link must provide a lossless service. Ethernet links on Cisco Nexus devices provide two mechanisms to ensure lossless transport for FCoE traffic: link-level flow control and priority flow control.

IEEE 802.3x link-level flow control allows a congested receiver to signal the far end to pause the data transmission for a short period of time. The pause functionality is applied to all the traffic on the link.

The priority flow control (PFC) feature applies pause functionality to specific classes of traffic on the Ethernet link. For example, PFC can provide lossless service for the FCoE traffic and best-effort service for the standard Ethernet traffic. PFC can provide different levels of service to specific classes of Ethernet traffic (using IEEE 802.1p traffic classes).

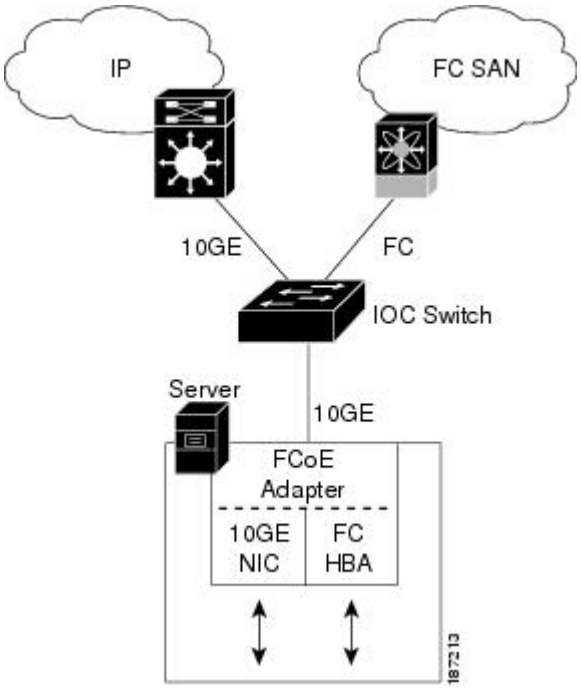
Data Center I/O Consolidation

I/O consolidation allows a single network technology to carry IP, SAN, and IPC traffic. FCoE is the single network technology that allows I/O consolidation. The upper Fibre Channel layers are unchanged, so the Fibre Channel operational model is maintained. FCoE network management and configuration is similar to a native Fibre Channel network.

Cisco Nexus devices use FCoE to carry Fibre Channel and Ethernet traffic on the same physical Ethernet connection between the switch and the server. At the server, the connection terminates to a converged network adapter (CNA). The adapter presents two interfaces to the server's operating system (OS): one Ethernet NIC interface and one Fibre Channel host bus adapter (HBA) interface.

The server OS is not aware of the FCoE encapsulation (see the following figure). At the switch, the incoming Ethernet port separates the Ethernet and Fibre Channel traffic (using EtherType to differentiate the frames). Ethernet frames and Fibre Channel frames are switched to their respective network-side interfaces.

Figure 1: I/O Consolidation



Cisco Nexus devices provide quality of service (QoS) capabilities to ensure lossless or best-effort service across the switch. For Fibre Channel traffic (FCoE) you should apply the lossless QoS classes. By default, best-effort service is applied to all of the Ethernet traffic. You can configure different QoS levels for specific classes of Ethernet traffic.

Virtual Interfaces

When FCoE is enabled, a physical Ethernet cable carries traffic for a logical Fibre Channel connection.

The Cisco Nexus device uses virtual interfaces to represent the logical Fibre Channel connections. For configuration purposes, virtual Fibre Channel interfaces are implemented as Layer 2 subinterfaces of the physical Ethernet interface.

Ethernet features (such as the link debounce timer and VLAN membership) are configured on the physical Ethernet interface. Logical Fibre Channel features (such as VSAN membership) are configured on the virtual Fibre Channel interfaces.

Ethernet Switching

Cisco Nexus devices are Layer 2 devices, which run Cisco NX-OS.

Cisco Nexus devices are designed to support high-density, high-performance Ethernet systems and provide the following Ethernet switching features:

- IEEE 802.1D-2004 Rapid and Multiple Spanning Tree Protocols (802.1w and 802.1s)
- IEEE 802.1Q VLANs and trunks
- IEEE 802.3ad link aggregation
- Private VLANs
- EtherChannels and virtual port channels (vPCs)
- Traffic suppression (unicast, multicast, and broadcast)

FCoE and Fibre Channel Switching

Cisco Nexus devices support data center I/O consolidation by providing FCoE interfaces (to the servers) and native Fibre Channel interfaces (to the SAN).

FCoE and Fibre Channel switching includes the following features:

- Cisco fabric services
- N-port virtualization
- VSANs and VSAN trunking
- Zoning
- Distributed device alias service
- SAN port channels

QoS

Cisco Nexus devices provide quality of service (QoS) capabilities such as traffic prioritization and bandwidth allocation on egress interfaces.

The default QoS configuration on the switch provides lossless service for Fibre Channel and FCoE traffic. QoS must be configured to use native FC or FCoE or FC and FCoE.

The following commands will enable the default QoS configuration which must be configured for native FC or FCoE or FC and FCoE:

```
switch(config)# system qos
switch(config-sys-qos)# service-policy type queuing input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-default-out-policy
switch(config-sys-qos)# service-policy type qos input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type network-qos fcoe-default-nq-policy
```

Note Before enabling FCoE on the Cisco Nexus 5500 Series device, you must attach the pre-defined FCoE policy maps to the type qos, type network-qos, and type queuing policy maps.

Virtual Port Channels

A virtual port channel (vPC) allows links that are physically connected to two different Cisco Nexus devices or Cisco Nexus 2000 Series Fabric Extenders to appear as a single port channel. A vPC can provide multipathing, which allows you to create redundancy by enabling multiple parallel paths between nodes and load balancing traffic where alternative paths exist.

Serviceability

The Cisco Nexus device serviceability functions provide data for network planning and help to improve problem resolution time.

Switched Port Analyzer

The switched port analyzer (SPAN) feature allows an administrator to analyze all traffic between ports by nonintrusively directing the SPAN session traffic to a SPAN destination port that has an external analyzer attached to it.

Ethanalyzer

Ethanalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open source code. Ethanalyzer is a command-line version of Wireshark for capturing and decoding packets. You can use Ethanalyzer to troubleshoot your network and analyse the control-plane traffic.

Call Home

The Call Home feature continuously monitors hardware and software components to provide e-mail-based notification of critical system events. A versatile range of message formats is available for optimal compatibility with pager services, standard e-mail, and XML-based automated parsing applications. The feature offers alert grouping capabilities and customizable destination profiles. This feature can be used, for example, to directly page a network support engineer, send an e-mail message to a network operations center (NOC), and employ Cisco AutoNotify services to directly generate a case with the Cisco Technical Assistance Center (TAC). This feature is a step toward autonomous system operation, which enables networking devices to inform IT when a problem occurs and helps to ensure that the problem is resolved quickly.

Online Diagnostics

Cisco generic online diagnostics (GOLD) is a suite of diagnostic facilities to verify that hardware and internal data paths are operating as designed. Boot-time diagnostics, continuous monitoring, and on-demand and scheduled tests are part of the Cisco GOLD feature set. GOLD allows rapid fault isolation and continuous system monitoring.

Switch Management

Simple Network Management Protocol

Cisco NX-OS is compliant with Simple Network Management Protocol (SNMP) version 1, version 2, and version 3. A full set of Management Information Bases (MIBs) is supported.

Role-Based Access Control

With role-based access control (RBAC), you can limit access to switch operations by assigning roles to users. Administrators can customize access and restrict it to the users who require it.

Configuration Methods

Configuring with CLI, XML Management Interface, or SNMP

You can configure Cisco Nexus devices using the command-line interface (CLI), the XML management interface over SSH, or SNMP as follows:

- CLI —You can configure switches using the CLI from an SSH session, a Telnet session, or the console port. SSH provides a secure connection to the device.
- XML Management Interface over SSH—You can configure switches using the XML management interface, which is a programming interface based on the NETCONF protocol that complements the CLI functionality. For more information, see the *Cisco NX-OS XML Interfaces User Guide*.
- SNMP—SNMP allows you to configure switches using Management Information Bases (MIBs).

Configuring with Cisco Data Center Network Manager

You can configure Cisco Nexus Series switches using the Data Center Network Manager (DCNM) client, which runs on a local PC and uses the DCNM server.

For more information, see the *Cisco DCNM Configuration Guides*.

Configuring with Cisco MDS Fabric Manager

You can configure Cisco Nexus Series switches using the Fabric Manager client, which runs on a local PC and uses the Fabric Manager server.

For more information, see the Cisco Nexus Fabric Manager Software guide for your device.

Network Security Features

Cisco NX-OS includes the following security features:

- Authentication, authorization, and accounting (AAA) and TACACS+
- RADIUS
- Secure Shell (SSH) Protocol Version 2
- Simple Network Management Protocol Version 3 (SNMPv3)
- MAC ACLs and IP ACLs, including port-based ACLs (PACLs) and VLAN-based ACLs (VACLs).

Virtual Device Contexts

Cisco NX-OS can segment operating system and hardware resources into virtual device contexts (VDC) that emulate virtual devices. The Cisco Nexus device does not support multiple VDCs. All switch resources are managed in the default VDC.

For more information, see the *Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts*.

Licensing

The Cisco Nexus device is shipped with its licenses installed. The switch provides commands to manage the licenses and install additional licenses.

Typical Deployment Topologies

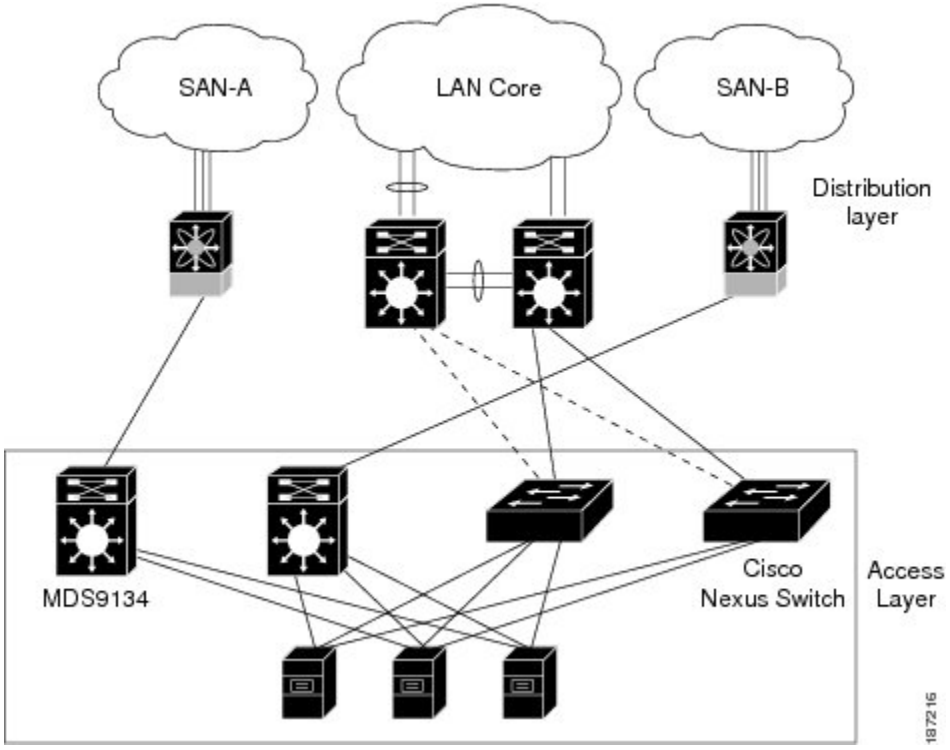
Ethernet TOR Switch Topology

The Cisco Nexus device can be deployed as a 10-Gigabit Ethernet top-of-rack (TOR) switch, with uplinks to the data center LAN distribution layer switches. An example configuration in shown in the following figure.

In this example, the blade server rack incorporates blade switches that support 10-Gigabit Ethernet uplinks to the Cisco Nexus device. The blade switches do not support FCoE, so there is no FCoE traffic and no Fibre Channel ports on the Cisco Nexus device.

In the example configuration, the Cisco Nexus device has Ethernet uplinks to two Catalyst switches. If STP is enabled in the data center LAN, the links to one of the switches will be STP active and the links to the other switch will be STP blocked.

Figure 2: Ethernet TOR Switch Topology



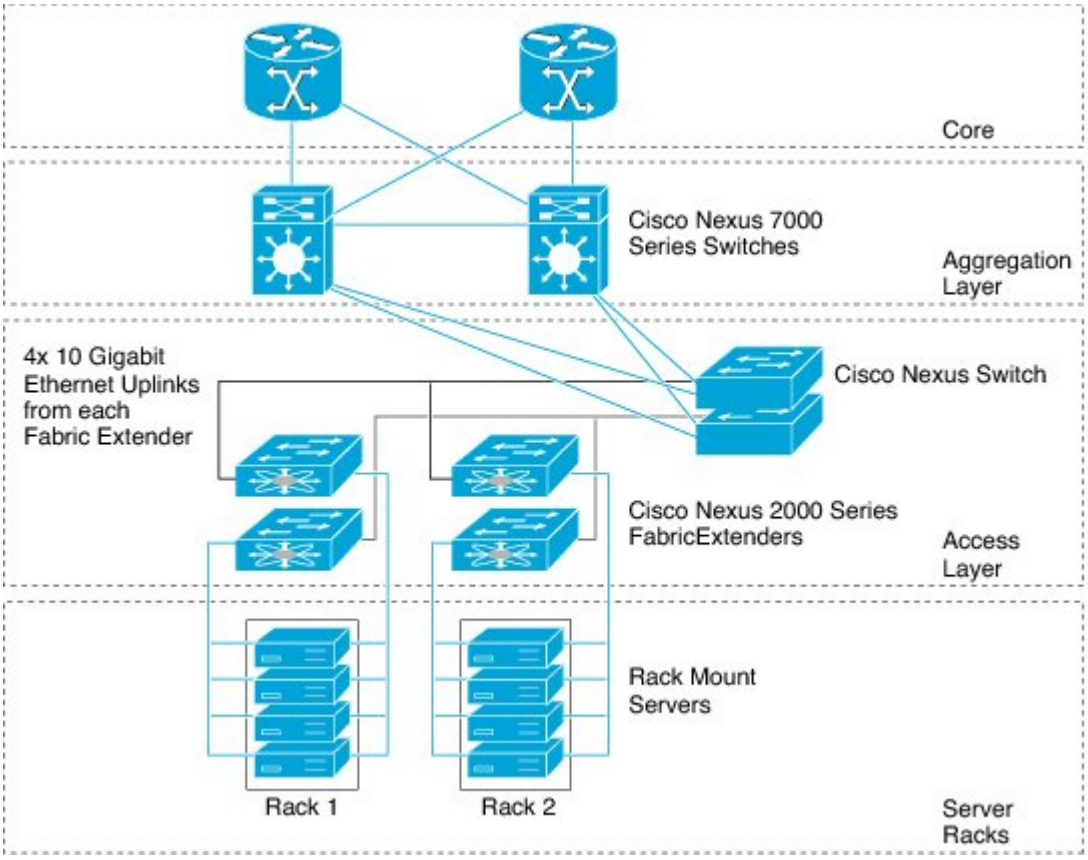
All of the server-side ports on the Cisco Nexus device are running standard Ethernet. FCoE is not required, so the server ports are connected using 10-Gigabit Ethernet NICs.

The servers are connected to the data center SAN through MDS 9134 SAN switches. The server Fibre Channel ports require standard Fibre Channel HBAs.

Fabric Extender Deployment Topology

The following figure shows a simplfied configuration using the Cisco Nexus 2000 Series Fabric Extender in combination with the Cisco Nexus device h to provide a simplified and cost-effective 1-Gigabit TOR solution.

Figure 3: Fabric Extender Deployment Topology



In the example configuration, the Fabric Extender top-of-rack units provide 1-Gigabit host interfaces connected to the servers. The Fabric Extender units are attached to their parent Cisco Nexus devices with 10-Gigabit fabric interfaces.

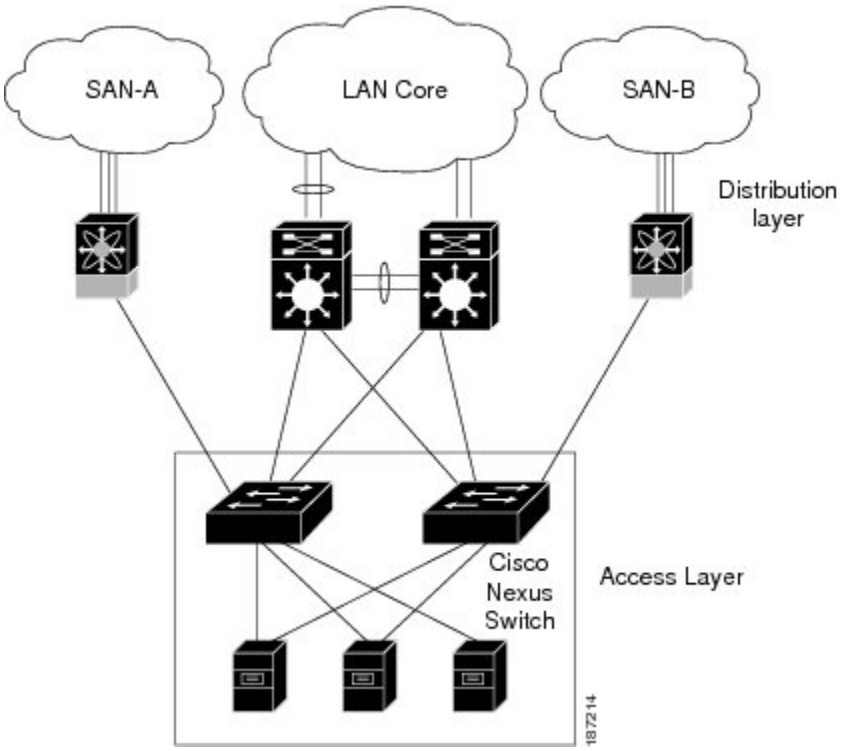
Each Fabric Extender acts as a Remote I/O Module on the parent Cisco Nexus device. All device configurations are managed on the Cisco Nexus device and configuration information is downloaded using inband communication to the Fabric Extender.

See the *Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide* for an overview of the Fabric Extender and configuration details.

Data Center I/O Consolidation Topology

The following figure shows a typical I/O consolidation scenario for the Cisco Nexus device.

Figure 4: I/O Consolidation Topology



The Cisco Nexus device connects to the server ports using FCoE. Ports on the server require converged network adapters. For redundancy, each server connects to both switches. Dual-port CNA adapters can be used for this purpose. The CNA is configured in active-passive mode, and the server needs to support server-based failover.

On the Cisco Nexus device, the Ethernet network-facing ports are connected to two Catalyst 6500 Series switches. Depending on required uplink traffic volume, there may be multiple ports connected to each Catalyst 6500 Series switch, configured as port channels. If STP is enabled in the data center LAN, the links to one of the switches will be STP active and the links to the other switch will be STP blocked.

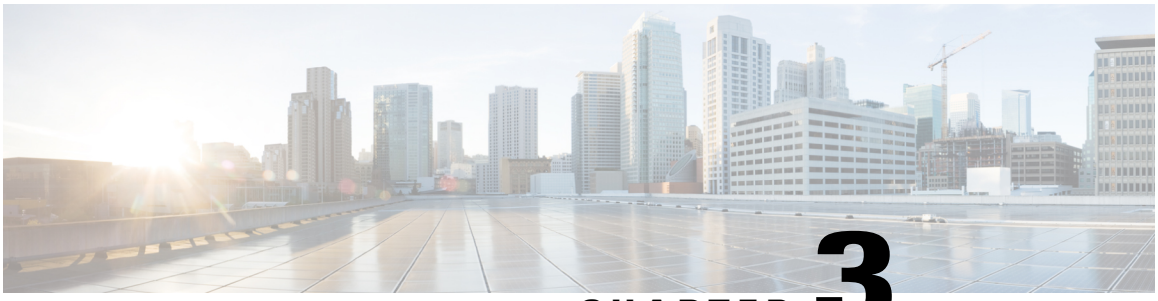
The SAN network-facing ports on the Cisco Nexus device are connected to Cisco MDS 9000 Family switches. Depending on the required traffic volume, there may be multiple Fibre Channel ports connected to each MDS 9000 Family switch, configured as SAN port channels.

Supported Standards

The following table lists the standards supported by the Cisco Nexus devices.

Table 2: IEEE Compliance

Standard	Description
802.1D	MAC Bridges
802.1s	Multiple Spanning Tree Protocol
802.1w	Rapid Spanning Tree Protocol
802.3ad	Link aggregation with LACP
802.3ae	10-Gigabit Ethernet
802.1Q	VLAN Tagging
802.1p	Class of Service Tagging for Ethernet frames



CHAPTER 3

Using the Cisco NX-OS Setup Utility

This chapter contains the following sections:

- Configuring the Switch, page 13

Configuring the Switch

Image Files on the Switch

The Cisco Nexus devices have the following images:

- BIOS and loader images combined in one file
- Kickstart image
- System image that includes a BIOS image that can be upgraded

The switch has flash memory that consists of two separate flash parts:

- A 2 MB flash part holds two BIOS and loader images.
- A 1 GB flash part holds configuration files, kickstart images, systems images, and other files.

The upgradeable BIOS and the golden BIOS are programmed onto the 2 MB flash part. You cannot upgrade the golden BIOS.

When you download a new pair of kickstart and system images, you also get a new BIOS image because it is included in the system image. You can use the **install all** command to upgrade the kickstart, system, and upgradeable BIOS images.

Starting the Switch

A Cisco Nexus switch starts its boot process as soon as its power cord is connected to an A/C source. The switch does not have a power switch.

Boot Sequence

When the switch boots, the golden BIOS validates the checksum of the upgradeable BIOS. If the checksum is valid, then control is transferred to the upgradeable BIOS image. The upgradeable BIOS launches the kickstart image, which then launches the system image. If the checksum of the upgradeable BIOS is not valid, then the golden BIOS launches the kickstart image, which then launches the system image.

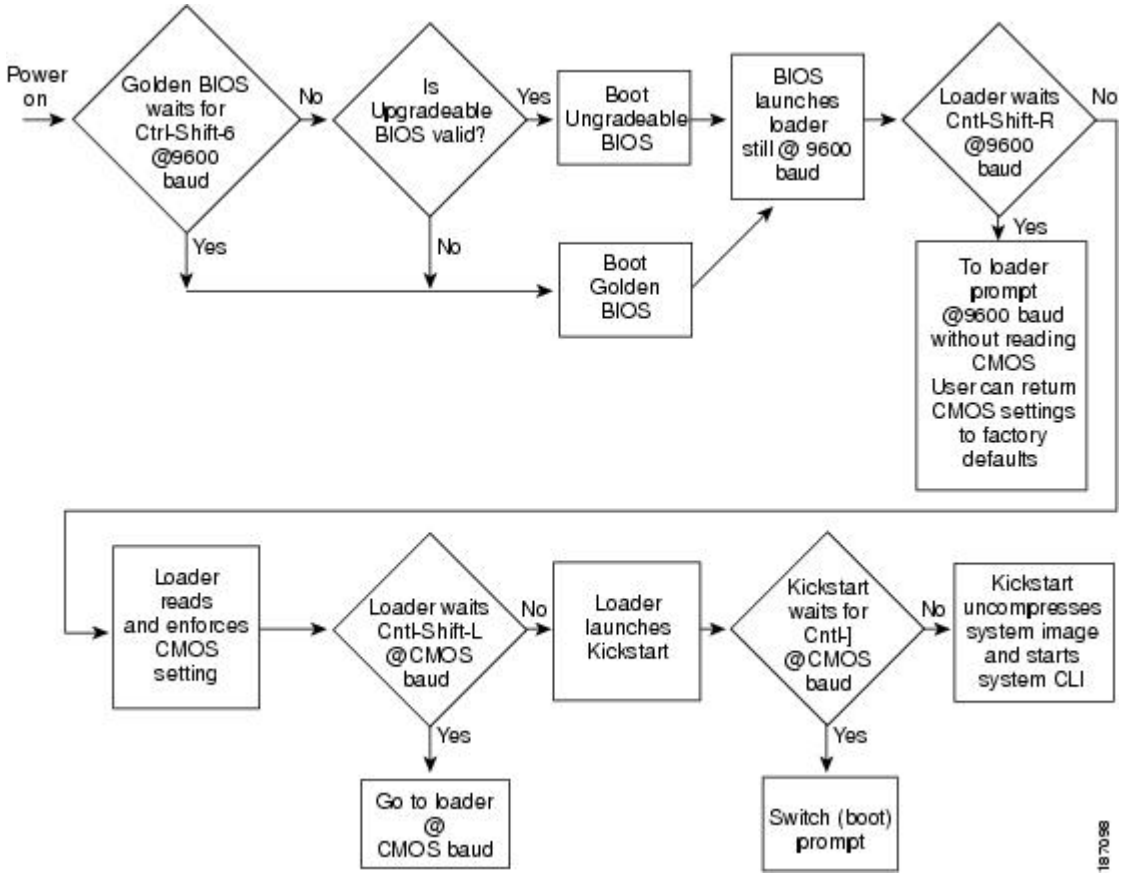
You can force the switch to bypass the upgradeable BIOS and use the golden BIOS instead. If you press **Ctrl-Shift-6** within two seconds of when power is supplied to the switch, the golden BIOS will be used to launch the kickstart image, even if the checksum of the upgradeable BIOS is valid.

Note When you press **Ctrl-Shift-6**, the console settings must be set to their defaults: 9600 baud, 8 data bits, no parity, and 1 stop bit.

Before the boot sequence starts, the BIOS performs internal tests on the switch. If the tests fail, then the loader does not gain control. Instead, the BIOS image retains control and prints a message to the console at 9600 baud every 30 seconds that indicates a failure.

The following figure shows the normal and recovery boot sequence.

Figure 5: Boot Sequence



For additional information, see *Troubleshooting*.

Console Settings

The loader, kickstart, and system images have the following factory default console settings:

- Speed—9600 baud
- Databits—8 bits per byte
- Stopbits—1 bit
- Parity—none

These settings are stored on the switch, and all three images use the stored console settings.

To change a console setting, use the **line console** command in configuration mode. The following example configures a line console and sets the options for that terminal line:

```
switch# configure terminal
switch(config)# line console
switch(config-console)# databits 7
switch(config-console)# exec-timeout 30
switch(config-console)# parity even
switch(config-console)# stopbits 2
```

You cannot change the BIOS console settings. These are the same as the default console settings.

Upgrading the Switch Software

Note You must have the network-admin role before you can upgrade the software image on the switch.

You must log in to the switch on its console port connection.

To upgrade the software on the switch, follow these steps:

SUMMARY STEPS

1. Log in to Cisco.com to access the Software Download Center. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.
2. Access the Software Download Center using this URL: http://www.cisco.com/cisco/web/download/index.html
3. Navigate to the software downloads for Cisco Nexus devices.
4. Read the release notes for the related image file.
5. Select and download the kickstart and system software files to a local server.
6. Ensure that the required space is available in the bootflash: directory for the image file(s) to be copied.
7. If you need more space on the active supervisor module bootflash, delete unnecessary files to make space available.
8. Copy the kickstart and system images to the switch bootflash using a transfer protocol. You can use **ftp**, **tftp**, **scp**, or **sftp**. The examples in this procedure use **scp**.
9. Install the new images, specifying the new image names that you downloaded in the previous step.
10. After the switch completes the installation, log in and verify that the switch is running the required software version.

DETAILED STEPS

Step 1 Log in to Cisco.com to access the Software Download Center. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.

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

Step 2 Access the Software Download Center using this URL: http://www.cisco.com/cisco/web/download/index.html

Step 3 Navigate to the software downloads for Cisco Nexus devices.
You see links to the download images for the switch.

Step 4 Read the release notes for the related image file.

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

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

Example:

```
switch# dir bootflash:
       4681     Nov 24 02:43:52 2008  config
   13176836     Nov 24 07:19:36 2008  gdb.1
      49152     Jan 12 18:38:36 2009  lost+found/
     310556     Dec 23 02:53:28 2008  n1
   20058112     Nov 07 02:35:22 2008  n5000-uk9-kickstart.4.0.1a.N1.0.62.bin
   20217856     Jan 12 18:26:54 2009  n5000-uk9-kickstart.4.0.1a.N2.0.140.bin
   76930262     Nov 07 02:35:22 2008  n5000-uk9.4.0.1a.N1.0.62.bin
  103484727     Jan 12 18:29:08 2009  n5000-uk9.4.0.1a.N2.0.140.bin

Usage for bootflash://sup-local
   74934272 bytes used
    5550080 bytes free
   80484352 bytes total

switch# dir bootflash:
       4681     Nov 24 02:43:52 2008  config
   13176836     Nov 24 07:19:36 2008  gdb.1
      49152     Jan 12 18:38:36 2009  lost+found/
```

```
     310556     Dec 23 02:53:28 2008  n1
   20058112     Nov 07 02:35:22 2008  n5500-uk9-kickstart.4.0.1a.N1.0.62.bin
   20217856     Jan 12 18:26:54 2009  n5500-uk9-kickstart.4.0.1a.N2.0.140.bin
   76930262     Nov 07 02:35:22 2008  n5500-uk9.4.0.1a.N1.0.62.bin
  103484727     Jan 12 18:29:08 2009  n5500-uk9.4.0.1a.N2.0.140.bin

Usage for bootflash://sup-local
   74934272 bytes used
    5550080 bytes free
   80484352 bytes total
```

Caution We recommend that you keep the kickstart and system image files for at least one previous software release to use if the new image files do not load successfully.

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

Example:

```
switch# delete bootflash:n5000-uk9-kickstart.4.0.1a.N1.0.62.bin
switch# delete bootflash:n5000-uk9.4.0.1a.N1.0.62.bin

switch# delete bootflash:n5500-uk9-kickstart.4.0.1a.N1.0.62.bin
switch# delete bootflash:n5500-uk9.4.0.1a.N1.0.62.bin
```

Step 8 Copy the kickstart and system images to the switch bootflash using a transfer protocol. You can use **ftp**, **tftp**, **scp**, or **sftp**. The examples in this procedure use **scp**.

Example:

```
switch# copy scp://user@scpserver.cisco.com/downloads/n5000-uk9.4.1.3.N1.0.96.bin
bootflash:n5000-uk9.4.1.3.N1.0.96.bin
switch# copy scp://user@scpserver.cisco.com/downloads/n5000-uk9-kickstart.4.1.3.N1.0.96.bin
bootflash:n5000-uk9-kickstart.4.1.3.N1.0.96.bin

switch# copy scp://user@scpserver.cisco.com/downloads/n5500-uk9.4.1.3.N1.0.96.bin
bootflash:n5500-uk9.4.1.3.N1.0.96.bin
switch# copy scp://user@scpserver.cisco.com/downloads/n5500-uk9-kickstart.4.1.3.N1.0.96.bin
bootflash:n5500-uk9-kickstart.4.1.3.N1.0.96.bin
```

Step 9 Install the new images, specifying the new image names that you downloaded in the previous step.

Example:

```
switch# install all kickstart bootflash:n5000-uk9-kickstart.4.1.3.N1.0.96.bin system
bootflash:n5000-uk9.4.1.3.N1.0.96.bin

switch# install all kickstart bootflash:n5500-uk9-kickstart.4.1.3.N1.0.96.bin system
bootflash:n5500-uk9.4.1.3.N1.0.96.bin
```

The **install all** command performs the following actions:

- Performs compatibility checks (equivalent to the **show incompatibility** command) for the images that you have specified. If there are compatibility issues, an error message is displayed and the installation does not proceed.
- Displays the compatibility check results and displays whether the installation is disruptive.
- Provides a prompt to allow you to continue or abort the installation.

  Caution After completing the installation, all traffic through the switch is disrupted while the switch reboots.

- Updates the boot variables to reference the specified images and saves the configuration to the startup configuration file.

Step 10 After the switch completes the installation, log in and verify that the switch is running the required software version.

Example:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.2.0
  loader:    version N/A
  kickstart: version 4.1(3)N1(1) [build 4.1(3)N1(0.96)]
  system:    version 4.1(3)N1(1) [build 4.1(3)N1(0.96)]
  BIOS compile time:       06/19/08
  kickstart image file is: bootflash:/n5000-uk9-kickstart.4.1.3.N1.0.96.bin
  kickstart compile time:  7/14/2009 4:00:00 [07/14/2009 04:27:38]
  system image file is:    bootflash:/n5000-uk9.4.1.3.N1.0.96.bin
  system compile time:     7/14/2009 4:00:00 [07/14/2009 05:20:12]

Hardware
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU    with 2074240 kB of memory.
  Processor Board ID JAB1232002F

  Device name: switch
  bootflash:    1003520 kB

Kernel uptime is 13 day(s), 23 hour(s), 25 minute(s), 5 second(s)

Last reset at 720833 usecs after  Tue Jul 14 11:18:32 2009

  Reason: Reset by installer
  System version: 4.1(3)N1(0.96)
  Service:

plugin
  Core Plugin, Ethernet Plugin

switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.2.0
  loader:    version N/A
  kickstart: version 4.1(3)N1(1) [build 4.1(3)N1(0.96)]
  system:    version 4.1(3)N1(1) [build 4.1(3)N1(0.96)]
  BIOS compile time:       06/19/08
  kickstart image file is: bootflash:/n5500-uk9-kickstart.4.1.3.N1.0.96.bin
  kickstart compile time:  7/14/2009 4:00:00 [07/14/2009 04:27:38]
  system image file is:    bootflash:/n5500-uk9.4.1.3.N1.0.96.bin
  system compile time:     7/14/2009 4:00:00 [07/14/2009 05:20:12]

Hardware
  cisco Nexus5500 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU    with 2074240 kB of memory.
  Processor Board ID JAB1232002F

  Device name: switch
  bootflash:    1003520 kB
```

```
Kernel uptime is 13 day(s), 23 hour(s), 25 minute(s), 5 second(s)

Last reset at 720833 usecs after  Tue Jul 14 11:18:32 2009

  Reason: Reset by installer
  System version: 4.1(3)N1(0.96)
  Service:

plugin
  Core Plugin, Ethernet Plugin
```

Downgrading from a Higher Release

The procedure to downgrade the switch is identical to a switch upgrade, except that the image files to be loaded are for an earlier release than the image currently running on the switch.

Note Prior to downgrading to a specific release, check the release notes for the current release installed on the switch, to ensure that your hardware is compatible with the specific release. There are special caveats you must be aware of before you downgrade the switch software to a 4.0(0)-based release. See the Cisco Nexus release notes for your device for details.

SUMMARY STEPS

1. Locate the image files you will use for the downgrade by entering the **dir bootflash:** command.
2. Install the new images.
3. After the switch completes the installation, log in and verify that the switch is running the required software version.

DETAILED STEPS

Step 1 Locate the image files you will use for the downgrade by entering the **dir bootflash:** command.
If the image files are not stored on the bootflash memory, download the files from Cisco.com:

a) Log in to Cisco.com to access the Software Download Center. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.
Note Unregistered Cisco.com users cannot access the links provided in this document.

b) Access the Software Download Center using this URL: http://www.cisco.com/cisco/web/download/index.html

c) Navigate to the software downloads for Cisco Nexus Series switches.
You see links to the download images for the switch.

d) Read the release notes for the related image file then select and download the kickstart and system software files to a local server

e) Ensure that the required space is available in the bootflash: directory for the image file(s) to be copied.
Caution We recommend that you keep the kickstart and system image files for at least one previous software release to use if the new image files do not load successfully.

f) Copy the kickstart and system images to the switch bootflash using a transfer protocol. You can use **ftp**, **tftp**, **scp**, or **sftp**.

Step 2 Install the new images.

Example:
```
switch# install all kickstart bootflash:n5000-uk9-kickstart.4.0.1a.N1.0.62.bin system
bootflash:n5000-uk9.4.0.1a.N1.0.62.bin

switch# install all kickstart bootflash:n5500-uk9-kickstart.4.0.1a.N1.0.62.bin system
bootflash:n5500-uk9.4.0.1a.N1.0.62.bin
```

The **install all** command performs the following actions:

- Performs compatibility checks (equivalent to the **show incompatibility** command) for the images that you have specified. If there are compatibility issues, an error message is displayed and the installation does not proceed.
- Displays the compatibility check results and displays whether the installation is disruptive.
- Provides a prompt to allow you to continue or abort the installation.

  Note A disruptive installation causes traffic disruption while the switch reboots.

- Updates the boot variables to reference the specified images and saves the configuration to the startup configuration file.

Step 3 After the switch completes the installation, log in and verify that the switch is running the required software version.

Example:
```
switch# show version
```

Initial Configuration

Configuration Prerequisites

The following procedure is a review of the tasks you should have completed during hardware installation. These tasks must be completed before you can configure the switch.

SUMMARY STEPS

1. Verify the following physical connections for the new Cisco Nexus device:
2. Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:

DETAILED STEPS

Step 1 Verify the following physical connections for the new Cisco Nexus device:

- The console port is physically connected to a computer terminal (or terminal server).
- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router.

Refer to the Cisco Nexus Hardware Installation guide for your device for more information.

Tip Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.

Step 2 Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

Initial Setup

The first time that you access a switch in your Cisco Nexus series, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the Ethernet interface. This information is required to configure and manage the switch.

Note The IP address can only be configured from the CLI. When the switch powers up for the first time, you should assign the IP address. After you perform this step, the Cisco MDS 9000 Family Fabric Manager can reach the switch through the console port.

Preparing to Configure the Switch

Before you configure Cisco Nexus device for the first time, you need the following information:

- Administrator password.

Note If a password is weak (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password.

- If you are using an IPv4 address for the management interface, you need the following information:
  - IPv4 subnet mask for the switch's management interface.
  - IPv4 address of the default gateway (optional).
- SSH service on the switch (optional).

To enable this service, select the type of SSH key (dsa/rsa/rsa1) and number of SSH key bits (768 to 2048).

- NTP server IPv4 address (optional).
- SNMP community string (optional).
- Switch name (optional).

  This is your switch prompt.

- An additional login account and password (optional).

Note If you are using IPv4, be sure to configure the IPv4 route, the IPv4 default network address, and the IPv4 default gateway address to enable SNMP access.

Default Login

The switch has the network administrator as a default user (admin). You cannot change the default user at any time.

There is no default password so you must explicitly configure a strong password. If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password. If you configure and subsequently forget this new password, you have the option to recover this password.

Note If you enter the **write erase** command and reload the switch, you must reconfigure the default user (admin) password using the setup procedure.

Configuring the Switch

This section describes how to initially configure the switch.

Note Press **Ctrl-C** at any prompt to skip the remaining configuration options and proceed with what you have configured up to that point. However, entering the new password for the administrator is a requirement and cannot be skipped.

Tip If you do not want to answer a previously configured question, or if you want to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

To configure the switch for first time, follow these steps:

SUMMARY STEPS

1. Ensure that the switch is on. Switches in the Cisco Nexus series boot automatically.
2. Enter the new password for the administrator.
3. Enter yes to enter the setup mode.
4. Enter the new password for the administrator (admin is the default).
5. Enter yes (no is the default) to create additional accounts.
6. Enter yes (yes is the default) to create an SNMP read-only community string.
7. Enter a name for the switch.
8. Enter yes (yes is the default) to configure out-of-band management and enter the mgmt0 IPv4 address.
9. Enter yes (yes is the default) to configure the IPv4 default gateway (recommended) and enter the IPv4 address for the default gateway.
10. Enter yes (yes is the default) to enable the Telnet service.
11. Enter yes (no is the default) to enable the SSH service.
12. Enter yes (no is the default) to configure the NTP server and enter the IPv4 address for the NTP server.
13. Enter yes (yes is the default) to configure basic Fibre Channel configurations.
14. Enter shut (shut is the default) to configure the default Fibre Channel switch port interface to the shut (disabled) state.
15. Enter on (on is the default) to configure the switch port trunk mode.
16. Enter permit (deny is the default) to deny a default zone policy configuration.
17. Enter yes (no is the default) to enable a full zone set distribution.
18. You see the new configuration. Review and edit the configuration that you have just entered. Enter no (no is the default) if you are satisfied with the configuration.
19. Enter yes (yes is default) to use and save this configuration:

DETAILED STEPS

Step 1 Ensure that the switch is on. Switches in the Cisco Nexus series boot automatically.

Step 2 Enter the new password for the administrator.

Example:
```
Enter the password for admin: <password>
```

Note Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, they cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>).

Tip If a password is weak (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password. Passwords are case-sensitive.

Step 3 Enter yes to enter the setup mode.

Example:
```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
```

```
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 4 Enter the new password for the administrator (admin is the default).

Example:
```
Enter the password for admin: admin
```

Step 5 Enter yes (no is the default) to create additional accounts.

Example:
```
Create another login account (yes/no) [n]: yes
```

While configuring your initial setup, you can create an additional user account (in the network-admin role) besides the administrator's account.

a) Enter the user login ID.

Example:
```
Enter the user login ID: user_name
```

b) Enter the user password.

Example:
```
Enter the password for user_name: user-password
```

Step 6 Enter yes (yes is the default) to create an SNMP read-only community string.

Example:
```
Configure read-only SNMP community string (yes/no) [n]:yes
SNMP community string: snmp_community
```

Step 7 Enter a name for the switch.

Note Starting with Cisco NX-OS Release 7.3(0)N1(1), the character limit of a switch name is increased from 32 to 63 alphanumeric characters. Also, 63 characters is the maximum length limit for setting hostname using SNMP. The default name is switch.

Example:
```
Enter the switch name: switch_name
```

Step 8 Enter yes (yes is the default) to configure out-of-band management and enter the mgmt0 IPv4 address.

Example:
```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes
Mgmt0 IPv4 address: ip_address
```

Step 9 Enter yes (yes is the default) to configure the IPv4 default gateway (recommended) and enter the IPv4 address for the default gateway.

Example:
```
Configure the default-gateway: (yes/no) [y]: yes
IPv4 address of the default-gateway: default_gateway
```

Step 10 Enter yes (yes is the default) to enable the Telnet service.

Example:
```
Enable the telnet service? (yes/no) [y]: yes
```

Step 11 Enter yes (no is the default) to enable the SSH service.

Example:
```
Enabled SSH service? (yes/no) [n]: yes
```

a) Enter the SSH key type that you would like to generate.

Example:
```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? dsa
```

b) Enter the number of key bits within the specified range.

Example:
```
Enter the number of key bits? (768 to 2048): 768
```

Step 12 Enter yes (no is the default) to configure the NTP server and enter the IPv4 address for the NTP server.

Example:
```
Configure NTP server? (yes/no) [n]: yes
NTP server IP address: ntp_server_IP_address
```

Step 13 Enter yes (yes is the default) to configure basic Fibre Channel configurations.

Example:
```
Enter basic FC configurations (yes/no) [n]: yes
```

Step 14 Enter shut (shut is the default) to configure the default Fibre Channel switch port interface to the shut (disabled) state.

Example:
```
Configure default physical FC switchport interface state (shut/noshut) [shut]: shut
```

Step 15 Enter on (on is the default) to configure the switch port trunk mode.

Example:
```
Configure default physical FC switchport trunk mode (on/off/auto) [on]: on
```

Step 16 Enter permit (deny is the default) to deny a default zone policy configuration.

Example:
```
Configure default zone policy (permit/deny) [deny]: permit
```

Permits traffic flow to all members of the default zone.

Note If you are executing the setup script after entering a **write erase** command, you explicitly must change the default zone policy to permit for VSAN 1 after finishing the script using the following command:

```
Configure read-only SNMP community string (yes/no) [n]: zone default-zone permit vsan 1
```

Step 17 Enter yes (no is the default) to enable a full zone set distribution.

Example:
```
Enable full zoneset distribution (yes/no) [n]: yes
```

Overrides the switch-wide default for the full zone set distribution feature.

Step 18 You see the new configuration. Review and edit the configuration that you have just entered. Enter no (no is the default) if you are satisfied with the configuration.

Example:
```
The following configuration will be applied:
  username admin password <user-password> role network-admin
  snmp-server community snmp_community ro
  switchname switch
  feature telnet
  ssh key dsa 768 force
  feature ssh
  system default switchport shutdown san
  system default switchport trunk mode on
  system default zone default-zone permit
  system default zone distribute full
Would you like to edit the configuration? (yes/no) [n]: no
```

Step 19 Enter yes (yes is default) to use and save this configuration:

Example:
```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type yes to save the new configuration. This operation ensures that the kickstart and system images are also automatically configured.

Changing the Initial Configuration

To make changes to the initial configuration at a later time, enter the **setup** command in EXEC mode:

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
```

```
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process.

Management Interface Configuration

The management interface on the switch allows multiple simultaneous Telnet, SSH, or SNMP sessions. You can remotely configure the switch through the management interface (mgmt0), but first you must configure some IP parameters so that the switch is reachable. You can manually configure the management interface from the CLI through the console port.

About the mgmt0 Interface

The mgmt0 interface on a Cisco Nexus device provides out-of-band management, which enables you to manage the switch by its IPv4 or IPv6 address. The mgmt0 interface is a 10/100/1000 Ethernet port.

Note Before you begin to configure the management interface manually, obtain the switch's IP address and subnet mask. Also make sure that the console cable is connected to the console port.

Configuring the Management Interface

To configure the management (mgmt0) Ethernet interface to connect over IP, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface mgmt 0**
3. Configure the IP address for IPv4 or IPv6:
4. switch(config-if)# **no shutdown**
5. switch(config-if)# **exit**
6. switch(config)# **vrf context management**
7. Configure the IP address (IPv4 or IPv6) for the next hop:
8. switch(config-vrf)# **end**
9. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Step 1 switch# **configure terminal**
Enters configuration mode.

Step 2 switch(config)# **interface mgmt 0**
Selects the management Ethernet interface on the switch and enters interface configuration submode.

Step 3 Configure the IP address for IPv4 or IPv6:

a) switch(config-if)# **ip address** *ipv4-address*[/ *length*]
Configures the IPv4 address and its subnet mask.

b) switch(config-if)# **ip address** *ipv4-address* [*subnet-mask*]
An alternative method that configures the IPv4 address and its subnet mask.

c) switch(config-if)# **ipv6 address** *ipv6-address*[/ *length*]
Configures the IPv6 address and its subnet mask.

Step 4 switch(config-if)# **no shutdown**
Enables the interface.

Step 5 switch(config-if)# **exit**
Returns to configuration mode.

Step 6 switch(config)# **vrf context management**
Enters VRF context management configuration mode.

Step 7 Configure the IP address (IPv4 or IPv6) for the next hop:

a) switch(config-vrf)# **ip route** *ipv4-prefix*[/ *length*] *ipv4-nexthop-address*
Configures the IPv4 address of the next hop.

b) switch(config-vrf)# **ipv6 route** *ipv6-prefix*[/ *length*] *ipv6-nexthop-address*
Configures the IPv6 address of the next hop.

Step 8 switch(config-vrf)# **end**
Returns to EXEC mode.

Step 9 (Optional) switch# **copy running-config startup-config**
Saves your configuration changes to the file system.

In some cases, a switch interface might be administratively shut down. You can check the status of an interface at any time by using the **show interface mgmt 0** command.

Displaying Management Interface Configuration

To display the management interface configuration, use the **show interface mgmt 0** command.

```
switch# show interface mgmt0

mgmt0 is up
    Hardware is GigabitEthernet, address is 000d.ec8f.cb00 (bia 000d.ec8f.cb00)
    Internet Address is 172.16.131.202/24
    MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
       reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA
    full-duplex, 1000 Mb/s
    Input flow-control is off, output flow-control is off
    8540 packets input, 2835036 bytes
    5202 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    570 packets output, 85555 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors
```

Shutting Down the Management Interface

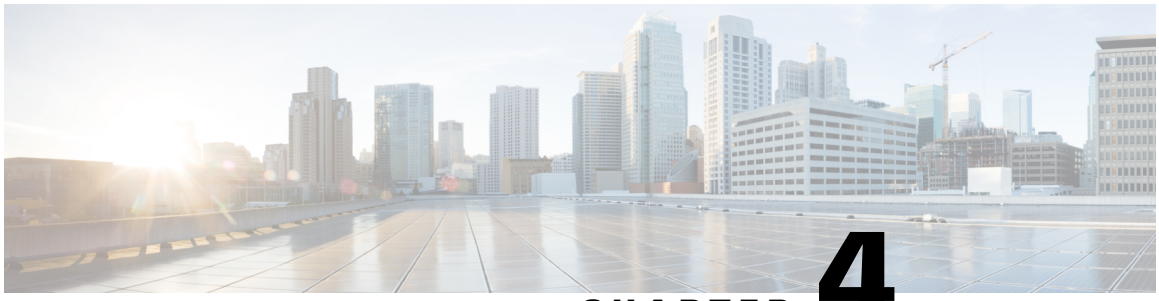
To shut down the management interface (mgmt0), you use the **shutdown** command. A system prompt requests you confirm your action before it executes the command. You can use the force option to bypass this confirmation.

The following example shuts down the interface without using the force option:

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown
Shutting down this interface will drop all telnet sessions.
Do you wish to continue (y/n)? y
```

The following example shuts down the interface using the force option:

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
```



CHAPTER 4

Using PowerOn Auto Provisioning

This chapter contains the following sections:

- Information About PowerOn Auto Provisioning, page 31
- Configuration_File_Selection_Methods, page 38
- Configuration Script Syslog Logging, page 39
- Guidelines and Limitations for POAP, page 39
- Setting Up the Network Environment To Use POAP, page 40
- Configuring a Switch Using POAP, page 40
- Verifying the Device Configuration, page 41

Information About PowerOn Auto Provisioning

PowerOn Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on Cisco Nexus switches that are being deployed in the network for the first time.

When a Cisco Nexus Series switch with the POAP feature boots and does not find the startup configuration, the switch enters POAP mode and checks for a USB device containing the configuration script file. If it finds one, it checks that device to see if it also contains the software image files and the switch configuration file.

If the switch does not find a USB device, or if the USB device does not contain the needed image files or switch configuration file, the switch also locates a DHCP server and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. The switch then obtains the IP address of a TFTP server or the URL of an HTTP server from which it downloads the necessary configuration files.

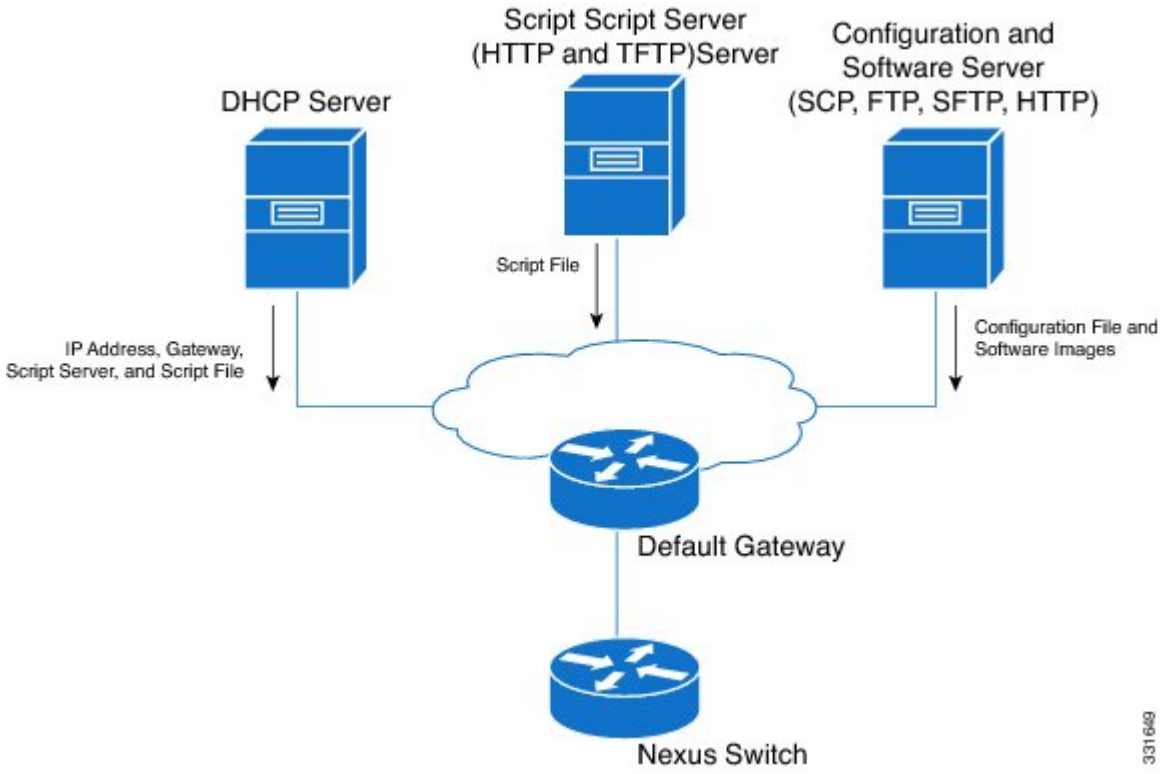
Note The DHCP information is used only during the POAP process if any configuration files are unavailable on the USB device.

Network Requirements for POAP

POAP requires the following network infrastructure:

- A DHCP server to bootstrap the interface IP address, gateway address, DNS server, and log server
- A TFTP or HTTP server containing the configuration script used to automate the software image installation and configuration process
- One or more servers containing the desired software images and configuration files

Figure 6: POAP Network Infrastructure



POAP Configuration Script

The reference script supplied by Cisco supports the following functionality:

- Downloads the configuration file based on the switch's serial number, hostname, MAC address, or location.
- Downloads the software image (system and kickstart images) if the files do not already exist on the switch. The software image is installed on the switch and is used at the next reboot.
- Schedules the downloaded configuration to be applied at the next switch reboot.
- Stores the configuration as the startup-configuration.

We provide sample configuration scripts that were developed using the Python programming language and Tool Command Language (Tcl). You can customize one of these scripts to meet the requirements of your network environment.

For information about customizing this script using Python, see the *Cisco NX-OS Python API Reference Guide* for your platform.

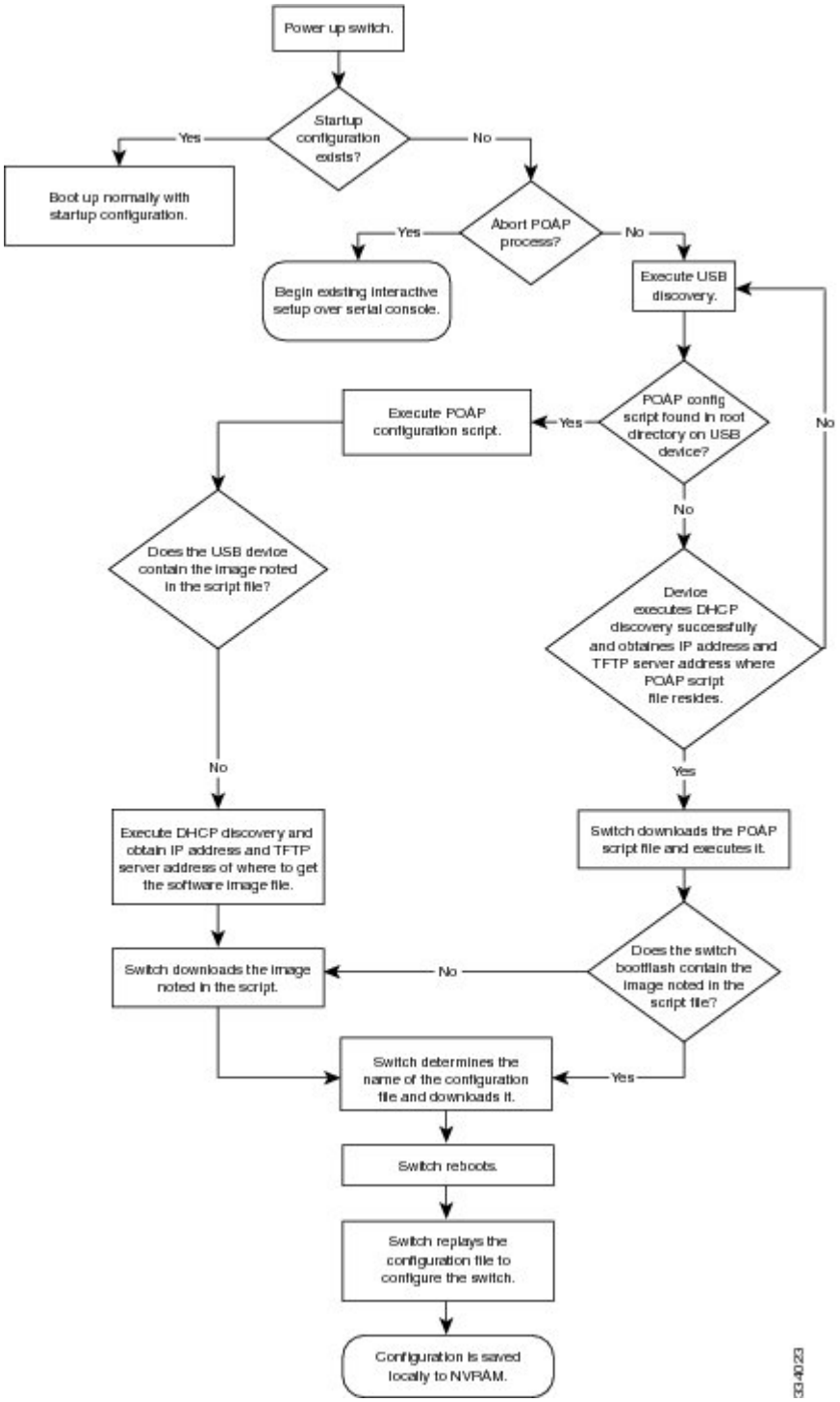
POAP Process

The POAP process has the following phases:

1. Power up
2. USB discovery
3. DHCP discovery
4. Script execution
5. Post-installation reload

Within these phases, other process and decision points occur. The following illustration shows a flow diagram of the POAP process.

Figure 7: POAP Process



Power-Up Phase

When you power-up a switch for the first time, it loads the software image installed at manufacturing and tries to find a configuration file to apply after the switch boots. When no configuration file is found, POAP mode starts.

During startup, a prompt appears asking if you want to abort POAP and continue with normal setup. You can choose to exit or continue with POAP.

Note No user intervention is required for POAP to continue. The prompt that asks if you want to abort POAP remains available until the POAP process is complete.

If you exit POAP mode, you enter the normal interactive setup script. If you continue in POAP mode, all the front-panel interfaces are set up in Layer 2 mode, which ensures that the device does not participate in any Layer 2 forwarding.

USB Discovery Phase

When POAP starts, the process searches the root directory of all accessible USB devices for the POAP configuration script file (either the Python script file, poap_script.py, or the Tcl script file, poap_script.tcl), configuration files, and system and kickstart images.

If the configuration script file is found on a USB device, POAP begins running the configuration script. If the configuration script file is not found on the USB device, POAP executes DHCP discovery. (When failures occur, the POAP process alternates between USB discovery and DHCP discovery, until POAP succeeds or you manually abort the POAP process.)

If the software image and switch configuration files specified in the configuration script are present, POAP uses those files to install the software and configure the switch. If the software image and switch configuration files are not on the USB device, POAP does some cleanup and starts DHCP phase from the beginning.

DHCP Discovery Phase

The switch sends out DHCP discover messages on all of the active interfaces (including the mgmt interface) soliciting DHCP offers from the DHCP server or servers. The DHCP client on the Cisco Nexus switch uses the switch serial number or its MAC address in the client-identifier option to identify itself to the DHCP server. The DHCP server can use this identifier to send information, such as the IP address and script file name, back to the DHCP client.

POAP requires a minimum DHCP lease period of 3600 seconds (1 hour). POAP checks the DHCP lease period. If the DHCP lease period is set to less than 3600 seconds (1 hour), POAP does not complete DHCP negotiation.

The DHCP discover message also mandates some of the options and solicits these options from the DHCP server after receiving the DHCP OFFER from the DHCP server.

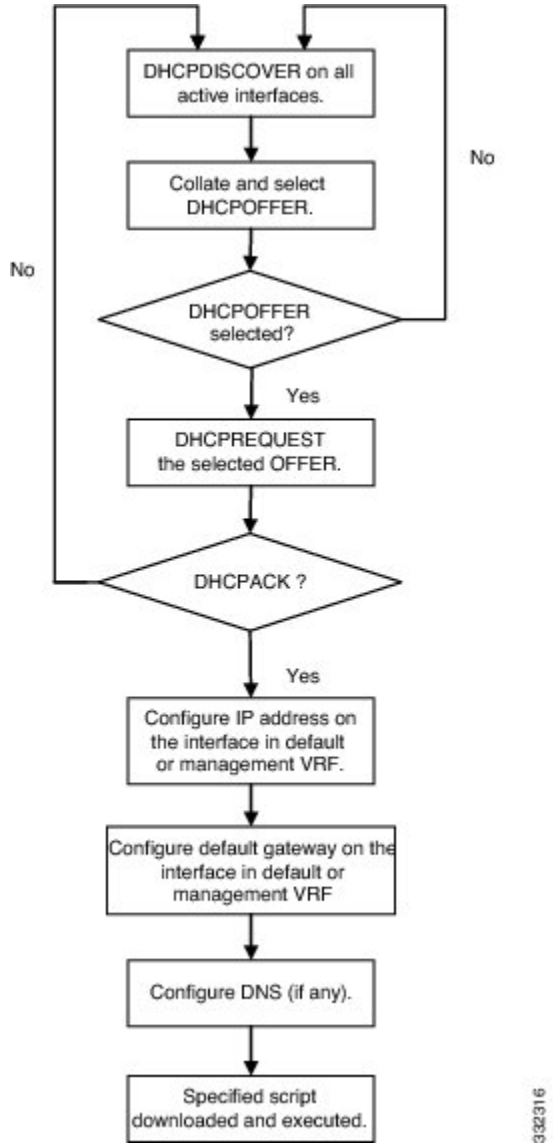
- Option 66 (TFTP server name) or Option 150 (TFTP server address)—The DHCP server relays the TFTP server name or TFTP server address to the DHCP client. The DHCP client uses this information to contact the TFTP server to obtain the script file.
- IP address

- Default gateway
- Option 67 (Bootfile name)—The DHCP server relays the bootfile name to the DHCP client. The bootfile name includes the complete path to the bootfile on the TFTP server. The DHCP client uses this information to download the script file.

When multiple DHCP offers that meet the requirement are received, an offer is randomly chosen. The device completes the DHCP negotiation (request and acknowledgment) with the selected DHCP server, and the DHCP server assigns an IP address to the switch. If there is a failure in any of the subsequent steps in the POAP process, the IP address is released back to the DHCP server.

If no DHCP offers meet the requirements, the switch does not complete the DHCP negotiation (request and acknowledgment) and an IP address is not assigned. The POAP process is reinitiated until it succeeds or you manually abort the POAP process.

Figure 8: DHCP Discovery Phase



Script Execution Phase

Once the device has bootstrapped itself using the information in the DHCP acknowledgement, the switch downloads the script file from the TFTP server or the HTTP server.

The switch runs the configuration script, which downloads and installs the software image and downloads a switch-specific configuration file.

However, the configuration file is not applied to the switch at this point, because the software image currently running on the switch might not support all of the commands in the configuration file. After the switch reboots, it begins running the new software image, if one was installed. At that point, the configuration is applied to the switch.

Note If the switch loses connectivity, the script stops, and the switch reloads its original software images and bootup variables.

Post-Installation Reload Phase

The switch restarts and applies (replays) the configuration on the upgraded software image. Afterward, the switch copies the running configuration to the startup configuration.

Configuration_File_Selection_Methods

Serial Number-Based Configuration File Selection

The switch can download a configuration file based on the switch's serial number. Name the configuration file with the serial number of the switch. For example, if a switch has serial number FOC1621R00R, the configuration file name is conf_FOC1621R00R.cfg.

Hostname-Based Configuration File Selection

When the switch solicits the DHCP server for its IP address and the configuration script filename, the DHCP server offers the switch hostname as well. Then, the switch downloads the configuration file for the specified hostname.

To download a configuration file based on the hostname of the switch, you must configure the following:

- On the DHCP server, add the **option host-name** *hostname* command to the DHCP configuration file (dhcpd.conf). For example, add **option host-name** *nexus-switch-1*.
- In the configuration script, enable hostname support by modifying the configuration script to include the **poap_config_file_mode = poap_hostname**. When the switch runs the configuration script, the switch downloads the file that is named, conf_*hostname*.cfg, that includes the hostname retrieved from the DHCP server.

MAC-Based Configuration File Selection

The switch can use the MAC address of the mgmt 0 interface or of a single Layer 3 interface on the front panel to select the configuration file to be downloaded.

To use the MAC address to identify the configuration file to download, you need to modify the configuration script to include the **poap_config_file_mode = poap_mac** statement. When the switch runs the configuration script, the switch downloads the file that is named conf_*mac-address*.cfg, where the *mac-address*is the MAC

address of the switch. For example, using the MAC address of the management interface, 00:22:AA:BB:CC, the name of the configuration file that the switch downloads is conf_001122AABBCC.cfg.

Location-Based Configuration File Selection

The switch can download a configuration file based on the switch's location. POAP uses the **show cdp neighbor interface** command to derive the configuration file name. To download a configuration file based on the location of the switch, you must indicate **poap_config_file_mode = poap_location** in the POAP configuration script.

For example, Ethernet interface 1/1 on the Nexus 5500 Series switch is connected th Ethernet interface 1/2 on a Nexus 7000 Series switch. The configuration file name should be conf_N7k_eth1/2.cfg

Configuration Script Syslog Logging

The configuration script logs messages locally (on the console) to syslog. To configure logging to a remote server, you need to add the **option log-servers** statement to the dhcpd.conf file on the DHCP server.

The logs identify the device by its serial number and MAC address in the format S/N[SSI151504TL]-MAC[BA:DB:AD:BA:D8:7C].

Guidelines and Limitations for POAP

- The Cisco Nexus switch software image must support POAP for this feature to function.
- POAP does not support provisioning of the switch after it has been configured and is operational. Only auto-provisioning of a switch with no startup configuration is supported.
- If you use POAP to bootstrap a Cisco Nexus device that is a part of a vPC pair using static port-channels on the VPC links, the Cisco Nexus device activates all of its links upon POAP startup. The dually connected device at the end of the VPC links might start sending some or all of its traffic to the port-channel member links connected to the Cisco Nexus device, and the traffic would be lost.

  To work around this issue, you can configure LACP on the vPC links so that the links do not incorrectly start forwarding traffic to the Cisco Nexus device that is being bootstrapped using POAP.
- If you use POAP to bootstrap a Cisco Nexus device that is connected downstream to a Cisco Nexus Series 7000 device through a LACP port-channel, the Cisco Nexus 7000 Series device defaults to suspend its member port if it cannot bundle it as a part of a port-channel. To work around this issue, configure the Cisco Nexus 7000 Series device to not suspend its member ports using the no lacp suspend-individual command from interface configuration mode.
- Important POAP updates are logged in the syslog and are available from the serial console.
- Critical POAP errors are logged to the bootflash. The filename format is *date-time*_poap_*PID*_[init,1,2].log, where *date-time* is in the YYYYMMDD_hhmmss format and *PID* is the process ID.
- Script logs are saved in the bootflash directory. The filename format is *date-time*_poap_*PID*_script.log, where *date-time* is in the YYYYMMDD_hhmmss format and *PID* is the process ID.

- If fabric extender or expansion module interfaces are configured in the configuration file that is used in the POAP process, you must use the Module Pre-Provisioning feature to provision these modules. For information about the Module Pre-Provisioning feature, see the Cisco Nexus System Management Configuration guide for your device.
- During POAP, the Cisco Nexus devices boot up in Layer 2 mode by default. Therefore, uplink connectivity through the front panel ports must be in Layer 2 mode.
- DHCP for NX-OS will be successful, if the DHCP response is set to IP address 255.255.255.255. Since not all the DHCP server including IOS DHCP server sends the DHCP responses to 255.255.255.255, NX-OS is unable to get an IP address as a result POAP does not succeed.
- The **poap transit** command is used if you are performing POAP over fabricpath. When POAP starts, fabricpath interface is converted to classical Ehternet (CE). The neighbor (transit) nodes uses the poap transit configuration for the initial traffic. This command was introduced in Cisco NX-OS Release 7.0(0)N1(1) and is used in global configuration mode. By default, this command is enabled on devices running 7.x images. To disable the **poap transit** command, use the **no poap transit** command.

Setting Up the Network Environment To Use POAP

SUMMARY STEPS

1. Modify the basic configuration script provided by Cisco or create your own script.
2. Deploy a DHCP server and configure it with the interface, gateway, and TFTP server IP addresses and a bootfile with the path and name of the configuration script file. (This information is provided to the switch when it first boots.)
3. Deploy a TFTP or HTTP server to host the configuration script.
4. Deploy one or more servers to host the software images and configuration files.

DETAILED STEPS

Step 1 Modify the basic configuration script provided by Cisco or create your own script.

Step 2 Deploy a DHCP server and configure it with the interface, gateway, and TFTP server IP addresses and a bootfile with the path and name of the configuration script file. (This information is provided to the switch when it first boots.)

Step 3 Deploy a TFTP or HTTP server to host the configuration script.

Step 4 Deploy one or more servers to host the software images and configuration files.

Configuring a Switch Using POAP

Before You Begin

Make sure that the network environment is set up to use POAP. For more information, see the Setting Up the Network Environment To Use POAP, on page 40 section immediately preceeding this section.

SUMMARY STEPS

1. Install the switch in the network.
2. Power on the switch.
3. (Optional) If you want to exit POAP mode and enter the normal interactive setup script, enter **y** (yes).

DETAILED STEPS

Step 1 Install the switch in the network.

Step 2 Power on the switch.
If no configuration file is found, the switch boots in POAP mode and displays a prompt that asks if you want to abort POAP and continue with a normal setup.

No entry is required to continue to boot in POAP mode.

Step 3 (Optional) If you want to exit POAP mode and enter the normal interactive setup script, enter **y** (yes).
The switch boots, and the POAP process begins. For more information, see the POAP Process section.

What to Do Next

Verify the configuration.

Verifying the Device Configuration

To verify the configuration after bootstrapping the device using POAP, use one of the following commands:

Command	Purpose
show running-config	Displays the running configuration.
show startup-config	Displays the startup configuration.

For detailed information about the fields in the output from these commands, see the Cisco Nexus command reference for your device.

CHAPTER 5

Understanding the Command-Line Interface

This chapter contains the following sections:

- Finding Feature Information, page 44
- Information About the CLI Prompt, page 44
- Command Modes, page 44
- Special Characters, page 49
- Keystroke Shortcuts, page 49
- Abbreviating Commands, page 52
- Completing a Partial Command Name, page 52
- Identifying Your Location in the Command Hierarchy, page 53
- Using the no Form of a Command , page 53
- Configuring CLI Variables, page 54
- Command Aliases, page 56
- Command Scripts, page 58
- Context-Sensitive Help , page 60
- Understanding Regular Expressions, page 62
- Searching and Filtering show Command Output, page 63
- Searching and Filtering from the --More-- Prompt, page 68
- Using the Command History, page 69
- Enabling or Disabling the CLI Confirmation Prompts, page 71
- Setting CLI Display Colors, page 71
- Sending Commands to Modules, page 72
- BIOS Loader Prompt, page 73
- Examples Using the CLI , page 73

- Additional References for the CLI, page 75

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information" chapter.

Information About the CLI Prompt

Once you have successfully accessed the device, the CLI prompt displays in the terminal window of your console port or remote workstation as shown in the following example:

```
User Access Verification
login: admin
Password:<password>
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
```

You can change the default device hostname.

From the CLI prompt, you can do the following:

- Use CLI commands for configuring features
- Access the command history
- Use command parsing functions

Note In normal operation, usernames are case sensitive. However, when you are connected to the device through its console port, you can enter a login username in all uppercase letters regardless of how the username was defined. As long as you provide the correct password, the device logs you in.

Command Modes

This section describes command modes in the Cisco NX-OS CLI.

EXEC Command Mode

When you first log in, the Cisco NX-OS software places you in EXEC mode. The commands available in EXEC mode include the **show** commands that display the device status and configuration information, the **clear** commands, and other commands that perform actions that you do not save in the device configuration.

Global Configuration Command Mode

Global configuration mode provides access to the broadest range of commands. The term indicates characteristics or features that affect the device as a whole. You can enter commands in global configuration mode to configure your device globally or to enter more specific configuration modes to configure specific elements such as interfaces or protocols.

SUMMARY STEPS

1. **configure terminal**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.
		
		Note The CLI prompt changes to indicate that you are in global configuration mode.

Interface Configuration Command Mode

One example of a specific configuration mode that you enter from global configuration mode is interface configuration mode. To configure interfaces on your device, you must specify the interface and enter interface configuration mode.

You must enable many features on a per-interface basis. Interface configuration commands modify the operation of the interfaces on the device, such as Ethernet interfaces or management interfaces (mgmt 0).

For more information about configuring interfaces, see the Cisco Nexus interfaces guide for your device.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number*

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**interface** *type number* **Example:** switch(config)# interface ethernet 2/2 switch(config-if)#	Specifies the interface that you want to configure. The CLI places you into interface configuration mode for the specified interface. **Note** The CLI prompt changes to indicate that you are in interface configuration mode.

Subinterface Configuration Command Mode

From global configuration mode, you can access a configuration submode for configuring VLAN interfaces called subinterfaces. In subinterface configuration mode, you can configure multiple virtual interfaces on a single physical interface. Subinterfaces appear to a protocol as distinct physical interfaces.

Subinterfaces also allow multiple encapsulations for a protocol on a single interface. For example, you can configure IEEE 802.1Q encapsulation to associate a subinterface with a VLAN.

For more information about configuring subinterfaces, see the Cisco Nexus interfaces guide for your device. For details about the subinterface commands, see the command reference guide for your device.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number**.**subint*

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**interface** *type number**.**subint*
	
	Example:
	`switch(config)# interface ethernet 2/2.1`
	`switch(config-subif)#`
		Specifies the VLAN interface to be configured.
		The CLI places you into a subinterface configuration mode for the specified VLAN interface.
		Note The CLI prompt changes to indicate that you are in global configuration mode.

	Command or Action	Purpose

Saving and Restoring a Command Mode

The Cisco NX-OS software allows you to save the current command mode, configure a feature, and then restore the previous command mode. The **push** command saves the command mode and the **pop** command restores the command mode.

This example shows how to save and restore a command mode:

```
switch# configure terminal
switch(config)# event manager applet test
switch(config-applet)# push
switch(config-applet)# configure terminal
switch(config)# username testuser password newtest
switch(config)# pop
switch(config-applet)#
```

Exiting a Configuration Command Mode

To exit from any configuration command mode, perform one of the following tasks:

SUMMARY STEPS

1. **exit**
2. **end**
3. (Optional) **Ctrl-Z**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**exit**
	
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits from the current configuration command mode and returns to the previous configuration command mode.

Step 2	**end**
	
	Example:
	`switch(config-if)# end`
	`switch#`
		Exits from the current configuration command mode and returns to EXEC mode.

	Command or Action	Purpose

Step 3	**Ctrl-Z**
	
	Example:
	`switch(config-if)# ^z`
	`switch#`
		(Optional)
		Exits the current configuration command mode and returns to EXEC mode.
		Caution If you press **Ctrl-Z** at the end of a command line in which a valid command has been typed, the CLI adds the command to the running configuration file. In most cases, you should exit a configuration mode using the **exit** or **end** command.

Command Mode Summary

This table summarizes information about the main command modes.

Table 3: Command Mode Summary

Mode	Access Method	Prompt	Exit Method
EXEC	From the login prompt, enter your username and password.	`switch#`	To exit to the login prompt, use the **exit** command.
Global configuration	From EXEC mode, use the **configure terminal** command.	`switch(config)#`	To exit to EXEC mode, use the **end** or **exit** command or press **Ctrl-Z**.
Interface configuration	From global configuration mode, use an interface command and specify an interface with an **interface** command.	`switch(config-if)#`	To exit to global configuration mode, use the **exit** command. To exit to EXEC mode, use the **exit** command or press **Ctrl-Z**.
Subinterface configuration	From global configuration mode, specify a subinterface with an **interface** command.	`switch(config-subif)#`	To exit to global configuration mode, use the **exit** command. To exit to EXEC mode, use the **end** command or press **Ctrl-Z**.

Special Characters

This table lists the characters that have special meaning in Cisco NX-OS text strings and should be used only in regular expressions or other special contexts.

Table 4: Special Characters

Character	Description
%	Percent
#	Pound, hash, or number
...	Ellipsis
|	Vertical bar
< >	Less than or greater than
[ ]	Brackets
{ }	Braces

Keystroke Shortcuts

This table lists command key combinations that can be used in both EXEC and configuration modes.

Table 5: Keystroke Shortcuts

Keystokes	Description
Ctrl-A	Moves the cursor to the beginning of the line.
Ctrl-B	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.
Ctrl-C	Cancels the command and returns to the command prompt.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Moves the cursor to the end of the line.

Keystokes	Description
Ctrl-F	Moves the cursor one character to the right.
Ctrl-G	Exits to the previous command mode without removing the command string.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-L	Redisplays the current command line.
Ctrl-N	Displays the next command in the command history.
Ctrl-O	Clears the terminal screen.
Ctrl-P	Displays the previous command in the command history.
Ctrl-R	Redisplays the current command line.
Ctrl-T	Transposes the character under the cursor with the character located to the right of the cursor. The cursor is then moved one character to the right.
Ctrl-U	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-V	Removes any special meaning for the following keystroke. For example, press Ctrl-V before entering a question mark (?) in a regular expression.
Ctrl-W	Deletes the word to the left of the cursor.
Ctrl-X, H	Lists the history of commands you have entered. When using this key combination, press and release the Ctrl and X keys together before pressing H.
Ctrl-Y	Recalls the most recent entry in the buffer (press keys simultaneously).
Ctrl-Z	Ends a configuration session, and returns you to EXEC mode. When used at the end of a command line in which a valid command has been typed, the resulting configuration is first added to the running configuration file.
Up arrow key	Displays the previous command in the command history.

<table>
<tr><th>Keystokes</th><th>Description</th></tr>
<tr><td>Down arrow key</td><td>Displays the next command in the command history.</td></tr>
<tr><td>Right arrow key
Left arrow key</td><td>Moves your cursor through the command string, either forward or backward, allowing you to edit the current command.</td></tr>
<tr><td>?</td><td>Displays a list of available commands.</td></tr>
<tr><td rowspan="4">Tab</td><td>Completes the word for you after you enter the first characters of the word and then press the Tab key. All options that match are presented.
Use tabs to complete the following items:
• Command names
• Scheme names in the file system
• Server names in the file system
• Filenames in the file system
Example:
<pre>switch(config)# xm<Tab>
switch(config)# xml<Tab>
switch(config)# xml server</pre></td></tr>
<tr><td>Example:
<pre>switch(config)# c<Tab>
callhome class-map clock cts
cdp   cli   control-plane
switch(config)# cl<Tab>
class-map   cli   clock
switch(config)# cla<Tab>
switch(config)# class-map</pre></td></tr>
<tr><td>Example:
<pre>switch# cd bootflash:<Tab>
bootflash: bootflash://sup-1/
bootflash:///   bootflash://sup-2/
bootflash://module-5/
bootflash://sup-active/
bootflash://module-6/ bootflash://sup-local/</pre></td></tr>
<tr><td>Example:
<pre>switch# cd bootflash://mo<Tab>
bootflash://module-5/
bootflash://module-6/cv
switch# cd bootflash://module-</pre></td></tr>
</table>

Abbreviating Commands

You can abbreviate commands and keywords by entering the first few characters of a command. The abbreviation must include sufficient characters to make it unique from other commands or keywords. If you are having trouble entering a command, check the system prompt and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

This table lists examples of command abbreviations.

Table 6: Examples of Command Abbreviations

Command	Abbreviation
configure terminal	**conf t**
copy running-config startup-config	**copy run start**
interface ethernet 1/2	**int e 1/2**
show running-config	**sh run**

Completing a Partial Command Name

If you cannot remember a complete command name, or if you want to reduce the amount of typing you have to perform, enter the first few letters of the command, and then press the **Tab** key. The command line parser will complete the command if the string entered is unique to the command mode. If your keyboard does not have a **Tab** key, press **Ctrl-I** instead.

The CLI recognizes a command once you have entered enough characters to make the command unique. For example, if you enter **conf** in EXEC mode, the CLI will be able to associate your entry with the **configure** command, because only the **configure** command begins with **conf**.

In the following example, the CLI recognizes the unique string for **conf** in EXEC mode when you press the **Tab** key:

```
switch# conf<Tab>
switch# configure
```

When you use the command completion feature the CLI displays the full command name. The CLI does not execute the command until you press the **Return** or **Enter** key. This feature allows you to modify the command if the full command was not what you intended by the abbreviation. If you enter a set of characters that could indicate more than one command, a list of matching commands displays.

For example, entering **co<Tab>** lists all commands available in EXEC mode beginning with **co**:

```
switch# co<Tab>
configure   copy
switch# co
```

Note that the characters you entered appear at the prompt again to allow you to complete the command entry.

Identifying Your Location in the Command Hierarchy

Some features have a configuration submode hierarchy nested more than one level. In these cases, you can display information about your present working context (PWC).

SUMMARY STEPS

1. **where detail**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**where detail**
	
	Example:
	`switch# configure terminal`
	`switch(config)# interface mgmt0`
	`switch(config-if)# where detail`
	`mode:  conf`
	`  interface mgmt0`
	`  username:  admin`
		Displays the PWC.

Using the no Form of a Command

Almost every configuration command has a **no** form that can be used to disable a feature, revert to a default value, or remove a configuration. The Cisco NX-OS command reference publications describe the function of the **no** form of the command whenever a **no** form is available.

This example shows how to disable a feature:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# no feature tacacs+
```

This example shows how to revert to the default value for a feature:

```
switch# configure terminal
switch(config)# banner motd #Welcome to the switch#
switch(config)# show banner motd
Welcome to the switch

switch(config)# no banner motd
switch(config)# show banner motd
User Access Verification
```

This example shows how to remove the configuration for a feature:

```
switch# configure terminal
switch(config)# radius-server host 10.10.2.2
switch(config)# show radius-server
retransmission count:0
```

```
timeout value:1
deadtime value:1
total number of servers:1

following RADIUS servers are configured:
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
        10.10.2.2:
                available for authentication on port:1812
                available for accounting on port:1813

switch(config)# no radius-server host 10.10.2.2
switch(config)# show radius-server
retransmission count:0
timeout value:1
deadtime value:1
total number of servers:1

following RADIUS servers are configured:
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
```

This example shows how to use the **no** form of a command in EXEC mode:

```
switch# cli var name testinterface ethernet1/2
switch# show cli variables
SWITCHNAME="switch"
TIMESTAMP="2009-05-12-13.43.13"
testinterface="ethernet1/2"

switch# cli no var name testinterface
switch# show cli variables
SWITCHNAME="switch"
TIMESTAMP="2009-05-12-13.43.13"
```

Configuring CLI Variables

This section describes CLI variables in the Cisco NX-OS CLI.

About CLI Variables

The Cisco NX-OS software supports the definition and use of variables in CLI commands.

You can refer to CLI variables in the following ways:

- Entered directly on the command line.
- Passed to a script initiated using the **run-script** command. The variables defined in the parent shell are available for use in the child **run-script** command process.

CLI variables have the following characteristics:

- Cannot have nested references through another variable
- Can persist across switch reloads or exist only for the current session

Cisco NX-OS supports one predefined variable: TIMESTAMP. This variable refers to the current time when the command executes in the format YYYY-MM-DD-HH.MM.SS.

Note The TIMESTAMP variable name is case sensitive. All letters must be uppercase.

Configuring CLI Session-Only Variables

You can define CLI session variables to persist only for the duration of your CLI session. These variables are useful for scripts that you execute periodically. You can reference the variable by enclosing the name in parentheses and preceding it with a dollar sign ($), for example $(*variable-name*).

SUMMARY STEPS

1. **cli var name** *variable-name variable-text*
2. (Optional) **show cli variables**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cli var name** *variable-name variable-text* **Example:** `switch# cli var name testinterface ethernet 2/1`	Configures the CLI session variable. The *variable-name* argument is alphanumeric, case sensitive, and has a maximum length of 31 characters. The *variable-text* argument is alphanumeric, case sensitive, can contain spaces, and has a maximum length of 200 characters.
Step 2	**show cli variables** **Example:** `switch# show cli variables`	(Optional) Displays the CLI variable configuration.

Configuring Persistent CLI Variables

You can configure CLI variables that persist across CLI sessions and device reloads.

SUMMARY STEPS

1. **configure terminal**
2. **cli var name** *variable-name variable-text*
3. **exit**
4. (Optional) **show cli variables**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cli var name** *variable-name variable-text* **Example:** `switch(config)# cli var name testinterface ethernet 2/1`	Configures the CLI persistent variable. The variable name is a case-sensitive, alphanumeric string and must begin with an alphabetic character. The maximum length is 31 characters.

Step 3	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	**show cli variables** **Example:** `switch# show cli variables`	(Optional) Displays the CLI variable configuration.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Command Aliases

This section provides information about command aliases.

About Command Aliases

You can define command aliases to replace frequently used commands. The command aliases can represent all or part of the command syntax.

Command alias support has the following characteristics:

- Command aliases are global for all user sessions.
- Command aliases persist across reboots if you save them to the startup configuration.
- Command alias translation always takes precedence over any keyword in any configuration mode or submode.
- Command alias configuration takes effect for other user sessions immediately.

- The Cisco NX-OS software provides one default alias, **alias**, which is the equivalent to the **show cli alias** command that displays all user-defined aliases.
- You cannot delete or change the default command alias **alias**.
- You can nest aliases to a maximum depth of 1. One command alias can refer to another command alias that must refer to a valid command, not to another command alias.
- A command alias always replaces the first command keyword on the command line.
- You can define command aliases for commands in any command mode.
- If you reference a CLI variable in a command alias, the current value of the variable appears in the alias, not the variable reference.
- You can use command aliases for **show** command searching and filtering.

Defining Command Aliases

You can define command aliases for commonly used commands.

SUMMARY STEPS

1. **configure terminal**
2. **cli alias name** *alias-name alias-text*
3. **exit**
4. (Optional) **alias**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**cli alias name** *alias-name alias-text* **Example:** `switch(config)# cli alias name ethint interface ethernet`	Configures the command alias. The alias name is an alphanumeric string that is not case sensitive and must begin with an alphabetic character. The maximum length is 30 characters.

Step 3	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

	Command or Action	Purpose
Step 4	**alias** **Example:** `switch# alias`	(Optional) Displays the command alias configuration.
Step 5	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring Command Aliases for a User Session

You can create a command alias for the current user session that is not available to any other user on the Cisco NX-OS device. You can also save the command alias for future use by the current user account.

SUMMARY STEPS

1. **terminal alias** [**persist**] *alias-name command -string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal alias** [**persist**] *alias-name command -string* **Example:** `switch# terminal alias shintbr show interface brief`	Configures a command alias for the current user session. Use the **persist** keyword to save the alias for future use by the user account. **Note** Do not abbreviate the **persist** keyword.

Command Scripts

This section describes how you can create scripts of commands to perform multiple tasks.

Running a Command Script

You can create a list of commands in a file and execute them from the CLI. You can use CLI variables in the command script.

Note You cannot create the script files at the CLI prompt. You can create the script file on a remote device and copy it to the bootflash:, slot0:, or volatile: directory on the Cisco NX-OS device.

SUMMARY STEPS

1. **run-script** [**bootflash:** | **slot0:** | **volatile:**]*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**run-script** [**bootflash:** | **slot0:** | **volatile:**]*filename* **Example:** `switch# run-script testfile`	Executes the commands in the file on the default directory.

Echoing Information to the Terminal

You can echo information to the terminal, which is particularly useful from a command script. You can reference CLI variables and use formatting options in the echoed text.

This table lists the formatting options that you can insert in the text.

Table 7: Formatting Options for the echo Command

Formatting Option	Description
\b	Inserts back spaces.
\c	Removes the new line character at the end of the text string.
\f	Inserts a form feed character.
\n	Inserts a new line character.
\r	Returns to the beginning of the text line.
\t	Inserts a horizontal tab character.
\v	Inserts a vertical tab character.
\\	Displays a backslash character.
nnn	Displays the corresponding ASCII octal character.

SUMMARY STEPS

1. **echo** [**backslash-interpret**] [*text*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**echo** [**backslash-interpret**] [*text*]
	
	Example:
	`switch# echo This is a test.`
	`This is a test.`
		The **backslash-interpret** keyword indicates that the text string contains formatting options. The *text* argument is alphanumeric, case sensitive, and can contain blanks. The maximum length is 200 characters. The default is a blank line.

Delaying Command Action

You can delay a command action for a period of time, which is particularly useful within a command script.

SUMMARY STEPS

1. **sleep** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**sleep** *seconds* **Example:** `switch# sleep 30`	Causes a delay for a number of seconds. The range is from 0 to 2147483647.

Context-Sensitive Help

The Cisco NX-OS software provides context-sensitive help in the CLI. You can use a question mark (?) at any point in a command to list the valid input options.

CLI uses the caret (^) symbol to isolate input errors. The ^ symbol appears at the point in the command string where you have entered an incorrect command, keyword, or argument.

This table shows example outputs of context sensitive help.

Table 8: Context-Sensitive Help Example

Example Outputs	Description

`switch# clock ?`
`  set  HH:MM:SS Current Time`
`switch# clock`
	Displays the command syntax for the **clock** command in EXEC mode.
	The switch output shows that the **set** keyword is required for using the **clock** command.

`switch# clock set ?`
`  WORD  HH:MM:SS Current Time`
`switch# clock set`
	Displays the command syntax for setting the time.
	The help output shows that the current time is required for setting the clock and how to format the time.

`switch# clock set 13:32:00<CR>`
`% Incomplete command`
`switch#`
	Adds the current time.
	The CLI indicates the command is incomplete.

`switch# <Ctrl-P>` `switch# clock set 13:32:00`	Displays the previous command that you entered.

`switch# clock set 13:32:00 ?`
`  <1-31>  Day of the month`
`switch# clock set 13:32:00`
	Displays the additional arguments for the **clock set** command.

`switch# clock set 13:32:00 18 ?`
`  April  Month of the year`
`  August  Month of the year`
`  December  Month of the year`
`  February  Month of the year`
`  January  Month of the year`
`  July  Month of the year`
`  June  Month of the year`
`  March  Month of the year`
`  May  Month of the year`
`  November  Month of the year`
`  October  Month of the year`
`  September  Month of the year`
`switch# clock set 13:32:00 18`
	Displays the additional arguments for the **clock set** command.

`switch# clock set 13:32:00 18 April 08<CR>` `% Invalid input detected at '^' marker.`	Adds the date to the clock setting. The CLI indicates an error with the caret symbol (^) at 08.

`switch# clock set 13:32:00 18 April ?`
`  <2000-2030>  Enter the year (no abbreviation)`
`switch# clock set 13:32:00 18 April`
	Displays the correct arguments for the year.

`switch# clock set 13:32:00 18 April 2008<CR>` `switch#`	Enters the correct syntax for the **clock set** command.

Understanding Regular Expressions

The Cisco NX-OS software supports regular expressions for searching and filtering in CLI output, such as the **show** commands. Regular expressions are case sensitive and allow for complex matching requirements.

Special Characters

You can also use other keyboard characters (such as ! or ~) as single-character patterns, but certain keyboard characters have special meanings when used in regular expressions.

This table lists the keyboard characters that have special meanings.

Table 9: Special Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
^	Matches the beginning of the string.
$	Matches the end of the string.
_ (underscore)	Matches a comma (,), left brace ({), right brace (}), left parenthesis (( ), right parenthesis ( )), the beginning of the string, the end of the string, or a space. **Note** The underscore is only treated as a regular expression for BGP related commands.

To use these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\). This example contains single-character patterns that match a dollar sign ($), an underscore (_), and a plus sign (+), respectively:

\$ _ \+

Multiple-Character Patterns

You can also specify a pattern that contains multiple characters by joining letters, digits, or keyboard characters that do not have special meanings. For example, a4% is a multiple-character regular expression.

With multiple-character patterns, the order is important. The regular expression a4% matches the character a followed by a 4 followed by a percent sign (%). If the string does not have a4%, in that order, pattern matching

fails. The multiple-character regular expression a. (the character a followed by a period) uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings ab, a!, or a2 are all valid matches for the regular expression.

You can remove the special meaning of a special character by inserting a backslash before it. For example, when the expression a\. is used in the command syntax, only the string a. will be matched.

Anchoring

You can match a regular expression pattern against the beginning or the end of the string by anchoring these regular expressions to a portion of the string using the special characters.

This table lists the special characters that you can use for anchoring.

Table 10: Special Characters Used for Anchoring

Character	Description
^	Matches the beginning of the string.
$	Matches the end of the string.

For example, the regular expression **^con** matches any string that starts with **con**, and **sole$** matches any string that ends with **sole**.

Note The ^ symbol can also be used to indicate the logical function "not" when used in a bracketed range. For example, the expression [^abcd] indicates a range that matches any single letter, as long as it is not a, b, c, or d.

Searching and Filtering show Command Output

Often, the output from **show** commands can be lengthy and cumbersome. The Cisco NX-OS software provides the means to search and filter the output so that you can easily locate information. The searching and filtering options follow a pipe character (|) at the end of the **show** command. You can display the options using the CLI context-sensitive help facility:

```
switch# show running-config | ?
  cut      Print selected parts of lines.
  diff     Show difference between current and previous invocation (creates temp files:
           remove them with 'diff-clean' command and don't use it on commands with big
           outputs, like 'show tech'!)
  egrep    Egrep - print lines matching a pattern
  grep     Grep - print lines matching a pattern
  head     Display first lines
  human    Output in human format
  last     Display last lines
  less     Filter for paging
  no-more  Turn-off pagination for command output
  perl     Use perl script to filter output
  section  Show lines that include the pattern as well as the subsequent lines that are
           more indented than matching line
  sed      Stream Editor
```

```
sort     Stream Sorter
sscp     Stream SCP (secure copy)
tr       Translate, squeeze, and/or delete characters
uniq     Discard all but one of successive identical lines
vsh      The shell that understands cli command
wc       Count words, lines, characters
xml      Output in xml format (according to .xsd definitions)
begin    Begin with the line that matches
count    Count number of lines
end      End with the line that matches
exclude  Exclude lines that match
include  Include lines that match
```

Filtering and Searching Keywords

The Cisco NX-OS CLI provides a set of keywords that you can use with the **show** commands to search and filter the command output.

This table lists the keywords for filtering and searching the CLI output.

Table 11: Filtering and Searching Keywords

Keyword Syntax	Description
begin *string* **Example:** `show version | begin Hardware`	Starts displaying at the line that contains the text that matches the search string. The search string is case sensitive.
count **Example:** `show running-config | count`	Displays the number of lines in the command output.
cut [**-d** *character*] {**-b** | **-c** | **-f** | **-s**} **Example:** `show file testoutput | cut -b 1-10`	Displays only part of the output lines. You can display a number of bytes (**-b**), characters (**-vcut** [**-d** *character*] {**-b** | **-c** | **-f** | **-s**}), or fields (**-f**). You can also use the **-d** keyword to define a field delimiter other than the tag character default. The **-s** keyword suppresses the display of the lines that do not contain the delimiter.
end *string* **Example:** `show running-config | end interface`	Displays all lines up to the last occurrence of the search string.
exclude *string* **Example:** `show interface brief | exclude down`	Displays all lines that do not include the search string. The search string is case sensitive.
head [**lines** *lines*] **Example:** `show logging logfile | head lines 50`	Displays the beginning of the output for the number of lines specified. The default number of lines is 10.

Keyword Syntax	Description
human **Example:** `show version | human`	Displays the output in normal format if you have previously set the output format to XML using the **terminal output xml** command. **Note** The **terminal output xml** command, having 1.0 and 6.x / 7.x versions is used to set the schema (.xsd) file while validating xml. Setting 1.0, the switch will validate /isan/etc/schema/<comp>.xsd file, and if 6.x / 7.x the switch validates /isan/ect/schema/6.x/<comp>.xsd file and /isan/ect/schema/7.x/<comp>.xsd file accordingly based on the version of the image, the switch is running.
include *string* **Example:** `show interface brief | include up`	Displays all lines that include the search string. The search string is case sensitive.
last [*lines*] **Example:** `show logging logfile | last 50`	Displays the end of the output for the number of lines specified. The default number of lines is 10.
no-more **Example:** `show interface brief | no-more`	Displays all the output without stopping at the end of the screen with the —More— prompt.
sscp *SSH-connection-name filename* **Example:** `show version | sscp MyConnection show_version_output`	Redirects the output using streaming secure copy (sscp) to a named SSH connection. You can create the SSH named connection using the **ssh name** command.
wc [**bytes** | **lines** | **words**] **Example:** `show file testoutput | wc bytes`	Displays counts of characters, lines, or words. The default is to display the number of lines, words, and characters.
xml **Example:** `show version | xml`	Displays the output in XML format.

diff Utility

You can compare the output from a **show** command with the output from the previous invocation of that command.

diff-clean [**all-session**] [**all-users**]

This table describes the keywords for the diff utility.

Keyword	Description
all-sessions	Removes diff temporary files from all sessions (past and present sessions) of the current user.
all-users	Removes diff temporary files from all sessions (past and present sessions) of all users.

The Cisco NX-OS software creates temporary files for the most current output for a **show** command for all current and previous users sessions. You can remove these temporary files using the **diff-clean** command.

diff-clean [**all-sessions** | **all-users**]

By default, the **diff-clean** command removes the temporary files for the current user's active session. The **all-sessions** keyword removes temporary files for all past and present sessions for the current user. The **all-users** keyword removes temporary files for all past and present sessions for the all users.

grep and egrep Utilities

You can use the Global Regular Expression Print (grep) and Extended grep (egrep) command-line utilities to filter the **show** command output.

The grep and egrep syntax is as follows:

{**grep** | **egrep**} [**count**] [**ignore-case**] [**invert-match**] [**line-exp**] [**line-number**] [**next** *lines*] [**prev** *lines*] [**word-exp**] *expression*}]

This table lists the **grep** and **egrep** parameters.

Table 12: grep and egrep Parameters

Parameter	Description
count	Displays only the total count of matched lines.
ignore-case	Specifies to ignore the case difference in matched lines.
invert-match	Displays lines that do not match the expression.
line-exp	Displays only lines that match a complete line.
line-number	Specifies to display the line number before each matched line.
next *lines*	Specifies the number of lines to display after a matched line. The default is 0. The range is from 1 to 999.
prev *lines*	Specifies the number of lines to display before a matched line. The default is 0. The range is from 1 to 999.

Parameter	Description
word-exp	Displays only lines that match a complete word.
expression	Specifies a regular expression for searching the output.

less Utility

You can use the less utility to display the contents of the **show** command output one screen at a time. You can enter **less** commands at the : prompt. To display all **less** commands you can use, enter h at the : prompt.

sed Utility

You can use the Stream Editor (sed) utility to filter and manipulate the **show** command output as follows:

sed *command*

The *command* argument contains sed utility commands.

sort Utility

You can use the sort utility to filter **show** command output.

The sort utility syntax is as follows:

sort [**-M**] [**-b**] [**-d**] [**-f**] [**-g**] [**-i**] [**-k** *field-number*[**.***char-position*][*ordering*]] [**-n**] [**-r**] [**-t** *delimiter*] [**-u**]
This table describes the sort utility parameters.

Table 13: sort Utility Parameters

Parameter	Description
-M	Sorts by month.
-b	Ignores leading blanks (space characters). The default sort includes the leading blanks.
-d	Sorts by comparing only blanks and alphanumeric characters. The default sort includes all characters.
-f	Folds lowercase characters into uppercase characters.
-g	Sorts by comparing a general numeric value.
-i	Sorts only using printable characters. The default sort includes nonprintable characters.

Parameter	Description
-k *field-number*[**.***char-position*][*ordering*]	Sorts according to a key value. There is no default key value.
-n	Sorts according to a numeric string value.
-r	Reverses order of the sort results. The default sort output is in ascending order.
-t *delimiter*	Sorts using a specified delimiter. The default delimiter is the space character.
-u	Removes duplicate lines from the sort results. The sort output displays the duplicate lines.

Searching and Filtering from the --More-- Prompt

You can search and filter output from `--More--` prompts in the **show** command output.

This table describes the `--More--` prompt commands.

Table 14: --More-- Prompt Commands

Commands	Description
[*lines*]<space>	Displays output lines for either the specified number of lines or the current screen size.
[*lines*]**z**	Displays output lines for either the specified number of lines or the current screen size. If you use the *lines* argument, that value becomes the new default screen size.
[*lines*]<return>	Displays output lines for either the specified number of lines or the current default number of lines. The initial default is 1 line. If you use the optional *lines* argument, that value becomes the new default number of lines to display for this command.
[*lines*]**d** or [*lines*]Ctrl+shift+D	Scrolls through output lines for either the specified number of lines or the current default number of lines. The initial default is 11 lines. If you use the optional *lines* argument, that value becomes the new default number of lines to display for this command.
q or **Q** or Ctrl-C	Exits the `--More--` prompt.

Commands	Description
[*lines*]**s**	Skips forward in the output for either the specified number of lines or the current default number of lines and displays a screen of lines. The default is 1 line.
[*lines*]**f**	Skips forward in the output for either the specified number of screens or the current default number of screens and displays a screen of lines. The default is 1 screen.
=	Displays the current line number.
[*count*]/*expression*	Skips to the line that matches the regular expression and displays a screen of output lines. Use the optional *count* argument to search for lines with multiple occurrences of the expression. This command sets the current regular expression that you can use in other commands.
[*count*]**n**	Skips to the next line that matches the current regular expression and displays a screen of output lines. Use the optional *count* argument to skip past matches.
{**!** | **:!**[*shell-cmd*]}	Executes the command specified in the *shell-cmd* argument in a subshell.
.	Repeats the previous command.

Using the Command History

The Cisco NX-OS software CLI allows you to access the command history for the current user session. You can recall and reissue commands, with or without modification. You can also clear the command history.

Recalling a Command

You can recall a command in the command history to optionally modify and enter again.

This example shows how to recall a command and reenter it:

```
switch(config)# show cli history
0  11:04:07   configure terminal
1  11:04:28   show interface ethernet 2/24
2  11:04:39     interface ethernet 2/24
3  11:05:13       no shutdown
4  11:05:19     exit
5  11:05:25   show cli history
switch(config)# !1
switch(config)# show interface ethernet 2/24
```

You can also use the **Ctrl-P** and **Ctrl-N** keystroke shortcuts to recall commands.

Controlling CLI History Recall

You can control the commands that you recall from the CLI history using the **Ctrl-P** and **Ctrl-N** keystroke shortcuts. Cisco NX-OS software recalls all commands from the current command mode and higher command modes. For example, if you are working in global configuration mode, the command recall keystroke shortcuts recall both EXEC mode and global configuration mode commands.

Configuring the CLI Edit Mode

You can recall commands from the CLI history using the **Ctrl-P** and **Ctrl-N** keystroke shortcuts and edit them before reissuing them. The default edit mode is emacs. You can change the edit mode to vi.

SUMMARY STEPS

1. [**no**] **terminal edit-mode vi** [**persist**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	[**no**] **terminal edit-mode vi** [**persist**] **Example:** `switch# terminal edit-mode vi`	Changes the CLI edit mode to vi for the user session. The **persist** keyword makes the setting persistent across sessions for the current username. Use the **no** to revert to using emacs.

Displaying the Command History

You can display the command history using the **show cli history** command.

The **show cli history** command has the following syntax:

By default, the number of lines displayed is 12 and the output includes the command number and timestamp.

The example shows how to display default number of lines of the command history:

```
switch# show cli history
```

The example shows how to display 20 lines of the command history:

```
switch# show cli history 20
```

The example shows how to display only the commands in the command history without the command number and timestamp:

```
switch(config)# show cli history unformatted
```

Enabling or Disabling the CLI Confirmation Prompts

For many features, the Cisco NX-OS software displays prompts on the CLI that ask for confirmation before continuing. You can enable or disable these prompts. The default is enabled.

SUMMARY STEPS

1. [**no**] **terminal dont-ask** [**persist**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	[**no**] **terminal dont-ask** [**persist**] **Example:** `switch# terminal dont-ask`	Disables the CLI confirmation prompt. The **persist** keyword makes the setting persistent across sessions for the current username. The default is enabled. Use the **no** form of the command to enable the CLI confirmation prompts.

Setting CLI Display Colors

You can change the CLI colors to display as follows:

- The prompt displays in green if the previous command succeeded.
- The prompt displays in red of the previous command failed.
- The user input displays in blue.
- The command output displays in the default color.

The default colors are those set by the terminal emulator software.

SUMMARY STEPS

1. **terminal color** [**evening**] [**persist**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal color** [**evening**] [**persist**] **Example:** `switch# terminal color`	Sets the CLI display colors for the terminal session. The **evening** keyword is not supported. The **persist** keyword makes the setting persistent across sessions for the current username. The default setting is not persistent.

Sending Commands to Modules

You can send commands directly to modules from the supervisor module session using the **slot** command.

The **slot** has the following syntax:

slot *slot-number* [**quoted**] *command-string*

By default, the keyword and arguments in the *command-string* argument are separated by a space. To send more than one command to a module, separate the commands with a space character, a semicolon character (;), and a space character.

The**quoted** keyword indicates that the command string begins and ends with double quotation marks ("). Use this keyword when you want to redirect the module command output to a filtering utility, such as diff, that is supported only on the supervisor module session.

The following example shows how to display and filter module information:

```
switch# slot 2 show version | grep lc
```

This example shows how to filter module information on the supervisor module session:

```
switch# slot 2 quoted "show version" | diff
switch# slot 4 quoted "show version" | diff -c
*** /volatile/vsh_diff_1_root_8430_slot__quoted_show_version.old       Wed Apr 29 20:10:41
 2009
--- -   Wed Apr 29 20:10:41 2009
***************
*** 1,5 ****
! RAM 1036860 kB
! lc2
  Software
    BIOS:      version 1.10.6
    system:    version 4.2(1) [build 4.2(0.202)]
--- 1,5 ----
! RAM 516692 kB
! lc4
  Software
    BIOS:      version 1.10.6
    system:    version 4.2(1) [build 4.2(0.202)]
***************
*** 12,16 ****
  Hardware
      bootflash: 0 blocks (block size 512b)

!    uptime is 0 days 1 hours 45 minute(s) 34 second(s)

--- 12,16 ----
  Hardware
      bootflash: 0 blocks (block size 512b)

!    uptime is 0 days 1 hours 45 minute(s) 42 second(s)
```

BIOS Loader Prompt

When the supervisor modules power up, a specialized BIOS image automatically loads and tries to locate a valid kickstart image for booting the system. If a valid kickstart image is not found, the following BIOS loader prompt displays:

```
loader>
```

For information on how to load the Cisco NX-OS software from the `<loader>` prompt, see the Cisco Nexus troubleshooting guide for your device.

Examples Using the CLI

This section includes examples of using the CLI.

Defining Command Aliases

This example shows how to define command aliases:

```
cli alias name ethint interface ethernet
cli alias name shintbr show interface brief
cli alias name shintupbr shintbr | include up | include ethernet
```

This example shows how to use a command alias:

```
switch# configure terminal
switch(config)# ethint 2/3
switch(config-if)#
```

Using CLI Session Variables

You can reference a variable using the syntax **$(***variable-name***)**.
This example shows how to reference a user-defined CLI session variable:

```
switch# show interface $(testinterface)
Ethernet2/1 is down (Administratively down)
  Hardware is 10/100/1000 Ethernet, address is 0000.0000.0000 (bia 0019.076c.4dac)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
  Last clearing of "show interface" counters never
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
```

```
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun  0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 0 Tx pause 0 reset
```

Using the System-Defined Timestamp Variable

This example uses $(TIMESTAMP) when redirecting **show** command output to a file:

```
switch# show running-config > rcfg.$(TIMESTAMP)
Preparing to copy....done
switch# dir
       12667     May 01 12:27:59 2008  rcfg.2008-05-01-12.27.59

Usage for bootflash://sup-local
8192 bytes used
20963328 bytes free
20971520 bytes total
```

Running a Command Script

This example displays the CLI commands specified in the script file:

```
switch# show file testfile
configure terminal
interface ethernet 2/1
no shutdown
end
show interface ethernet 2/1
```

This example displays the **run-script** command execution output:

```
switch# run-script testfile
`configure terminal`
`interface ethernet 2/1`
`no shutdown`
`end`
`show interface ethernet 2/1 `
Ethernet2/1 is down (Link not connected)
  Hardware is 10/100/1000 Ethernet, address is 0019.076c.4dac (bia 0019.076c.4dac)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
```

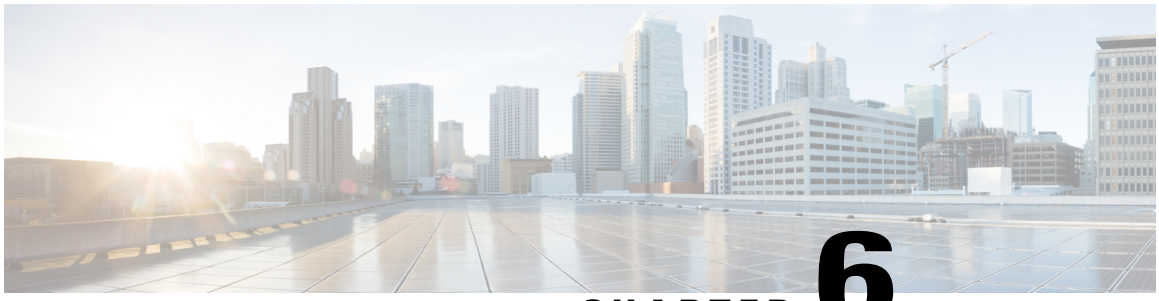
```
Last clearing of "show interface" counters 1d26.2uh
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
Rx
  0 input packets 0 unicast packets 0 multicast packets
  0 broadcast packets 0 jumbo packets 0 storm suppression packets
  0 bytes
Tx
  0 output packets 0 multicast packets
  0 broadcast packets 0 jumbo packets
  0 bytes
  0 input error 0 short frame 0 watchdog
  0 no buffer 0 runt 0 CRC 0 ecc
  0 overrun  0 underrun 0 ignored 0 bad etype drop
  0 bad proto drop 0 if down drop 0 input with dribble
  0 input discard
  0 output error 0 collision 0 deferred
  0 late collision 0 lost carrier 0 no carrier
  0 babble
  0 Rx pause 0 Tx pause 0 reset
```

Additional References for the CLI

This section includes additional information related to the CLI.

Related Documents for the CLI

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 5000 Series NX-OS Command Reference*



CHAPTER 6

Configuring Terminal Settings and Sessions

This chapter contains the following sections:

- Information About Terminal Settings and Sessions, page 77
- Licensing Requirements for Terminal Settings and Sessions, page 79
- Configuring the Console Port, page 79
- Configuring the COM1 Port, page 81
- Configuring Virtual Terminals , page 83
- Configuring Modem Connections, page 85
- Clearing Terminal Sessions, page 90
- Displaying Terminal and Session Information, page 90
- Default Settings for File System Parameters, page 91
- Additional References for Terminal Settings and Sessions, page 91

Information About Terminal Settings and Sessions

This section includes information about terminal settings and sessions.

Terminal Session Settings

The Cisco NX-OS software features allow you to manage the following characteristics of terminals:

Terminal type

Name used by Telnet when communicating with remote hosts

Length

Number of lines of command output displayed before pausing

Width

Number of characters displayed before wrapping the line

Inactive session timeout

Number of minutes that a session remains inactive before the device terminates it

Console Port

The console port is an asynchronous serial port that allows you to connect to the device for initial configuration through a standard RS-232 port with an RJ-45 connector. Any device connected to this port must be capable of asynchronous transmission. You can configure the following parameters for the console port:

Data bits

Specifies the number of bits in an 8-bit byte that is used for data.

Inactive session timeout

Specifies the number of minutes a session can be inactive before it is terminated.

Parity

Specifies the odd or even parity for error detection.

Speed

Specifies the transmission speed for the connection.

Stop bits

Specifies the stop bits for an asynchronous line.

Configure your terminal emulator with 9600 baud, 8 data bits, 1 stop bit, and no parity.

COM1 Port

A COM1 port is an RS-232 port with a DB-9 interface that enables you to connect to an external serial communication device such as a modem. You can configure the following parameters for the COM1 port:

Data bits

Specifies the number of bits in an 8-bit byte that is used for data.

Hardware flowcontrol

Enables the flow-control hardware.

Parity

Specifies the odd or even parity for error detection.

Speed

Specifies the transmission speed for the connection.

Stop bits

Specifies the stop bits for an asynchronous line.

Configure your terminal emulator with 9600 baud, 8 data bits, 1 stop bit, and no parity.

Virtual Terminals

You can use virtual terminal lines to connect to your Cisco NX-OS device. Secure Shell (SSH) and Telnet create virtual terminal sessions. You can configure an inactive session timeout and a maximum sessions limit for virtual terminals.

Licensing Requirements for Terminal Settings and Sessions

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Terminal setting configuration requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the .

Configuring the Console Port

You can set the following characteristics for the console port:

- Data bits
- Inactive session timeout
- Parity
- Speed
- Stop bits

Before You Begin

Log in to the console port.

SUMMARY STEPS

1. **configure terminal**
2. **line console**
3. **databits** *bits*
4. **exec-timeout** *minutes*
5. **parity** {**even** | **none** | **odd**}
6. **speed** {**300** | **1200** | **2400** | **4800** | **9600** | **38400** | **57600** | **115200**}
7. **stopbits** {**1** | **2**}
8. **exit**
9. (Optional) **show line console**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**line console**
	
	Example:
	`switch# line console`
	`switch(config-console)#`
		Enters console configuration mode.

Step 3	**databits** *bits* **Example:** `switch(config-console)# databits 7`	Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.
Step 4	**exec-timeout** *minutes* **Example:** `switch(config-console)# exec-timeout 30`	Configures the timeout for an inactive session. The range is from 0 to 525600 minutes (8760 hours). A value of 0 minutes disables the session timeout. The default is 30 minutes.
Step 5	**parity** {**even**	**none**	**odd**} **Example:** `switch(config-console)# parity even`	Configures the parity. The default is **none**.
Step 6	**speed** {**300**	**1200**	**2400**	**4800**	**9600**	**38400**	**57600**	**115200**} **Example:** `switch(config-console)# speed 115200`	Configures the transmit and receive speed. The default is **115200**.

	Command or Action	Purpose
Step 7	**stopbits** {**1** | **2**} **Example:** `switch(config-console)# stopbits 2`	Configures the stop bits. The default is **1**.

Step 8	**exit**
	
	Example:
	`switch(config-console)# exit`
	`switch(config)#`
		Exits console configuration mode.

Step 9	**show line console** **Example:** `switch(config)# show line console`	(Optional) Displays the console settings.
Step 10	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the COM1 Port

You can set the following characteristics for the COM1 port:

- Data bits
- Flow control on the hardware
- Parity
- Speed
- Stop bits

Before You Begin

Log in to the console port or COM1 port.

SUMMARY STEPS

1. **configure terminal**
2. **line com1**
3. **databits** *bits*
4. **flowcontrol hardware**
5. **parity** {**even** | **none** | **odd**}
6. **speed** {**300** | **1200** | **2400** | **4800** | **9600** | **38400** | **57600** | **115200**}
7. **stopbits** {**1** | **2**}
8. **exit**
9. (Optional) **show line com1**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**line com1**
	
	Example:
	`switch# line com1`
	`switch(config-com1)#`
		Enters COM1 configuration mode.

Step 3	**databits** *bits* **Example:** `switch(config-com1)# databits 7`	Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.
Step 4	**flowcontrol hardware** **Example:** `switch(config-com1)# flowcontrol hardware`	Enables flow control on the hardware. The default is enabled. Use the **no flowcontrol hardware** command to disable flow control on the hardware.
Step 5	**parity** {**even**	**none**	**odd**} **Example:** `switch(config-com1)# parity even`	Configures the parity. The default is **none**.
Step 6	**speed** {**300**	**1200**	**2400**	**4800**	**9600**	**38400**	**57600**	**115200**} **Example:** `switch(config-com1)# speed 115200`	Configures the transmit and receive speed. The default is **9600**.

	Command or Action	Purpose
Step 7	**stopbits** {**1** | **2**} **Example:** `switch(config-com1)# stopbits 2`	Configures the stop bits. The default is **1**.

Step 8	**exit**
	
	Example:
	`switch(config-com1)# exit`
	`switch(config)#`
		Exits COM1 configuration mode.

Step 9	**show line com1** **Example:** `switch(config)# show line com1`	(Optional) Displays the COM1 port settings.
Step 10	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring Virtual Terminals

This section describes how to configure virtual terminals on Cisco NX-OS devices.

Configuring the Inactive Session Timeout

You can configure a timeout for inactive virtual terminal sessions on a Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. **line vty**
3. **exec-timeout** *minutes*
4. **exit**
5. (Optional) **show running-config all | begin vty**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**line vty**
	
	Example:
	`switch# line vty`
	`switch(config-line)#`
		Enters line configuration mode.

Step 3	**exec-timeout** *minutes* **Example:** `switch(config-line)# exec-timeout 30`	Configures the inactive session timeout. The range is from 0 to 525600 minutes (8760 hours). A value of 0 minutes disables the timeout. The default value is 30.

Step 4	**exit**
	
	Example:
	`switch(config-line)# exit`
	`switch(config)#`
		Exits line configuration mode.

Step 5	**show running-config all | begin vty** **Example:** `switch(config)# show running-config all | begin vty`	(Optional) Displays the virtual terminal configuration.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the Session Limit

You can limit the number of virtual terminal sessions on your Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. **line vty**
3. **session-limit** *sessions*
4. **exit**
5. (Optional) **show running-config all | being vty**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**line vty**
	
	Example:
	`switch# line vty`
	`switch(config-line)#`
		Enters line configuration mode.

Step 3	**session-limit** *sessions* **Example:** `switch(config-line)# session-limit 10`	Configures the maximum number of virtual sessions for the Cisco NX-OS device. The range is from 1 to 60. The default is 32.

Step 4	**exit**
	
	Example:
	`switch(config-line)# exit`
	`switch(config)#`
		Exits line configuration mode.

Step 5	**show running-config all | being vty** **Example:** `switch(config)# show running-config all | begin vty`	(Optional) Displays the virtual terminal configuration.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring Modem Connections

You can connect a modem to either the COM1 port or the console port.

We recommend that you use the COM1 port to connect the modem.

Enabling a Modem Connection

You must enable the modem connection on the port before you can use the modem.

Before You Begin

Log in to the console port.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
3. **modem in**
4. **exit**
5. (Optional) **show line**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	Enter one of the following commands:
	Command / **Purpose**
	line com1 — Enters COM1 configuration mode.
	line console — Enters console configuration mode.
	
	Example:
	`switch# line com1`
	`switch(config-com1)#`
		Enters COM1 configuration mode or console configuration mode.

Step 3	**modem in** **Example:** `switch(config-com1)# modem in`	Enables modem input on the COM1 or console port.

Step 4	**exit**
	
	Example:
	`switch(config-com1)# exit`
	`switch(config)#`
		Exits COM1 or console configuration mode.

Step 5	**show line** **Example:** `switch(config)# show line`	(Optional) Displays the console and COM1 settings.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Downloading the Default Initialization String

The Cisco NX-OS software provides a default initialization string that you can download for connecting with the modem. The default initialization string is ATE0Q1&D2&C1S0=1\015.

Before You Begin

Log in to the console port.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
3. **modem init-string default**
4. **exit**
5. (Optional) **show line**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	Enter one of the following commands:
	Option / **Description**
	line com1 — Enters COM1 configuration mode.
	line console — Enters console configuration mode.
	
	Example:
	`switch# line com1`
	`switch(config-com1)#`	

Step 3	**modem init-string default** **Example:** `switch(config-com1)# modem init-string default`	Writes the default initialization string to the modem.

Step 4	**exit**
	
	Example:
	`switch(config-com1)# exit`
	`switch(config)#`
		Exits COM1 or console configuration mode.

	Command or Action	Purpose
Step 5	**show line** **Example:** `switch(config)# show line`	(Optional) Displays the COM1 and console settings.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring and Downloading a User-Specified Initialization String

You can configure and download your own initialization when the default initialization string is not compatible with your modem.

Before You Begin

Log in to the console port.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
3. **modem set-string user-input** *string*
4. **modem init-string user-input**
5. **exit**
6. (Optional) **show line**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	Enter one of the following commands: **Option** / **Description** **line com1** — Enters COM1 configuration mode. **line console** — Enters console configuration mode.	

	Command or Action	Purpose

	Example:
	`switch# line com1`
	`switch(config-com1)#`	

Step 3	**modem set-string user-input** *string* **Example:** `switch(config-com1)# modem set-string user-input ATE0Q1&D2&C1S0=3\015`	Sets the user-specified initialization string for the COM1 or console port. The initialization string is alphanumeric and case sensitive, can contain special characters, and has a maximum of 100 characters. **Note** You must first set the user-input string before initializing the string.
Step 4	**modem init-string user-input** **Example:** `switch(config-com1)# modem init-string user-input`	Writes the user-specified initialization string to the modem connected to the COM1 or console port.

Step 5	**exit**
	Example:
	`switch(config-com1)# exit`
	`switch(config)#`
		Exits COM1 or console configuration mode.

Step 6	**show line** **Example:** `switch(config)# show line`	(Optional) Displays the COM1 and console settings.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Initializing a Modem for a Powered-Up Cisco NX-OS Device

If you connect a modem to a powered-up physical device, you must initialize the modem before you can use it.

Before You Begin

After waiting until the Cisco NX-OS device has completed the boot sequence and the system image is running, connect the modem to either the COM1 port or the console port on the device.

Enable the modem connection on the port.

SUMMARY STEPS

1. **modem connect line** {**com1** | **console**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**modem connect line** {**com1** | **console**} **Example:** `switch# modem connect line com1`	Initializes the modem connected to the device.

Related Topics

Enabling a Modem Connection, on page 85

Clearing Terminal Sessions

You can clear terminal sessions on the Cisco NX-OS device.

SUMMARY STEPS

1. (Optional) **show users**
2. **clear line** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show users** **Example:** `switch# show users`	(Optional) Displays the user sessions on the device.
Step 2	**clear line** *name* **Example:** `switch# clear line pts/0`	Clears a terminal session on a specific line. The line name is case sensitive.

Displaying Terminal and Session Information

To display terminal and session information, perform one of the following tasks:

Command	Purpose
show terminal	Displays terminal settings.

Command	Purpose
show line	Displays the COM1 and console ports settings.
show users	Displays virtual terminal sessions.
show running-config [**all**]	Displays the user account configuration in the running configuration. The **all** keyword displays the default values for the user accounts.

For detailed information about the fields in the output from these commands, see the Cisco Nexus command reference guide for your device.

Default Settings for File System Parameters

This table lists the default settings for the file system parameters.

Table 15: Default File System Settings

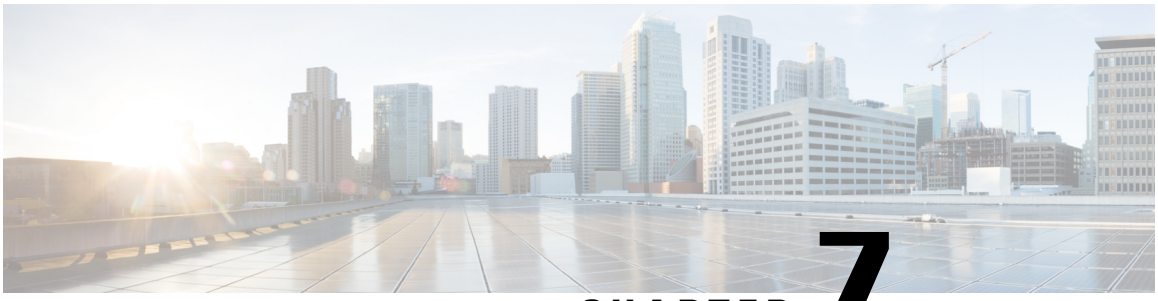
Parameters	Default
Default filesystem	bootflash:

Additional References for Terminal Settings and Sessions

This section includes additional references for terminal settings and sessions on NX-OS devices.

Related Documents for Terminal Settings and Sessions

Related Topic	Document Title
Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 5000 Series Command Reference*



CHAPTER 7

Basic Device Management

This chapter contains the following sections:

- Finding Feature Information, page 93
- Information About Basic Device Management, page 94
- Licensing Requirements for Basic Device Management, page 95
- Changing the Device Hostname, page 95
- Configuring the MOTD Banner, page 96
- Configuring the EXEC Banner, page 97
- Configuring the Time Zone, page 98
- Configuring Summer Time (Daylight Saving Time), page 99
- Manually Setting the Device Clock, page 101
- Setting the Clock Manager, page 101
- Managing Users, page 102
- Verifying the Device Configuration, page 103
- Default Settings for Basic Device Parameters, page 104
- Additional References for Basic Device Management, page 104

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information" chapter or the Feature History table below.

Information About Basic Device Management

This section provides information about basic device management.

Device Hostname

You can change the device hostname displayed in the command prompt from the default (switch) to another character string. When you give the device a unique hostname, you can easily identify the device from the command-line interface (CLI) prompt.

Message-of-the-Day Banner

The message-of-the-day (MOTD) banner displays before the user login prompt on the device. This message can contain any information that you want to display for users of the device.

EXEC Banner

Starting with the Cisco NX-OS Release 7.3(0)N1(1), the EXEC banner is displayed after a user logs in to a switch. This banner can be used to post reminders to your network administrators.

Device Clock

If you do not synchronize your device with a valid outside timing mechanism, such as an NTP clock source, you can manually set the clock time when your device boots.

Clock Manager

The Cisco Nexus chassis may contain clocks of different types that may need to be synchronized. These clocks are a part of various components (such as the supervisor, LC processors, or line cards) and each may be using a different protocol.

The clock manager provides a way to synchronize these different clocks.

Time Zone and Summer Time (Daylight Saving Time)

You can configure the time zone and summer time (daylight saving time) setting for your device. These values offset the clock time from Coordinated Universal Time (UTC). UTC is International Atomic Time (TAI) with leap seconds added periodically to compensate for the Earth's slowing rotation. UTC was formerly called Greenwich Mean Time (GMT).

User Sessions

You can display the active user session on your device. You can also send messages to the user sessions. For more information about managing user sessions and accounts, see the Cisco Nexus security configuration guide for your device.

Licensing Requirements for Basic Device Management

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Basic device management requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the .

Changing the Device Hostname

You can change the device hostname displayed in the command prompt from the default (switch) to another character string.

SUMMARY STEPS

1. **configure terminal**
2. {**hostname** | **switchname**} *name*
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	{**hostname**	**switchname**} *name* **Example:**	Changes the device hostname. The *name* argument is alphanumeric, case sensitive, and has a maximum length of 63 characters. The default name is switch.

	Command or Action	Purpose

	Using the **hostname** command:
	`switch(config)# hostname Engineering1`
	`Engineering1(config)#`
	Using the **switchname** command:
	`Engineering1(config)# switchname Engineering2`
	`Engineering2(config)#`
		Note The **switchname** command performs the same function as the **hostname** command.

Step 3	**exit**
	
	Example:
	`Engineering2(config)# exit`
	`Engineering2#`
		Exits global configuration mode.

Step 4	**copy running-config startup-config** **Example:** `Engineering2# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the MOTD Banner

You can configure the MOTD to display before the login prompt on the terminal when a user logs in. The MOTD banner has the following characteristics:

- Maximum of 80 characters per line
- Maximum of 40 lines

SUMMARY STEPS

1. **configure terminal**
2. **banner motd** *delimiting-character message delimiting-character*
3. **exit**
4. (Optional) **show banner motd**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

	Command or Action	Purpose

Step 2	**banner motd** *delimiting-character message delimiting-character*
	
	Example:
	`switch(config)# banner motd #Welcome to the Switch#`
	`switch(config)#`
		Configures the MOTD banner. Do not use the *delimiting-character* in the *message* text.
		
		Note Do not use " or % as a delimiting character.

Step 3	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	**show banner motd** **Example:** `switch# show banner motd`	(Optional) Displays the configured MOTD banner.
Step 5	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the EXEC Banner

You can configure the EXEC banner to display a message when a user logs in to a device. The EXEC banner has the following characteristics:

- Maximum of 254 characters per line including the delimiting characters
- Maximum of 40 lines

SUMMARY STEPS

1. **configure terminal**
2. **banner exec** *delimiting-character message delimiting-character*
3. (Optional) **no banner exec**
4. **exit**
5. (Optional) **show banner exec**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**banner exec** *delimiting-character message delimiting-character*
	
	Example:
	`switch(config)# banner exec #Welcome to the Test#`
	`switch(config)#`
		Configures the EXEC banner. Do not use the *delimiting-character* in the *message* text.

Step 3	**no banner exec** **Example:** `switch(config)# no banner exec`	(Optional) Resets the value of EXEC banner to the default value. **Note** The default value of the EXEC banner is blank.

Step 4	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	**show banner exec** **Example:** `switch# show banner exec`	(Optional) Displays the configured EXEC banner.
Step 6	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the EXEC Banner

This example shows how to configure the EXEC banner.

```
# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# banner exec #Unauthorized access to this device is prohibited!#
switch(config)# exit
switch# show banner exec
Unauthorized access to this device is prohibited!
```

Configuring the Time Zone

You can configure the time zone to offset the device clock time from UTC.

SUMMARY STEPS

1. **configure terminal**
2. **clock timezone** *zone-name offset-hours offset-minutes*
3. **exit**
4. (Optional) **show clock**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**clock timezone** *zone-name offset-hours offset-minutes* **Example:** `switch(config)# clock timezone EST -5 0`	Configures the time zone. The *zone-name* argument is a 3-character string for the time zone acronym (for example, PST or EST). The *offset-hours* argument is the offset from the UTC and the range is from –23 to 23 hours. The range for the *offset-minutes* argument is from 0 to 59 minutes.

Step 3	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	**show clock** **Example:** `switch# show clock`	(Optional) Displays the time and time zone.
Step 5	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring Summer Time (Daylight Saving Time)

You can configure when summer time, or daylight saving time, is in effect for the device and the offset in minutes.

SUMMARY STEPS

1. **configure terminal**
2. **clock summer-time** *zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes*
3. **exit**
4. (Optional) **show clock detail**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**clock summer-time** *zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes* **Example:** `switch(config)# clock summer-time PDT 1 Sunday March 02:00 1 Sunday November 02:00 60`	Configures summer time or daylight saving time. The *zone-name* argument is a three character string for the time zone acronym (for example, PST and EST). The values for the *start-day* and *end-day* arguments are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, and **Sunday**. The values for the *start-month* and *end-month* arguments are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**. The value for the *start-time* and *end-time* arguments are in the format *hh*:*mm*. The range for the *offset-minutes* argument is from 0 to 1440 minutes.

Step 3	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	**show clock detail** **Example:** `switch(config)# show clock detail`	(Optional) Displays the configured MOTD banner.
Step 5	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Manually Setting the Device Clock

You can set the clock manually if your device cannot access a remote time source.

Before You Begin

Configure the time zone.

SUMMARY STEPS

1. **clock set** *time day month year*
2. (Optional) **show clock**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**clock set** *time day month year*
	
	Example:
	`switch# clock set 15:00:00 30 May 2008`
	`Fri May 30 15:14:00 PDT 2008`
		Configures the device clock.
		The format for the *time* argument is *hh*:*mm*:*ss*.
		The range for the *day* argument is from 1 to 31.
		The values for the *month* argument are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**.
		The range for the *year* argument is from 2000 to 2030.

Step 2	**show clock** **Example:** `switch(config)# show clock`	(Optional) Displays the current clock value.

Related Topics

Configuring the Time Zone, on page 98

Setting the Clock Manager

You can configure the clock manager to synchronize all the clocks of the components in the Cisco Nexus chassis.

SUMMARY STEPS

1. **clock protocol** *protocol* **vdc** *vdc-num*
2. (Optional) **show run clock_manager**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clock protocol** *protocol* **vdc** *vdc-num* **Example:** `# clock protocol ptp vdc 2`	Configures the clock manager. The values for the *protocol* argument are **ptp**, **ntp**, and **none**. The following describes the values: • **ptp—**Synchronizes clocks with Precision Time Protocol (PTP) as described by IEEE 1588. • **ntp—** Synchronizes clocks with Network Time Protocol (NTP). • **none—**Use **clock set** to set supervisor clocks. **Note** When **none** is used, the clock in the specified VDC must be configured. **Note** Once the protocol is configured, the clock in the specified VDC must use that protocol. For example, if the **clock protocol ptp vdc 2** command is entered, then PTP should be configured in VDC 2. The range for the *vdc* argument is 1 to 8.
Step 2	**show run clock_manager** **Example:** `#show run clock_manager`	(Optional) Displays the configuration of the clock manager.

Managing Users

You can display information about users logged into the device and send messages to those users.

Displaying Information about the User Sessions

You can display information about the user session on the device.

SUMMARY STEPS

1. **show users**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show users** **Example:** `switch# show users`	Displays the user sessions.

Sending a Message to Users

You can send a message to active users currently using the device CLI.

SUMMARY STEPS

1. (Optional) **show users**
2. **send** [**session** *line*] *message-text*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show users** **Example:** `switch# show users`	(Optional) Displays the active user sessions.
Step 2	**send** [**session** *line*] *message-text* **Example:** `switch# send Reloading the device is 10 minutes!`	Sends a message to all active users or to a specific user. The message can be up to 80 alphanumeric characters and is case sensitive.

Verifying the Device Configuration

To verify the configuration after bootstrapping the device using POAP, use one of the following commands:

Command	Purpose
show running-config	Displays the running configuration.
show startup-config	Displays the startup configuration.

For detailed information about the fields in the output from these commands, see the Cisco Nexus command reference for your device.

Default Settings for Basic Device Parameters

This table lists the default settings for basic device parameters.

Table 16: Default Basic Device Parameters

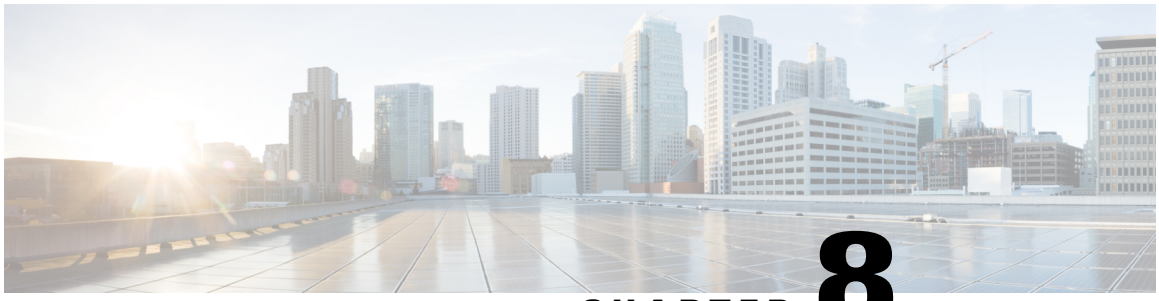
Parameters	Default
MOTD banner text	User Access Verification
Clock time zone	UTC

Additional References for Basic Device Management

You can find additional information related to basic device management.

Related Documents for Basic Device Management

Related Topic	Document Title
Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference Cisco Nexus 5500 Series Command Reference*



CHAPTER 8

Using the Device File Systems, Directories, and Files

This chapter contains the following sections:

- Information about the External Storage Devices, Device File Systems, Directories, and Files, page 105
- Licensing Requirements for File Systems, Directories, and Files, page 107
- Working with Directories, page 107
- Working with Files, page 110
- Working with Archive Files, page 115
- Examples of Using the File System, page 118
- Default Settings for File System Parameters, page 122
- Additional References for File Systems, page 122

Information about the External Storage Devices, Device File Systems, Directories, and Files

This section describes file systems, directories, and files on the Cisco NX-OS device.

File Systems

The syntax for specifying a local file system is *filesystem*:[//*modules*/].
This table describes file systems that you can reference on your device.

Table 17: File System Syntax Components

File System Name	Module	Description
bootflash	sup-active sup-local	Internal CompactFlash memory located on the active supervisor module used for storing image files, configuration files, and other miscellaneous files. The initial default directory is bootflash.
	sup-standby sup-remote	Internal CompactFlash memory located on the standby supervisor module used for storing image files, configuration files, and other miscellaneous files.
volatile	—	Volatile random-access memory (VRAM) located on a supervisor module used for temporary or pending changes.
log	—	Memory on the active supervisor that stores logging file statistics.
system	—	Memory on a supervisor module used for storing the running-configuration file.
debug	—	Memory on a supervisor module used for debug logs.

Directories

You can create directories on bootflash: and external flash memory (slot0:, usb1:, and usb2:). You can navigate through these directories and use them for files.

Files

You create and access files on bootflash:. volatile:, slot0:, usb1:, and usb2: file systems. You can only access files on the system: file systems. You can use the debug: file system for debug log files specified in the **debug logfile** command.

You can download files, such as system image files, from remote servers using FTP, Secure Copy (SCP), Secure Shell FTP (SFTP), and TFTP. You can also copy files from an external server to the device, because the device can act as an SCP server.

Licensing Requirements for File Systems, Directories, and Files

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Using the file systems, directories, and files requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Working with Directories

This section describes how to work with directories on the Cisco NX-OS device.

Identifying the Current Directory

You can display the directory name of your current directory.

SUMMARY STEPS

1. **pwd**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**pwd** **Example:** `switch# pwd`	Displays the name of your current directory.

Changing the Current Directory

You can change the current directory for file system operations. The initial default directory is bootflash:.

SUMMARY STEPS

1. (Optional) **pwd**
2. **cd** {*directory* | *filesystem*:[//*module*/][*directory*]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**pwd** **Example:** `switch# pwd`	(Optional) Displays the name of your current default directory.
Step 2	**cd** {*directory* | *filesystem*:[//*module*/][*directory*]} **Example:** `switch# cd slot0:`	Changes to a new current directory. The file system, module, and directory names are case sensitive.

Creating a Directory

You can create directories in the bootflash: and flash device file systems.

SUMMARY STEPS

1. (Optional) **pwd**
2. (Optional) **cd** {*directory* | *filesystem*:[//*module*/][*directory*]}
3. **mkdir** [*filesystem*:[//*module*/]]*directory*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**pwd** **Example:** `switch# pwd`	(Optional) Displays the name of your current default directory.
Step 2	**cd** {*directory* | *filesystem*:[//*module*/][*directory*]} **Example:** `switch# cd slot0:`	(Optional) Changes to a new current directory. The file system, module, and directory names are case sensitive.
Step 3	**mkdir** [*filesystem*:[//*module*/]]*directory* **Example:** `switch# mkdir test`	Creates a new directory. The *filesystem* argument is case sensitive. The *directory* argument is alphanumeric, case sensitive, and has a maximum of 64 characters.

Displaying Directory Contents

You can display the contents of a directory.

SUMMARY STEPS

1. **dir** [*directory* | *filesystem*:[//*module*/][*directory*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir** [*directory* | *filesystem*:[//*module*/][*directory*]] **Example:** `switch# dir bootflash:test`	Displays the directory contents. The default is the current working directory. The file system and directory names are case sensitive.

Deleting a Directory

You can remove directories from the file systems on your device.

Before You Begin

Ensure that the directory is empty before you try to delete it.

SUMMARY STEPS

1. (Optional) **pwd**
2. (Optional) **dir** [*filesystem* :[//*module*/][*directory*]]
3. **rmdir** [*filesystem* :[//*module*/]]*directory*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**pwd** **Example:** `switch# pwd`	(Optional) Displays the name of your current default directory.
Step 2	**dir** [*filesystem* :[//*module*/][*directory*]] **Example:** `switch# dir bootflash:test`	(Optional) Displays the contents of the current directory. The file system, module, and directory names are case sensitive. If the directory is not empty, you must delete all the files before you can delete the directory.

	Command or Action	Purpose
Step 3	**rmdir** [*filesystem* **:**[*//module/*]]*directory* **Example:** `switch# rmdir test`	Deletes a directory. The file system and directory name are case sensitive.

Accessing Directories on the Standby Supervisor Module

You can access all file systems on the standby supervisor module (remote) from a session on the active supervisor module. This feature is useful when copying files to the active supervisor modules requires similar files to exist on the standby supervisor module. To access the file systems on the standby supervisor module from a session on the active supervisor module, you specify the standby supervisor module in the path to the file using either *filesystem***://sup-remote/** or *filesystem***://sup-standby/**.

Working with Files

This section describes how to work with files on the Cisco NX-OS device.

Moving Files

You can move a file from one directory to another directory.

Caution If a file with the same name already exists in the destination directory, that file is overwritten by the moved file.

You can use the **move** command to rename a file by moving the file within the same directory.

SUMMARY STEPS

1. (Optional) **pwd**
2. (Optional) **dir** [*filesystem***:**[*//module/*][*directory*]]
3. **move** [*filesystem***:**[*//module/*][*directory /*] | *directory/*]*source-filename* {{*filesystem***:**[*//module/*][*directory /*] | *directory/*}[*target-filename*] | *target-filename*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**pwd** **Example:** `switch# pwd`	(Optional) Displays the name of your current default directory.
Step 2	**dir** [*filesystem*:[//*module*/][*directory*]] **Example:** `switch# dir bootflash`	(Optional) Displays the contents of the current directory. The file system and directory name are case sensitive.
Step 3	**move** [*filesystem*:[//*module*/][*directory* /] | *directory*/]*source-filename* {{*filesystem*:[//*module*/][*directory* /] | *directory*/}[*target-filename*] | *target-filename*} **Example:** `switch# move test old_tests/test1`	Moves a file. The file system, module, and directory names are case sensitive. The *target-filename* argument is alphanumeric, case sensitive, and has a maximum of 64 characters. If the *target-filename* argument is not specified, the filename defaults to the *source-filename* argument value.

Copying Files

You can make copies of files, either within the same directory or on another directory.

Note Use the **dir** command to ensure that enough space is available in the target file system. If enough space is not available, use the **delete** command to remove unneeded files.

SUMMARY STEPS

1. (Optional) **pwd**
2. (Optional) **dir** [*filesystem*:[//*module*/][*directory*]]
3. **copy** [*filesystem*:[//*module*/][*directory*/] | *directory*/]*source-filename* | {*filesystem*:[//*module*/][*directory*/]] | *directory*/}[*target-filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**pwd** **Example:** `switch# pwd`	(Optional) Displays the name of your current default directory.

	Command or Action	Purpose
Step 2	**dir** [*filesystem*:[//*module*/][*directory*]] **Example:** `switch# dir bootflash`	(Optional) Displays the contents of the current directory. The file system and directory name are case sensitive.
Step 3	**copy** [*filesystem*:[//*module*/][*directory*/] | *directory*/]*source-filename* | {*filesystem*:[//*module*/][*directory*/]] | *directory*/}[*target-filename*] **Example:** `switch# copy test old_tests/test1`	Copies a file. The file system, module, and directory names are case sensitive. The *source-filename* argument is alphanumeric, case sensitive, and has a maximum of 64 characters. If the *target-filename* argument is not specified, the filename defaults to the *source-filename* argument value. The copy command supports ftp, scp, sftp, tftp and http protocols.

Deleting Files

You can delete a file from a directory.

SUMMARY STEPS

1. (Optional) **dir** [*filesystem*:[//*module*/][*directory*]]
2. **delete** {*filesystem*:[//*module*/][*directory*/] | *directory*/}*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir** [*filesystem*:[//*module*/][*directory*]] **Example:** `switch# dir bootflash`	(Optional) Displays the contents of the current directory. The file system and directory name are case sensitive.
Step 2	**delete** {*filesystem*:[//*module*/][*directory*/] | *directory*/}*filename* **Example:** `switch# delete test old_tests/test1`	Deletes a file. The file system, module, and directory names are case sensitive. The *source-filename* argument is case sensitive. **Caution** If you specify a directory, the **delete** command deletes the entire directory and all its contents.

Displaying File Contents

You can display the contents of a file.

SUMMARY STEPS

1. **show file** [*filesystem*:[//*module*/]][*directory*/]*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show file** [*filesystem*:[//*module*/]][*directory*/]*filename* **Example:** `switch# show file bootflash:test-results`	Displays the file contents.

Displaying File Checksums

You can display checksums to check the file integrity.

SUMMARY STEPS

1. **show file** [*filesystem*:[//*module*/]][*directory*/]*filename* {**cksum** | **md5sum**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show file** [*filesystem*:[//*module*/]][*directory*/]*filename* {**cksum** | **md5sum**} **Example:** `switch# show file bootflash:trunks2.cfg cksum`	Displays the checksum or MD5 checksum of the file.

Compressing and Uncompressing Files

You can compress and uncompress files on your Cisco NX-OS device using Lempel-Ziv 1977 (LZ77) coding.

SUMMARY STEPS

1. (Optional) **dir** [*filesystem*:[//*module*/]*directory*]]
2. **gzip** [*filesystem*:[//*module*/][*directory*/] | *directory*/]*filename*
3. **gunzip** [*filesystem*:[//*module*/][*directory*/] | *directory*/]*filename* **.gz**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir** [*filesystem*:[//*module*/]*directory*]] **Example:** `switch# dir bootflash:`	(Optional) Displays the contents of the current directory. The file system and directory name are case sensitive.
Step 2	**gzip** [*filesystem*:[//*module*/][*directory*/] | *directory*/]*filename* **Example:** `switch# gzip show_tech`	Compresses a file. After the file is compressed, it has a .gz suffix.
Step 3	**gunzip** [*filesystem*:[//*module*/][*directory*/] | *directory*/]*filename* **.gz** **Example:** `switch# gunzip show_tech.gz`	Uncompresses a file. The file to uncompress must have the .gz suffix. After the file is uncompressed, it does not have the .gz suffix.

Displaying the Last Lines in a File

You can display the last lines of a file.

SUMMARY STEPS

1. **tail** [*filesystem*:[//*module*/]][*directory*/]*filename* [*lines*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**tail** [*filesystem*:[//*module*/]][*directory*/]*filename* [*lines*] **Example:** `switch# tail ospf-gr.conf`	Displays the last lines of a file. The default number of lines is 10. The range is from 0 to 80 lines.

Redirecting show Command Output to a File

You can redirect **show** command output to a file on bootflash:, slot0:, volatile:, or on a remote server.

SUMMARY STEPS

1. *show-command* > [*filesystem*:[//*module*/][*directory*] | [directory /]]*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	*show-command* **>** [*filesystem*:[//*module*/][*directory*] | [directory /]]*filename* **Example:** `switch# show tech-support > bootflash:techinfo`	Redirects the output from a **show** command to a file.

Finding Files

You can find the files in the current working directory and its subdirectories that have names that begin with a specific character string.

SUMMARY STEPS

1. (Optional) **pwd**
2. (Optional) **cd** {*filesystem*:[//*module*/][*directory*] | *directory*}
3. **find** *filename-prefix*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**pwd** **Example:** `switch# pwd`	(Optional) Displays the name of your current default directory.
Step 2	**cd** {*filesystem*:[//*module*/][*directory*] | *directory*} **Example:** `switch# cd bootflash:test_scripts`	(Optional) Changes the default directory.
Step 3	**find** *filename-prefix* **Example:** `switch# find bgp_script`	Finds all filenames in the default directory and in its subdirectories beginning with the filename prefix. The filename prefix is case sensitive.

Working with Archive Files

The Cisco NX-OS software supports archive files. You can create an archive file, append files to an existing archive file, extract files from an archive file, and list the files in an archive file.

Creating an Archive Files

You can create an archive file and add files to it. You can specify the following compression types:

- bzip2
- gzip
- Uncompressed

The default is gzip.

SUMMARY STEPS

1. **tar create** {**bootflash:** | **volatile:**}*archive-filename* [**absolute**] [**bz2-compress**] [**gz-compress**] [**remove**] [**uncompressed**] [**verbose**] *filename-list*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**tar create** {**bootflash:** | **volatile:**}*archive-filename* [**absolute**] [**bz2-compress**] [**gz-compress**] [**remove**] [**uncompressed**] [**verbose**] *filename-list*	Creates an archive file and adds files to it. The filename is alphanumeric, not case sensitive, and has a maximum length of 240 characters. The **absolute** keyword specifies that the leading backslash characters (\) should not be removed from the names of the files added to the archive file. By default, the leading backslash characters are removed. The **bz2-compress**, **gz-compress**, and **uncompressed** keywords determine the compression utility used when files are added, or later appended, to the archive and the decompression utility to use when extracting the files. If you do not specify an extension for the archive file, the defaults are as follows: • For **bz2-compress**, the extension is .tar.bz2. • For **gz-compress**, the extension is .tar.gz. • For **uncompressed**, the extension is .tar. The **remove** keyword specifies that the Cisco NX-OS software should delete the files from the file system after adding them to the archive. By default, the files are not deleted. The **verbose** keyword specifies that the Cisco NX-OS software should list the files as they are added to the archive. By default, the files are listed as they are added.

This example shows how to create a gzip compressed archive file:

```
switch# tar create bootflash:config-archive gz-compress bootflash:config-file
```

Appending Files to an Archive File

You can append files to an existing archive file on your Cisco NX-OS device.

Before You Begin

You have created an archive file on your Cisco NX-OS device.

SUMMARY STEPS

1. **tar append** {**bootflash:** | **volatile:**}*archive-filename* [**absolute**] [**remove**] [**verbose**] *filename-list*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**tar append** {**bootflash:** | **volatile:**}*archive-filename* [**absolute**] [**remove**] [**verbose**] *filename-list*	Adds files to an existing archive file. The archive filename is not case sensitive. The **absolute** keyword specifies that the leading backslash characters (\) should not be removed from the names of the files added to the archive file. By default, the leading backslash characters are removed. The **remove** keyword specifies that the Cisco NX-OS software should delete the files from the filesystem after adding them to the archive. By default, the files are not deleted. The **verbose** keyword specifies that the Cisco NX-OS software should list the files as they are added to the archive. By default, the files are listed as they are added.

This example shows how to append a file to an existing archive file:

```
switch# tar append bootflash:config-archive.tar.gz bootflash:new-config
```

Extracting Files from an Archive File

You can extract files to an existing archive file on your Cisco NX-OS device.

Before You Begin

You have created an archive file on your Cisco NX-OS device.

SUMMARY STEPS

1. **tar extract** {**bootflash:** | **volatile:**}*archive-filename* [**keep-old**] [**screen**] [**to** {**bootflash:** | **volatile:**}[*/directory-name*]] [**verbose**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**tar extract** {**bootflash:** | **volatile:**}*archive-filename* [**keep-old**] [**screen**] [**to** {**bootflash:** | **volatile:**}[*/directory-name*]] [**verbose**]	Extracts files from an existing archive file. The archive filename is not case sensitive. The **keep-old** keyword indicates that the Cisco NX-OS software should not overwrite files with the same name as the files being extracted. The **screen** keyword specifies that the Cisco NX-OS software should display the contents of the extracted files to the terminal screen. The **to** keyword specifies the target file system. You can include a directory name. The directory name is alphanumeric, case sensitive, and has a maximum length of 240 characters. The **verbose** keyword specifies that the Cisco NX-OS software should display the names of the files as they are extracted.

This example shows how to extract files from an existing archive file:

```
switch# tar extract bootflash:config-archive.tar.gz
```

Displaying the Filenames in an Archive File

You can display the names of the files in an archive files using the **tar list** command.

tar list {**bootflash:** | **volatile:**}*archive-filename*

The archive filename is not case sensitive.

```
switch# tar list bootflash:config-archive.tar.gz
config-file
new-config
```

Examples of Using the File System

This section includes example of using the file system on the Cisco NX-OS device.

Accessing Directories on Standby Supervisor Modules

This example shows how to list the files on the standby supervisor module:

```
switch# dir bootflash://sup-remote
   12198912     Aug 27 16:29:18 2003  m9500-sf1ek9-kickstart-mzg.1.3.0.39a.bin
    1864931     Apr 29 12:41:59 2003  dplug2
      12288     Apr 18 20:23:11 2003  lost+found/
   12097024     Nov 21 16:34:18 2003  m9500-sf1ek9-kickstart-mz.1.3.1.1.bin
   41574014     Nov 21 16:34:47 2003  m9500-sf1ek9-mz.1.3.1.1.bin

Usage for bootflash://sup-remote
   67747169 bytes used
```

```
  116812447 bytes free
  184559616 bytes total
```

This example shows how to delete a file on the standby supervisor module:

```
switch# delete bootflash://sup-remote/aOldConfig.txt
```

Moving Files

This example shows how to move a file on an external flash device:

```
switch# move slot0:samplefile slot0:mystorage/samplefile
```

This example shows how to move a file in the default file system:

```
switch# move samplefile mystorage/samplefile
```

Copying Files

This example shows how to copy the file called samplefile from the root directory of the slot0: file system to the mystorage directory:

```
switch# copy slot0:samplefile slot0:mystorage/samplefile
```

This example shows how to copy a file from the current directory level:

```
switch# copy samplefile mystorage/samplefile
```

This example shows how to copy a file from the active supervisor module bootflash to the standby supervisor module bootflash:

```
switch# copy bootflash:system_image bootflash://sup-2/system_image
```

You can also use the **copy** command to upload and download files from the slot0: or bootflash: file system to or from a FTP, TFTP, SFTP, or SCP server.

Deleting a Directory

You can remove directories from the file systems on your device.

Before You Begin

Ensure that the directory is empty before you try to delete it.

SUMMARY STEPS

1. (Optional) **pwd**
2. (Optional) **dir** [*filesystem* **:**[*//module/*][*directory*]]
3. **rmdir** [*filesystem* **:**[*//module/*]]*directory*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**pwd** **Example:** `switch# pwd`	(Optional) Displays the name of your current default directory.
Step 2	**dir** [*filesystem* **:**[*//module/*][*directory*]] **Example:** `switch# dir bootflash:test`	(Optional) Displays the contents of the current directory. The file system, module, and directory names are case sensitive. If the directory is not empty, you must delete all the files before you can delete the directory.
Step 3	**rmdir** [*filesystem* **:**[*//module/*]]*directory* **Example:** `switch# rmdir test`	Deletes a directory. The file system and directory name are case sensitive.

Displaying File Contents

This example shows how to display the contents of a file on an external flash device:

```
switch# show file slot0:test
configure terminal
interface ethernet 1/1
no shutdown
end
show interface ethernet 1/1
```

This example shows how to display the contents of a file that resides in the current directory:

```
switch# show file myfile
```

Displaying File Checksums

This example shows how to display the checksum of a file:

```
switch# show file bootflash:trunks2.cfg cksum
583547619
```

This example shows how to display the MD5 checksum of a file:

```
switch# show file bootflash:trunks2.cfg md5sum
3b94707198aabefcf46459de10c9281c
```

Compressing and Uncompressing Files

This example shows how to compress a file:

```
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
...
switch# gzip volatile:Samplefile
switch# dir
     266069     Jul 04 00:51:03 2003 Samplefile.gz
...
```

This example shows how to uncompress a compressed file:

```
switch# dir
     266069     Jul 04 00:51:03 2003 Samplefile.gz
...
switch# gunzip samplefile
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
...
```

Redirecting show Command Output

This example shows how to direct the output to a file on the bootflash: file system:

```
switch# show interface > bootflash:switch1-intf.cfg
```

This example shows how to direct the output to a file on external flash memory:

```
switch# show interface > slot0:switch-intf.cfg
```

This example shows how to direct the output to a file on a TFTP server:

```
switch# show interface > tftp://10.10.1.1/home/configs/switch-intf.cfg
Preparing to copy...done
```

This example shows how to direct the output of the **show tech-support** command to a file:

```
switch# show tech-support > Samplefile
Building Configuration ...
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
```

Finding Files

This example shows how to find a file in the current default directory:

```
switch# find smm_shm.cfg
/usr/bin/find: ./lost+found: Permission denied
./smm_shm.cfg
```

```
./newer-fs/isan/etc/routing-sw/smm_shm.cfg
./newer-fs/isan/etc/smm_shm.cfg
```

Default Settings for File System Parameters

This table lists the default settings for the file system parameters.

Table 18: Default File System Settings

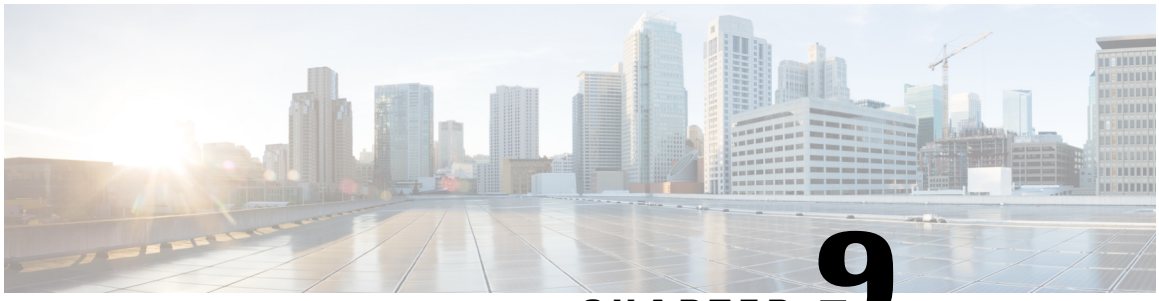
Parameters	Default
Default filesystem	bootflash:

Additional References for File Systems

This section includes additional information related to the file systems.

Related Documents for File Systems

Related Topic	Document Title
Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*



CHAPTER 9

Working with Configuration Files

This chapter contains the following sections:

- Information About Configuration Files, page 123
- Licensing Requirements for Configuration Files, page 124
- Managing Configuration Files, page 124
- Verifying the Device Configuration, page 136
- Examples of Working with Configuration Files, page 136
- Additional References for Configuration Files, page 137

Information About Configuration Files

Configuration files contain the Cisco NX-OS software commands used to configure the features on a Cisco NX-OS device. Commands are parsed (translated and executed) by the Cisco NX-OS software when the system is booted (from the startup-config file) or when you enter commands at the CLI in a configuration mode.

To change the startup configuration file, you can either save the running-configuration file to the startup configuration using the **copy running-config startup-config** command or copy a configuration file from a file server to the startup configuration.

Types of Configuration Files

The Cisco NX-OS software has two types of configuration files, running configuration and startup configuration. The device uses the startup configuration (startup-config) during device startup to configure the software features. The running configuration (running-config) contains the current changes that you make to the startup-configuration file. The two configuration files can be different. You might want to change the device configuration for a short time period rather than permanently. In this case, you would change the running configuration by using commands in global configuration mode but not save the changes to the startup configuration.

To change the running configuration, use the **configure terminal** command to enter global configuration mode. As you use the Cisco NX-OS configuration modes, commands generally are executed immediately

and are saved to the running configuration file either immediately after you enter them or when you exit a configuration mode.

To change the startup-configuration file, you can either save the running configuration file to the startup configuration or download a configuration file from a file server to the startup configuration.

Related Topics

Saving the Running Configuration to the Startup Configuration, on page 124

Downloading the Startup Configuration From a Remote Server, on page 127

Licensing Requirements for Configuration Files

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Configuration files require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Managing Configuration Files

This section describes how to manage configuration files.

Saving the Running Configuration to the Startup Configuration

You can save the running configuration to the startup configuration to save your changes for the next time you that reload the device.

SUMMARY STEPS

1. (Optional) **show running-config**
2. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show running-config** **Example:** `switch# show running-config`	(Optional) Displays the running configuration.

	Command or Action	Purpose
Step 2	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Copying a Configuration File to a Remote Server

You can copy a configuration file stored in the internal memory to a remote server as a backup or to use for configuring other Cisco NX-OS devices.

SUMMARY STEPS

1. **copy running-config** *scheme*:*//server/*[*url /*]*filename*
2. **copy startup-config** *scheme*:*//server/*[*url /*]*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**copy running-config** *scheme*:*//server/*[*url /*]*filename* **Example:** `switch# copy running-config tftp://10.10.1.1/sw1-run-config.bak`	Copies the running-configuration file to a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.
Step 2	**copy startup-config** *scheme*:*//server/*[*url /*]*filename* **Example:** `switch# copy startup-config tftp://10.10.1.1/sw1-start-config.bak`	Copies the startup-configuration file to a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.

This example shows how to copy the bootflash file using FTP:

```
switch# copy ftp: bootflash:
Enter source filename: n5000-uk9-kickstart.5.0.2.N2.1.bin
Warning: There is already a file existing with this name. Do you want to
overwrite (y/n)?[n] y
Enter vrf (If no input, current vrf 'default' is considered): management
Enter hostname for the ftp server: 172.1.1.10
Enter username: xxx
Password:
***** Transfer of file Completed Successfully *****
Note: Boot variable kickstart is set to
bootflash:/n5000-uk9-kickstart.5.0.2.N2.1.bin
```

This example shows how to copy the bootflash file using FTP:

```
switch# copy ftp: bootflash:
Enter source filename: n5500-uk9-kickstart.5.0.2.N2.1.bin
Warning: There is already a file existing with this name. Do you want to
overwrite (y/n)?[n] y
Enter vrf (If no input, current vrf 'default' is considered): management
Enter hostname for the ftp server: 172.1.1.10
Enter username: xxx
Password:
***** Transfer of file Completed Successfully *****
Note: Boot variable kickstart is set to
bootflash:/n5500-uk9-kickstart.5.0.2.N2.1.bin
```

Downloading the Running Configuration From a Remote Server

You can configure your Cisco NX-OS device by using configuration files that you created on another Cisco NX-OS device and uploaded to a remote server. You then download the file from the remote server to your device using TFTP, FTP, Secure Copy (SCP), or Secure Shell FTP (SFTP) to the running configuration.

Before You Begin

Ensure that the configuration file that you want to download is in the correct directory on the remote server.

Ensure that the permissions on the file are set correctly. Permissions on the file should be set to world-read.

Ensure that your Cisco NX-OS device has a route to the remote server. The Cisco NX-OS device and the remote server must be in the same subnetwork if you do not have a router or a default gateway to route traffic between subnets.

Check connectivity to the remote server using the **ping** or **ping6** command.

SUMMARY STEPS

1. **copy** *scheme***:**//*server*/[*url*/]*filename* **running-config**
2. (Optional) **show running-config**
3. (Optional) **copy running-config startup-config**
4. (Optional) **show startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**copy** *scheme***:**//*server*/[*url*/]*filename* **running-config** **Example:** `switch# copy tftp://10.10.1.1/my-config running-config`	Downloads the running-configuration file from a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.
Step 2	**show running-config** **Example:** `switch# show running-config`	(Optional) Displays the running configuration.

	Command or Action	Purpose
Step 3	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.
Step 4	**show startup-config** **Example:** `switch# show startup-config`	(Optional) Displays the startup configuration.

Related Topics

Copying Files, on page 119

Downloading the Startup Configuration From a Remote Server

You can configure your Cisco NX-OS device by using configuration files that you created on another Cisco NX-OS device and uploaded to a remote server. You then download the file from the remote server to your device using TFTP, FTP, Secure Copy (SCP), or Secure Shell FTP (SFTP) to the startup configuration.

Caution This procedure disrupts all traffic on the Cisco NX-OS device.

Before You Begin

Log in to a session on the console port.

Ensure that the configuration file that you want to download is in the correct directory on the remote server.

Ensure that the permissions on the file are set correctly. Permissions on the file should be set to world-read.

Ensure that your Cisco NX-OS device has a route to the remote server. The Cisco NX-OS device and the remote server must be in the same subnetwork if you do not have a router or a default gateway to route traffic between subnets.

Check connectivity to the remote server using the **ping** or **ping6** command.

SUMMARY STEPS

1. **write erase**
2. **reload**
3. **copy** *scheme*:*//server/*[*url /*]*filename* **running-config**
4. **copy running-config startup-config**
5. (Optional) **show startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**write erase** **Example:** `switch# write erase`	Erases the startup configuration file.

Step 2	**reload**
	
	Example:
	`switch# reload`
	`This command will reboot the system. (y/n)?`
	`[n] y`
	`...`
	`Enter the password for "admin": <password>`
	`Confirm the password for "admin": <password>`
	`...`
	`Would you like to enter the basic configuration`
	
	`dialog (yes/no): n`
	`switch#`
		Reloads the Cisco NX-OS device.
		Note Do not use the setup utility to configure the device.

Step 3	**copy** *scheme*:*//server/*[*url /*]*filename* **running-config** **Example:** `switch# copy tftp://10.10.1.1/my-config running-config`	Downloads the running configuration file from a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.
Step 4	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Saves the running configuration file to the startup configuration file.
Step 5	**show startup-config** **Example:** `switch# show startup-config`	(Optional) Displays the running configuration.

Related Topics

Copying Files, on page 119

Copying Configuration Files to an External Flash Memory Device

You can copy configuration files to an external flash memory device as a backup for later use.

Before You Begin

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

SUMMARY STEPS

1. (Optional) **dir** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]
2. **copy running-config** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]*filename*
3. **copy startup-config** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir** {**slot0:** | **usb1:** | **usb2:**}[*directory/*] **Example:** `switch# dir slot0:`	(Optional) Displays the files on the external flash memory device.
Step 2	**copy running-config** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]*filename* **Example:** `switch# copy running-config slot0:dsn-running-config.cfg`	Copies the running configuration to an external flash memory device. The *filename* argument is case sensitive.
Step 3	**copy startup-config** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]*filename* **Example:** `switch# copy startup-config slot0:dsn-startup-config.cfg`	Copies the startup configuration to an external flash memory device. The *filename* argument is case sensitive.

Related Topics

Copying Files, on page 119

Copying the Running Configuration from an External Flash Memory Device

You can configure your Cisco NX-OS device by copying configuration files created on another Cisco NX-OS device and saved to an external flash memory device.

Before You Begin

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

SUMMARY STEPS

1. (Optional) **dir** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]
2. **copy** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]*filename* **running-config**
3. (Optional) **show running-config**
4. (Optional) **copy running-config startup-config**
5. (Optional) **show startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir** {**slot0:** | **usb1:** | **usb2:**}[*directory/*] **Example:** `switch# dir slot0:`	(Optional) Displays the files on the external flash memory device.
Step 2	**copy** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]*filename* **running-config** **Example:** `switch# copy slot0:dsn-config.cfg running-config`	Copies the running configuration from an external flash memory device. The *filename* argument is case sensitive.
Step 3	**show running-config** **Example:** `switch# show running-config`	(Optional) Displays the running configuration.
Step 4	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.
Step 5	**show startup-config** **Example:** `switch# show startup-config`	(Optional) Displays the startup configuration.

Related Topics

Copying Files, on page 119

Copying the Startup Configuration from an External Flash Memory Device

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

Before You Begin

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

SUMMARY STEPS

1. (Optional) **dir** {**slot0:** | **usb1:** | **usb2:**}[*directory/*]
2. **copy** {**slot0:** | **usb1:** | **usb2:**}[*directory /*]*filename* **startup-config**
3. (Optional) **show startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir** {**slot0:** | **usb1:** | **usb2:**}[*directory/*] **Example:** `switch# dir slot0:`	(Optional) Displays the files on the external flash memory device.
Step 2	**copy** {**slot0:** | **usb1:** | **usb2:**}[*directory /*]*filename* **startup-config** **Example:** `switch# copy slot0:dsn-config.cfg startup-config`	Copies the startup configuration from an external flash memory device. The *filename* argument is case sensitive.
Step 3	**show startup-config** **Example:** `switch# show startup-config`	(Optional) Displays the startup configuration.

Related Topics

Copying Files, on page 119

Copying Configuration Files to an Internal File System

You can copy configuration files to the internal memory as a backup for later use.

SUMMARY STEPS

1. **copy running-config** [*filesystem***:**][*directory/*] | [*directory/*]*filename*
2. **copy startup-config** [*filesystem***:**][*directory/*] | [*directory/*]*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**copy running-config** [*filesystem***:**][*directory/*] | [*directory/*]*filename*	Copies the running-configuration file to internal memory. The *filesystem*, *directory*, and *filename* arguments are case sensitive.

	Command or Action	Purpose
	Example: `switch# copy running-config bootflash:sw1-run-config.bak`	
Step 2	**copy startup-config** [*filesystem***:**][*directory/*] | [*directory/*]*filename* **Example:** `switch# copy startup-config bootflash:sw1-start-config.bak`	Copies the startup-configuration file to internal memory. The *filesystem*, *directory*, and *filename* arguments are case sensitive.

Related Topics

Copying Files, on page 111

Rolling Back to a Previous Configuration

Problems, such as memory corruption, can occur that make it necessary for you to recover your configuration from a backed up version.

Note Each time that you enter a **copy running-config startup-config** command, a binary file is created and the ASCII file is updated. A valid binary configuration file reduces the overall boot time significantly. A binary file cannot be uploaded, but its contents can be used to overwrite the existing startup configuration. The **write erase** command clears the binary file.

SUMMARY STEPS

1. **write erase**
2. **reload**
3. **copy** *configuration_file* **running-configuration**
4. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**write erase** **Example:** `switch# write erase`	Clears the current configuration of the switch.

	Command or Action	Purpose
Step 2	**reload** **Example:** `switch# reload`	Restarts the device. You will be prompted to provide a kickstart and system image file for the device to boot and run. **Note** By default, the **reload** command reloads the device from a binary version of the startup configuration. Beginning with Cisco NX-OS 6.2(2), you can use the **reload ascii** command to copy an ASCII version of the configuration to the start up configuration when reloading the device.
Step 3	**copy** *configuration_file* **running-configuration** **Example:** `switch# copy bootflash:start-config.bak running-configuration`	Copies a previously saved configuration file to the running configuration. **Note** The *configuration_file* filename argument is case sensitive.
Step 4	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the start-up configuration.

Removing the Configuration for a Missing Module

When you remove an I/O module from the chassis, you can also remove the configuration for that module from the running configuration.

Note You can only remove the configuration for an empty slot in the chassis.

Before You Begin

Remove the I/O module from the chassis.

SUMMARY STEPS

1. (Optional) **show hardware**
2. **purge module** *slot* **running-config**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show hardware** **Example:** `switch# show hardware`	(Optional) Displays the installed hardware for the device.
Step 2	**purge module** *slot* **running-config** **Example:** `switch# purge module 3 running-config`	Removes the configuration for a missing module from the running configuration.
Step 3	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Erasing a Configuration

You can erase the configuration on your device to return to the factory defaults.

You can erase the following configuration files saved in the persistent memory on the device:

- Startup
- Boot
- Debug

Note The **write erase** command erases the entire startup configuration, except for the following:

- Boot variable definitions
- The IPv4 configuration on the mgmt0 interface, including the following:
  - Address
  - Subnet mask

To remove the boot variable definitions and the IPv4 configuration on the mgmt0 interface, use the **write erase boot** command.

SUMMARY STEPS

1. **write erase** [**boot** | **debug**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**write erase** [**boot** | **debug**]
	
	Example:
	`switch# write erase`
	`Warning: This command will erase the startup-configuration.`
	`Do you wish to proceed anyway? (y/n) [n]`
	`y`
		Erases configurations in persistent memory. The default action erases the startup configuration.
		The **boot** option erases the boot variable definitions and the IPv4 configuration on the mgmt0 interface.
		The **debug** option erases the debugging configuration.
		Note The running configuration file is not affected by this command.

Clearing Inactive Configurations

You can clear inactive Quality of Service (QoS) and/or access control list (ACL) configurations.

SUMMARY STEPS

1. (Optional) **show running-config** *type* **inactive-if-config**
2. **clear inactive-config** *policy*
3. (Optional) **show inactive-if-config log**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show running-config** *type* **inactive-if-config** **Example:** `# show running-config ipqos inactive-if-config`	(Optional) Displays any inactive ACL or QoS configurations. The values for the *type* argument are **aclmgr** and **ipqos**. • **aclmgr—** Displays any inactive configurations for aclmgr. • **ipqos—**Displays any inactive configurations for qosmgr.

Step 2	**clear inactive-config** *policy*
	
	Example:
	`# clear inactive-config qos`
	`clear qos inactive config`
	`Inactive if config for QoS manager is saved at/bootflash/qos_inactive_if_config.cfg`
	`for vdc default & for other than default vdc: /bootflash/vdc_x/qos_inactive_if_config.cfg`
	`(where x is vdc number)`
		Clears inactive configurations.
		The values for the *policy* argument are **qos** and **acl**.
		The following describes the values:
		• **qos—**Clears inactive QoS configurations.
		• **acl—** Clears inactive ACL configurations.
		• **acl qos—**Clears inactive ACL configurations and inactive QoS configurations.

	Command or Action	Purpose
	`you can see the log file @ show inactive-if-config log`	
Step 3	**show inactive-if-config log** **Example:** `# show inactive-if-config log`	(Optional) Displays the commands that were used to clear the inactive configurations.

Verifying the Device Configuration

To verify the configuration after bootstrapping the device using POAP, use one of the following commands:

Command	Purpose
show running-config	Displays the running configuration.
show startup-config	Displays the startup configuration.

For detailed information about the fields in the output from these commands, see the Cisco Nexus command reference for your device.

Examples of Working with Configuration Files

This section includes examples of working with configuration files.

Copying Configuration Files

This example shows how to copy a running configuration to the bootflash: file system:

Backing Up Configuration Files

This example shows how to back up the startup configuration to the bootflash: file system (ASCII file):

```
switch# copy startup-config bootflash:my-config
```

This example shows how to back up the startup configuration to the TFTP server (ASCII file):

```
switch# copy startup-config tftp://172.16.10.100/my-config
```

This example shows how to back up the running configuration to the bootflash: file system (ASCII file):

```
switch# copy running-config bootflash:my-config
```

Rolling Back to a Previous Configuration

To roll back your configuration to a snapshot copy of a previously saved configuration, you need to perform the following steps:

1. Clear the current running image with the **write erase** command.
2. Restart the device with the **reload** command.

Note By default, the **reload** command reloads the device from a binary version of the startup configuration.

Beginning with Cisco NX-OS 6.2(2), you can use the **reload ascii** command to copy an ASCII version of the configuration to the start up configuration when reloading the device.

3. Copy the previously saved configuration file to the running configuration with the **copy** *configuration_file* **running-configuration** command.
4. Copy the running configuration to the start-up configuration with the **copy running-config startup-config** command.

Additional References for Configuration Files

This section includes additional information related to managing configuration files.

Related Documents for Configuration Files

Related Topic	Document Title
Licensing	*Cisco NX-OS Licensing Guide*
Command reference	

INDEX

--More-- prompt 68
  filtering output 68
  searching output 68

A

aliases, See command aliases
archive files 116, 117, 118
  appending files 117
  creating 116
  displaying the contents to the screen 117
  extracting files 117
  listing archived filenames 118

B

banners, See EXEC banners
basic device management 95
  licensing 95
BIOS 73
  loader> prompt 73
boot variables 134
  erasing configuration 134

C

characters 49
  special 49
CLI 44, 52, 69, 70, 71, 73
  command history 69
  command modes 44
  command name completion 52
  command prompt 44
  configuring the edit mode 70
  disabling confirmation prompts 71
  enabling confirmation prompts 71
  examples 73
  setting display colors 71
CLI history 70
  controlling command recall 70
CLI prompt 44
  description 44
CLI variables 54, 55, 73, 74
  characteristics 54
  description 54
  examples 73
  persistent 55
  referencing 54
  session-only 55
  system-defined variables 74
clocks 94, 101, 104
  clock manager 94
  default settings 104
  description 94
  setting clock manager 101
  setting manually 101
COM1 port 78
  settings 78
COM1 ports 81, 85
  configuring settings 81
  enabling modem connections 85
command aliases 56, 57, 58, 73
  characteristics 56
  defining 57
  description 56
  examples 73
  user session only 58
command history 69, 70
  description 69
  displaying 70
command modes 44, 45, 46, 47, 48
  description 44
  EXEC 45
  exiting 47
  global configuration 45
  interface 45
  restoring 47
  saving 47
  subinterface 46
  summary (table) 48

command scripts 58, 59, 60, 74
delaying command actions 60
description 58
echoing text to terminals 59
examples 74
commands 52, 53, 69
abbreviations 52
no form 53
recalling 69
commands scripts 58
running 58
configuration 41, 103, 136
displaying 41, 103, 136
configuration files 123, 124, 125, 128, 131, 132, 134, 135, 136, 137
clear inactive-config 135
copying from remote servers 125
copying to external memory 128
copying to internal file systems 131
description 123
erasing 134
example backup 136
example copy 136
example roll back 137
licensing 124
rolling back to previous configurations 132
types 123
configuration prompts 71
disabing 71
enabing 71
configuring devices 31, 32, 33, 35, 37, 38, 40
POAP process 33, 35, 37, 38
DHCP phase 35
post-installation reload phase 38
power up phase 35
script execution phase 37
using POAP 31, 32, 40
console ports 78, 79, 85
configuring settings 79
enabling modem connections 85
settings 78
context-sensitive help 60
syntax checking 60

D

daylight savings time, See summer time
default settings 91, 104, 122
clocks 104
file systems 91, 122
MOTD banners 104
Telnet servers 104
default users 21
description 21
diff utility 65
description 65
directories 106, 107, 108, 109
changing current directories 107
creating 108
description 106
displaying contents 109
displaying current directory 107
licensing requirements 107
working with 107

E

egrep utility 66
filtering show command output 66
searching show command output 66
examples 118, 119, 120, 121, 136, 137
accessing directories on standby supervisor modules 118
backing up configuration files 136
compressing files 121
copying configuration files 136
copying files 119
displaying file checksums 120
displaying file contents 120
finding files 121
moving files 119
redirecting show command output 121
rolling back to a previous configuration 137
uncompressing files 121
EXEC banner 97
configuring 97
EXEC banners 94
See also EXEC banners
description 94
See also EXEC banners
EXEC command mode 45
description 45

F

FCoE 3
Fibre Channel over Ethernet 3
file systems 91, 105, 107, 110, 122
accessing standby supervisor modules 110
changing current directories 107
default settings 91, 122
description 105
licensing requirements 107
specifying 105

files 106, 107, 110, 111, 112, 113, 114, 115, 119, 120, 121
compressing 113
compressing, examples 121
copying 111
copying, examples 119
deleting 112
description 106
displaying checksums 113
displaying contents 112
displaying files checksums, examples 120
displaying files contents, examples 120
displaying last lines 114
finding 115
finding, example 121
licensing requirements 107
moving 110
moving, examples 119
redirecting command output 114
renaming 110
tar files 115
uncompressing 113
uncompressing, examples 121
files systems 107
displaying current directory 107
filtering 63, 64, 65, 66, 67, 68
--More-- prompt 68
diff utility 65
egrep utility 66
grep utility 66
keywords 64
less utility 67
sed utility 67
show command output 63

G

global configuration command mode 45
description 45
global configuration mode 48
summary 48
grep utility 66
searching show command output 66
grep utility filtering show command output 66
guidelines and limitations 39
POAP 39

H

hostname 94, 95
configuring 95
description 94

I

IEEE 802.1p 3
IEEE 802.3x 3
Interface configuration command mode 45
description 45
interface configuration mode 48
summary 48

K

keystrokes 49
shortcuts 49

L

less utility 67
filtering show command output 67
searching show command output 67
licensing 79, 95, 107, 124
basic device management 95
configuration files 124
directories 107
file systems 107
files 107
terminal settings 79
loader> prompt 73
description 73

M

management access 26
description 26
management interfaces 27, 28, 29
displaying information 28
using force option during shutdown 29
message-of-the-day banners, See MOTD banners
mgmt0 interfaces 27
description 27
modems 85, 87, 88, 89
configuring connections 85
configuring user-specific initialization strings 88
downloading initialization string 87
enabling connections 85
initializing connection 89
modes, See command modes
modules 72, 133
removing configuration after removal 133
sending commands from the supervisor mdoule session 72

MOTD banner 96
configuring 96
MOTD banners 94, 104
default settings 104
description 94

P

passwords 21, 22
administrator 21
setting administrator default 22
POAP 31, 32, 33, 35, 38, 39, 40
configuration script 32
DHCP discovery phase 35
guidelines and limitations 39
post-installation reload phase 38
process 33
setting up the network environment 40
using to configure a switch 40
Power On Auto Provisioning 35
power up phase 35
provisioning devices 35
POAP process 35
power up phase 35
PowerOn Auto Provisioning 37
See also POAP
script execution phase 37
See also POAP
privileged EXEC mode 48
summary 48
prompts, See confirmation prompts
provisioning devices 31, 32, 33, 35, 37, 38
POAP process 33, 35, 37, 38
DHCP phase 35
post-installation reload phase 38
script execution phase 37
using POAP 31, 32

R

regular expressions 62, 63
anchoring 63
filtering CLI output 62
multiple-character patterns 62
special characters 62
running configuration 41, 103, 136
displaying 41, 103, 136
running configurations 124, 126, 129, 131, 132, 133, 136, 137
copying from external memory devices 129
copying to internal file systems 131
downloading from remote servers 126
running configurations *(continued)*
example backup 136
example copy 136
example roll back 137
removing configuration for missing modules 133
rolling back to previous configurations 132
saving to startup configurations 124

S

scripts, See command scripts
searching 63, 64, 65, 66, 67, 68
--More-- prompt 68
diff utility 65
egrep utility 66
grep utility 66
keywords 64
less utility 67
sed utility 67
show command output 63
sed utility 67
filtering show command output 67
searching show command output 67
shortcuts 49
keystrokes 49
show command output 121
redirecting, example 121
show commands 63
filtering output 63
searching output 63
sort utility 67
description 67
special characters 49
description 49
sscp 64
redirecting show command output 64
standby supervisor modules 110, 118
accessing directories, examples 118
accessing file systems 110
startup configuration 41, 103, 134, 136
displaying 41, 103, 136
erasing 134
startup configurations 124, 127, 130, 131, 132, 136, 137
copying from external memory devices 130
copying from running configurations 124
copying to internal file systems 131
downloading from remote servers 127
example backup 136
example copy 136
example roll back 137
rolling back to previous configurations 132

subinterface configuration command mode 46
description 46
subinterface configuration mode 48
summary 48
summer time 94, 99
configuring 99
description 94
switchname 95
See also hostname
configuring 95
See also hostname
syntax checking, See context-sensitive help

T

Telnet servers 104
default settings 104
terminal sessions 77, 90
clearing 90
displaying information 90
settings 77
terminal settings 79
licensing 79
time zones 94, 98
configuring 98
time zones *(continued)*
description 94

U

user sessions 95, 103
description 95
sending messages 103
users 102
managing 102
users sessions 102
displaying information 102

V

variables, See CLI variables
VDC 8
defined 8
virtual device contexts 8
virtual terminals 79, 83, 84
configuring 83
configuring session limits 84
settings 79