



Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 7.x

First Published: 2015-02-01

Last Modified: 2021-09-14

Americas Headquarters

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](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. (1721R)

© 2016–2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface	xi
Audience	xi
Document Conventions	xi
Related Documentation for Cisco Nexus 9000 Series Switches	xii
Documentation Feedback	xii
Communications, Services, and Additional Information	xii

CHAPTER 1

New and Changed Information	1
New and Changed Information	1

CHAPTER 2

Overview	3
Licensing Requirements	3
Supported Platforms	3
Software Image	3
Software Compatibility	4
Spine/Leaf Topology	4
Modular Software Design	4
Serviceability	4
Switched Port Analyzer	4
Ethanalyzer	5
Smart Call Home	5
Online Diagnostics	5
Embedded Event Manager	5
Manageability	5
Simple Network Management Protocol	5
Configuration Verification and Rollback	5

- Role-Based Access Control 6
- Cisco NX-OS Device Configuration Methods 6
- Programmability 6
 - Python API 6
 - Tcl 6
 - Cisco NX-API 7
 - Bash Shell 7
 - Broadcom Shell 7
- Traffic Routing, Forwarding, and Management 7
 - Ethernet Switching 7
 - IP Routing 8
 - IP Services 8
 - IP Multicast 8
- Quality of Service 9
- Network Security Features 9
- Supported Standards 10

CHAPTER 3

- Using the Cisco NX-OS Setup Utility 15**
 - About the Cisco NX-OS Setup Utility 15
 - Prerequisites for the Setup Utility 16
 - Setting Up Your Cisco NX-OS Device 17
 - Additional References for the Setup Utility 21
 - Related Documents for the Setup Utility 21

CHAPTER 4

- Using PowerOn Auto Provisioning 23**
 - About PowerOn Auto Provisioning 23
 - Network Requirements for POAP 23
 - POAP Configuration Script 24
 - Using the POAP Script and POAP Script Options 24
 - Setting up the DHCP Server without DNS for POAP 27
 - Downloading and Using User Data, Agents, and Scripts as part of POAP 28
 - POAP Process 28
 - Power-Up Phase 29
 - DHCP Discovery Phase 30

Script Execution Phase	32
Post-Installation Reload Phase	32
Guidelines and Limitations for POAP	32
Setting Up the Network Environment to Use POAP	33
Configuring a Switch Using POAP	34
Creating md5 Files	34
Verifying the Device Configuration	36
Troubleshooting for POAP	36
Managing the POAP Personality	37
POAP Personality	37
Backing Up the POAP Personality	37
Configuring the POAP Personality	38
Restoring the POAP Personality	39
POAP Personality Sample Script	40

CHAPTER 5

Understanding the Command-Line Interface	41
About the CLI Prompt	41
Command Modes	42
EXEC Command Mode	42
Global Configuration Command Mode	42
Interface Configuration Command Mode	43
Subinterface Configuration Command Mode	43
Saving and Restoring a Command Mode	44
Exiting a Configuration Command Mode	44
Command Mode Summary	45
Special Characters	46
Keystroke Shortcuts	46
Abbreviating Commands	49
Completing a Partial Command Name	49
Identifying Your Location in the Command Hierarchy	50
Using the no Form of a Command	50
Configuring CLI Variables	51
About CLI Variables	51
Configuring CLI Session-Only Variables	52

Configuring Persistent CLI Variables	52
Command Aliases	53
About Command Aliases	53
Defining Command Aliases	54
Configuring Command Aliases for a User Session	54
Command Scripts	55
Running a Command Script	55
Echoing Information to the Terminal	55
Delaying Command Action	56
Context-Sensitive Help	56
Understanding Regular Expressions	58
Special Characters	58
Multiple-Character Patterns	58
Anchoring	59
Searching and Filtering show Command Output	59
Filtering and Searching Keywords	60
diff Utility	61
grep and egrep Utilities	62
less Utility	62
Mini AWK Utility	62
sed Utility	63
sort Utility	63
Searching and Filtering from the --More-- Prompt	64
Using the Command History	65
Recalling a Command	65
Controlling CLI History Recall	65
Configuring the CLI Edit Mode	65
Displaying the Command History	66
Enabling or Disabling the CLI Confirmation Prompts	66
Setting CLI Display Colors	67
Sending Commands to Modules	67
Sending Command Output in Email	68
BIOS Loader Prompt	70
Examples Using the CLI	70

Using the System-Defined Timestamp Variable	70
Using CLI Session Variables	70
Defining Command Aliases	71
Running a Command Script	71
Sending Command Output in Email	72

CHAPTER 6**Configuring Terminal Settings and Sessions 75**

About Terminal Settings and Sessions	75
Terminal Session Settings	75
Console Port	75
Virtual Terminals	76
Default Settings for File System Parameters	76
Configuring the Console Port	76
Configuring Virtual Terminals	78
Configuring the Inactive Session Timeout	78
Configuring the Session Limit	78
Clearing Terminal Sessions	79
Displaying Terminal and Session Information	80

CHAPTER 7**Basic Device Management 81**

About Basic Device Management	81
Device Hostname	81
Message-of-the-Day Banner	81
Device Clock	81
Clock Manager	82
Time Zone and Summer Time (Daylight Saving Time)	82
User Sessions	82
Default Settings for Basic Device Parameters	82
Changing the Device Hostname	82
Configuring the MOTD Banner	83
Configuring the Time Zone	84
Configuring Summer Time (Daylight Saving Time)	85
Manually Setting the Device Clock	86
Setting the Clock Manager	86

Managing Users	87
Displaying Information about the User Sessions	87
Sending a Message to Users	87
Verifying the Device Configuration	88

CHAPTER 8**Using the Device File Systems, Directories, and Files 89**

About the Device File Systems, Directories, and Files	89
File Systems	89
Directories	90
Files	90
Default Settings for File System Parameters	91
Configuring the FTP, HTTP, or TFTP Source Interface	91
Working with Directories	91
Identifying the Current Directory	91
Changing the Current Directory	92
Creating a Directory	92
Displaying Directory Contents	93
Deleting a Directory	93
Accessing Directories on the Standby Supervisor Module	93
Working with Files	94
Moving Files	94
Copying Files	94
Deleting Files	95
Displaying File Contents	95
Displaying File Checksums	96
Compressing and Uncompressing Files	96
Displaying the Last Lines in a File	97
Redirecting show Command Output to a File	97
Finding Files	97
Formatting the Bootflash	98
Working with Archive Files	98
Creating an Archive File	98
Appending Files to an Archive File	99
Extracting Files from an Archive File	100

Displaying the Filenames in an Archive File	101
Examples of Using the File System	101
Accessing Directories on Standby Supervisor Modules	101
Moving Files	101
Copying Files	102
Deleting a Directory	102
Displaying File Contents	103
Displaying File Checksums	103
Compressing and Uncompressing Files	103
Redirecting show Command Output	104
Finding Files	104
<hr/>	
CHAPTER 9	Working with Configuration Files 105
About Configuration Files	105
Types of Configuration Files	105
Guidelines and Limitations for Configuration Files	106
Managing Configuration Files	106
Saving the Running Configuration to the Startup Configuration	106
Copying a Configuration File to a Remote Server	106
Downloading the Running Configuration From a Remote Server	107
Downloading the Startup Configuration From a Remote Server	108
Copying Configuration Files to an External Flash Memory Device	109
Copying the Running Configuration from an External Flash Memory Device	110
Copying the Startup Configuration From an External Flash Memory Device	111
Copying Configuration Files to an Internal File System	112
Rolling Back to a Previous Configuration	112
Removing the Configuration for a Missing Module	113
Erasing a Configuration	114
Clearing Inactive Configurations	114
Configuration Archive and Configuration Log	115
Information About Configuration Archive	115
Configuring the Characteristics of the Configuration Archive	115
Information About Configuration Log	117
Displaying Configuration Log Entries	118

Verifying the Device Configuration 119

Examples of Working with Configuration Files 119

- Copying Configuration Files 119
- Backing Up Configuration Files 119
- Rolling Back to a Previous Configuration 120



Preface

This preface includes the following sections:

- [Audience, on page xi](#)
- [Document Conventions, on page xi](#)
- [Related Documentation for Cisco Nexus 9000 Series Switches, on page xii](#)
- [Documentation Feedback, on page xii](#)
- [Communications, Services, and Additional Information, on page xii](#)

Audience

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

Document Conventions

Command descriptions use the following conventions:

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

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

Examples use the following conventions:

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

Related Documentation for Cisco Nexus 9000 Series Switches

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

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

Documentation Feedback

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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



CHAPTER 1

New and Changed Information

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

- [New and Changed Information, on page 1](#)

New and Changed Information

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

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

Feature	Description	Changed in Release	Where Documented
Erase Configuration	Added support for preserving the IPv6 address on mgmt 0 interface and the IPv6 Default Gateway in Management VRF after write erase, reload operation.	7.0(3)I7(7)	Erasing a Configuration, on page 114
Reload timer	Added support for reload timer command.	7.0(3)I7(4)	Guidelines and Limitations for Configuration Files, on page 106
POAP	Added support for RFC 3004 (User Class Option for DHCP).	7.0(3)I7(4)	Guidelines and Limitations for POAP, on page 32
POAP	Added support for POAP over IPv6.	7.0(3)I7(4)	Guidelines and Limitations for POAP, on page 32
POAP	Added POAP skip option.	7.0(3)I7(3)	Guidelines and Limitations for POAP, on page 32
POAP	Added procedure to re-create the md5 checksum files.	7.0(3)I6(1)	Creating md5 Files, on page 34

Feature	Description	Changed in Release	Where Documented
POAP	Introduced a single POAP script and the ability to start a service on boot across all Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.	7.0(3)I6(1)	Using PowerOn Auto Provisioning, on page 23
Support for Configuration Archive and Archive Log	Added support for configuration archive and archive log.	7.0(3)I5(1)	Configuration Archive and Configuration Log, on page 115
Command-line interface	Enabled Cisco NX-OS CLI variables to contain hyphens and underscores.	7.0(3)I4(1)	Configuring CLI Session-Only Variables, on page 52 and Configuring Persistent CLI Variables, on page 52
POAP	Introduced the POAP personality and dynamic breakout features.	7.0(3)I4(1)	Using PowerOn Auto Provisioning, on page 23
copy command	Added support for the HTTPS file system.	7.0(3)I1(1)	Copying Files, on page 94



CHAPTER 2

Overview

This chapter contains the following sections:

- [Licensing Requirements, on page 3](#)
- [Supported Platforms, on page 3](#)
- [Software Image, on page 3](#)
- [Software Compatibility, on page 4](#)
- [Serviceability, on page 4](#)
- [Manageability, on page 5](#)
- [Programmability, on page 6](#)
- [Traffic Routing, Forwarding, and Management, on page 7](#)
- [Quality of Service, on page 9](#)
- [Network Security Features, on page 9](#)
- [Supported Standards, on page 10](#)

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the [Cisco NX-OS Licensing Guide](#) and the [Cisco NX-OS Licensing Options Guide](#).

Supported Platforms

Starting with Cisco NX-OS release 7.0(3)I7(1), use the [Nexus Switch Platform Support Matrix](#) to know from which Cisco NX-OS releases various Cisco Nexus 9000 and 3000 switches support a selected feature.

Software Image

The Cisco NX-OS software consists of one NXOS software image. This image runs on all Cisco Nexus 3400 Series switches.

Software Compatibility

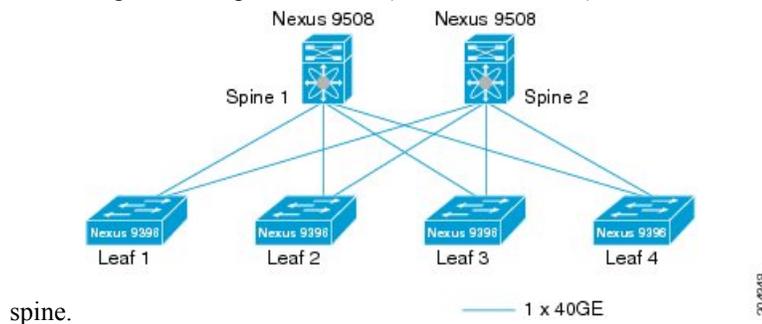
The Cisco NX-OS software interoperates with Cisco products that run any variant of the Cisco IOS software. The Cisco NX-OS software also interoperates with any networking operating system that conforms to the IEEE and RFC compliance standards.

Spine/Leaf Topology

The Cisco Nexus 9000 Series switches support a two-tier spine/leaf topology.

Figure 1: Spine/Leaf Topology

This figure shows an example of a spine/leaf topology with four leaf switches (Cisco Nexus 9396 or 93128) connecting into two spine switches (Cisco Nexus 9508) and two 40G Ethernet uplinks from each leaf to each



spine.

Modular Software Design

The Cisco NX-OS software supports distributed multithreaded processing on symmetric multiprocessors (SMPs), multi-core CPUs, and distributed data module processors. The Cisco NX-OS software offloads computationally intensive tasks, such as hardware table programming, to dedicated processors distributed across the data modules. The modular processes are created on demand, each in a separate protected memory space. Processes are started and system resources are allocated only when you enable a feature. A real-time preemptive scheduler helps to ensure the timely processing of critical functions.

Serviceability

The Cisco NX-OS software has serviceability functions that allow the device to respond to network trends and events. These features help you with network planning and improving response times.

Switched Port Analyzer

The Switched Port Analyzer (SPAN) feature allows you to analyze all traffic between ports (called the SPAN source ports) by nonintrusively directing the SPAN session traffic to a SPAN destination port that has an external analyzer attached to it. For more information about SPAN, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

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 analyze the control-plane traffic. For more information about Ethanalyzer, see the *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*.

Smart 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. It offers alert grouping capabilities and customizable destination profiles. You can use this feature, 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). For more information about Smart Call Home, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Online Diagnostics

Cisco generic online diagnostics (GOLD) 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. For information about configuring GOLD, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Embedded Event Manager

Cisco Embedded Event Manager (EEM) is a device and system management feature that helps you to customize behavior based on network events as they happen. For information about configuring EEM, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Manageability

This section describes the manageability features for the Cisco Nexus 9000 Series switches.

Simple Network Management Protocol

The Cisco NX-OS software is compliant with Simple Network Management Protocol (SNMP) version 1, version 2, and version 3. A large number of MIBs is supported. For more information about SNMP, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Configuration Verification and Rollback

The Cisco NX-OS software allows you to verify the consistency of a configuration and the availability of necessary hardware resources prior to committing the configuration. You can preconfigure a device and apply the verified configuration at a later time. Configurations also include checkpoints that allow you to roll back

to a known good configuration as needed. For more information about rollbacks, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Role-Based Access Control

With role-based access control (RBAC), you can limit access to device operations by assigning roles to users. You can customize access and restrict it to the users who require it. For more information about RBAC, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Cisco NX-OS Device Configuration Methods

You can use these methods to configure Cisco NX-OS devices:

- The CLI from a Secure Shell (SSH) session, a Telnet session, or the console port. SSH provides a secure connection to the device. The CLI configuration guides are organized by feature. For more information, see the Cisco NX-OS configuration guides. For more information about SSH and Telnet, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.
- The XML management interface, which is a programmatic method based on the NETCONF protocol that complements the CLI. For more information, see the *Cisco NX-OS XML Interface User Guide*.
- The Cisco Data Center Network Management (DCNM) client, which runs on your local PC and uses web services on the Cisco DCNM server. The Cisco DCNM server configures the device over the XML management interface. For more information about the Cisco DCNM client, see the *Cisco DCNM Fundamentals Guide*.

Programmability

This section describes the programmability features for the Cisco Nexus 9000 Series switches.

Python API

Python is an easy-to-learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming. Python's elegant syntax and dynamic typing, together with its interpreted nature, make it an ideal language for scripting and rapid application development in many areas on most platforms. The Python interpreter and the extensive standard library are freely available in source or binary form for all major platforms from the Python website: <http://www.python.org/>. The Python scripting capability gives programmatic access to the CLI to perform various tasks and Power-On Auto Provisioning (POAP) or Embedded Event Manager (EEM) actions. For more information about the Python API and Python scripting, see the *Cisco Nexus 9000 Series NX-OS Programmability Guide*.

Tcl

Tool Command Language (Tcl) is a scripting language. With Tcl, you gain more flexibility in your use of the CLI commands on the device. You can use Tcl to extract certain values in the output of a **show** command, perform switch configurations, run Cisco NX-OS commands in a loop, or define EEM policies in a script.

Cisco NX-API

The Cisco NX-API provides web-based programmatic access to the Cisco Nexus 9000 Series switches. This support is delivered through the NX-API open-source web server. The Cisco NX-API exposes the complete configuration and management capabilities of the command-line interface (CLI) through web-based APIs. You can configure the switch to publish the output of the API calls in either XML or JSON format. For more information about the Cisco NX-API, see the *Cisco Nexus 9000 Series NX-OS Programmability Guide*.



Note NX-API performs authentication through a programmable authentication module (PAM) on the switch. Use cookies to reduce the number of PAM authentications and thus reduce the load on PAM.

Bash Shell

The Cisco Nexus 9000 Series switches support direct Linux shell access. With Linux shell support, you can access the Linux system on the switch in order to use Linux commands and manage the underlying system. For more information about Bash shell support, see the *Cisco Nexus 9000 Series NX-OS Programmability Guide*.

Broadcom Shell

The Cisco Nexus 9000 Series switch front-panel and fabric module line cards contain several Broadcom ASICs. You can use the CLI to access the command-line shell (bcm shell) for these ASICs. The benefit of using this method to access the bcm shell is that you can use Cisco NX-OS command extensions such as **pipe include** and **redirect output to file** to manage the output. In addition, the activity is recorded in the system accounting log for audit purposes, unlike commands entered directly from the bcm shell, which are not recorded in the accounting log. For more information about Broadcom shell support, see the *Cisco Nexus 9000 Series NX-OS Programmability Guide*.



Caution Use Broadcom shell commands with caution and only under the direct supervision or request of Cisco Support personnel.

Traffic Routing, Forwarding, and Management

This section describes the traffic routing, forwarding, and management features supported by the Cisco NX-OS software.

Ethernet Switching

The Cisco NX-OS software supports high-density, high-performance Ethernet systems and provides 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
- Unidirectional Link Detection (UDLD) in aggressive and standard modes

For more information, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide* and the *Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*.

IP Routing

The Cisco NX-OS software supports IP version 4 (IPv4) and IP version 6 (IPv6) and the following routing protocols:

- Open Shortest Path First (OSPF) Protocol Versions 2 (IPv4) and 3 (IPv6)
- Intermediate System-to-Intermediate System (IS-IS) Protocol (IPv4 and IPv6)
- Border Gateway Protocol (BGP) (IPv4 and IPv6)
- Enhanced Interior Gateway Routing Protocol (EIGRP) (IPv4 only)
- Routing Information Protocol Version 2 (RIPv2) (IPv4 only)

The Cisco NX-OS software implementations of these protocols are fully compliant with the latest standards and include 4-byte autonomous system numbers (ASNs) and incremental shortest path first (SPF). All unicast protocols support Non-Stop Forwarding Graceful Restart (NSF-GR). All protocols support all interface types, including Ethernet interfaces, VLAN interfaces, subinterfaces, port channels, and loopback interfaces.

For more information, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

IP Services

The following IP services are available in the Cisco NX-OS software:

- Virtual routing and forwarding (VRF)
- Dynamic Host Configuration Protocol (DHCP) helper
- Hot Standby Router Protocol (HSRP)
- Enhanced object tracking
- Policy-based routing (PBR)
- Unicast graceful restart for all protocols in IPv4 unicast graceful restart for OPSFv3 in IPv6

For more information, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

IP Multicast

The Cisco NX-OS software includes the following multicast protocols and functions:

- Protocol Independent Multicast (PIM) Version 2 (PIMv2)
- PIM sparse mode (Any-Source Multicast [ASM] for IPv4)
- Anycast rendezvous point (Anycast-RP)

- Multicast NSF for IPv4
- RP-Discovery using bootstrap router (BSR) (Auto-RP and static)
- Internet Group Management Protocol (IGMP) Versions 1, 2, and 3 router role
- IGMPv2 host mode
- IGMP snooping
- Multicast Source Discovery Protocol (MSDP) (for IPv4)



Note The Cisco NX-OS software does not support PIM dense mode.

For more information, see the *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*.

Quality of Service

The Cisco NX-OS software supports quality of service (QoS) functions for classification, marking, queuing, policing, and scheduling. Modular QoS CLI (MQC) supports all QoS features. You can use MQC to provide uniform configurations across various Cisco platforms. For more information, see the *Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*.

Network Security Features

The Cisco NX-OS software includes the following security features:

- Control Plane Policing (CoPP)
- Message-digest algorithm 5 (MD5) routing protocol authentication
- Authentication, authorization, and accounting (AAA)
- RADIUS and TACACS+
- SSH Protocol Version 2
- SNMPv3
- Policies based on MAC and IPv4 addresses supported by named ACLs (port-based ACLs [PACLs], VLAN-based ACLs [VACLs], and router-based ACLs [RACLs])
- Traffic storm control (unicast, multicast, and broadcast)

For more information, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Supported Standards

This table lists the IEEE compliance standards.

Table 2: IEEE Compliance Standards

Standard	Description
802.1D	MAC Bridges
802.1p	Class of Service Tagging for Ethernet frames
802.1Q	VLAN Tagging
802.1s	Multiple Spanning Tree Protocol
802.1w	Rapid Spanning Tree Protocol
802.3ab	1000Base-T (10/100/1000 Ethernet over copper)
802.3ad	Link aggregation with LACP
802.3ae	10-Gigabit Ethernet

This table lists the RFC compliance standards. For information on each RFC, see www.ietf.org.

Table 3: RFC Compliance Standards

Standard	Description
BGP	
RFC 1997	<i>BGP Communities Attribute</i>
RFC 2385	<i>Protection of BGP Sessions via the TCP MD5 Signature Option</i>
RFC 2439	<i>BGP Route flap damping</i>
RFC 2519	<i>A Framework for Inter-Domain Route Aggregation</i>
RFC 2545	<i>Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing</i>
RFC 2858	<i>Multiprotocol Extensions for BGP-4</i>
RFC 2918	<i>Route Refresh Capability for BGP-4</i>
RFC 3065	<i>Autonomous System Confederations for BGP</i>

Standard	Description
RFC 3392	<i>Capabilities Advertisement with BGP-4</i>
RFC 4271	<i>BGP version 4</i>
RFC 4273	<i>BGP4 MIB - Definitions of Managed Objects for BGP-4</i>
RFC 4456	<i>BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)</i>
RFC 4486	<i>Subcodes for BGP cease notification message</i>
RFC 4724	<i>Graceful Restart Mechanism for BGP</i>
RFC 4893	<i>BGP Support for Four-octet AS Number Space</i>
RFC 5004	<i>Avoid BGP Best Path Transitions from One External to Another</i>
RFC 5396	<i>Textual Representation of Autonomous System (AS) Numbers</i> Note RFC 5396 is partially supported. The asplain and asdot notations are supported, but the asdot+ notation is not.
RFC 5549	<i>Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop</i>
RFC 5668	<i>4-Octet AS Specific BGP Extended Community</i>
ietf-draft	Bestpath transition avoidance (draft-ietf-idr-avoid-transition-05.txt)
ietf-draft	Peer table objects (draft-ietf-idr-bgp4-mib-15.txt)
ietf-draft	Dynamic Capability (draft-ietf-idr-dynamic-cap-03.txt)
IP Multicast	

Standard	Description
RFC 2236	<i>Internet Group Management Protocol, Version 2</i>
RFC 3376	<i>Internet Group Management Protocol, Version 3</i>
RFC 3446	<i>Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)</i>
RFC 3569	<i>An Overview of Source-Specific Multicast (SSM)</i>
RFC 3618	<i>Multicast Source Discovery Protocol (MSDP)</i>
RFC 4601	<i>Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)</i>
RFC 4607	<i>Source-Specific Multicast for IP</i>
RFC 4610	<i>Anycast-RP Using Protocol Independent Multicast (PIM)</i>
RFC 6187	<i>X.509v3 Certificates for Secure Shell Authentication</i>
ietf-draft	Mtrace server functionality, to process mtrace-requests, draft-ietf-idmr-traceroute-ipm-07.txt
IP Services	
RFC 768	<i>UDP</i>
RFC 783	<i>TFTP</i>
RFC 791	<i>IP</i>
RFC 792	<i>ICMP</i>
RFC 793	<i>TCP</i>
RFC 826	<i>ARP</i>
RFC 854	<i>Telnet</i>
RFC 959	<i>FTP</i>
RFC 1027	<i>Proxy ARP</i>

Standard	Description
RFC 1305	<i>NTP v3</i>
RFC 1519	<i>CIDR</i>
RFC 1542	<i>BootP relay</i>
RFC 1591	<i>DNS client</i>
RFC 1812	<i>IPv4 routers</i>
RFC 2131	<i>DHCP Helper</i>
RFC 2338	<i>VRRP</i>
IS-IS	
RFC 1142 (OSI 10589)	<i>OSI 10589 Intermediate system to intermediate system intra-domain routing exchange protocol</i>
RFC 1195	<i>Use of OSI IS-IS for routing in TCP/IP and dual environment</i>
RFC 2763	<i>Dynamic Hostname Exchange Mechanism for IS-IS</i>
RFC 2966	<i>Domain-wide Prefix Distribution with Two-Level IS-IS</i>
RFC 2973	<i>IS-IS Mesh Groups</i>
RFC 3277	<i>IS-IS Transient Blackhole Avoidance</i>
RFC 3373	<i>Three-Way Handshake for IS-IS Point-to-Point Adjacencies</i>
RFC 3567	<i>IS-IS Cryptographic Authentication</i>
RFC 3847	<i>Restart Signaling for IS-IS</i>
ietf-draft	Internet Draft Point-to-point operation over LAN in link-state routing protocols (draft-ietf-isis-igp-p2p-over-lan-06.txt)
OSPF	
RFC 2328	<i>OSPF Version 2</i>
RFC 2370	<i>OSPF Opaque LSA Option</i>
RFC 2740	<i>OSPF for IPv6 (OSPF version 3)</i>

Standard	Description
RFC 3101	<i>OSPF Not-So-Stubby-Area (NSSA) Option</i>
RFC 3137	<i>OSPF Stub Router Advertisement</i>
RFC 3509	<i>Alternative Implementations of OSPF Area Border Routers</i>
RFC 3623	<i>Graceful OSPF Restart</i>
RFC 4750	<i>OSPF Version 2 MIB</i>
Per-Hop Behavior (PHB)	
RFC 2597	<i>Assured Forwarding PHB Group</i>
RFC 3246	<i>An Expedited Forwarding PHB</i>
RIP	
RFC 1724	<i>RIPv2 MIB extension</i>
RFC 2082	<i>RIPv2 MD5 Authentication</i>
RFC 2453	<i>RIP Version 2</i>
SNMP	
RFC 2579	<i>Textual Conventions for SMIV2</i>
RFC 2819	<i>Remote Network Monitoring Management Information Base</i>
RFC 2863	<i>The Interfaces Group MIB</i>
RFC 3164	<i>The BSD syslog Protocol</i>
RFC 3176	<i>InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks</i>
RFC 3411 and RFC 3418	<i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i>
RFC 3413	<i>Simple Network Management Protocol (SNMP) Applications</i>
RFC 3417	<i>Transport Mappings for the Simple Network Management Protocol (SNMP)</i>



CHAPTER 3

Using the Cisco NX-OS Setup Utility

This chapter contains the following sections:

- [About the Cisco NX-OS Setup Utility, on page 15](#)
- [Prerequisites for the Setup Utility, on page 16](#)
- [Setting Up Your Cisco NX-OS Device, on page 17](#)
- [Additional References for the Setup Utility, on page 21](#)

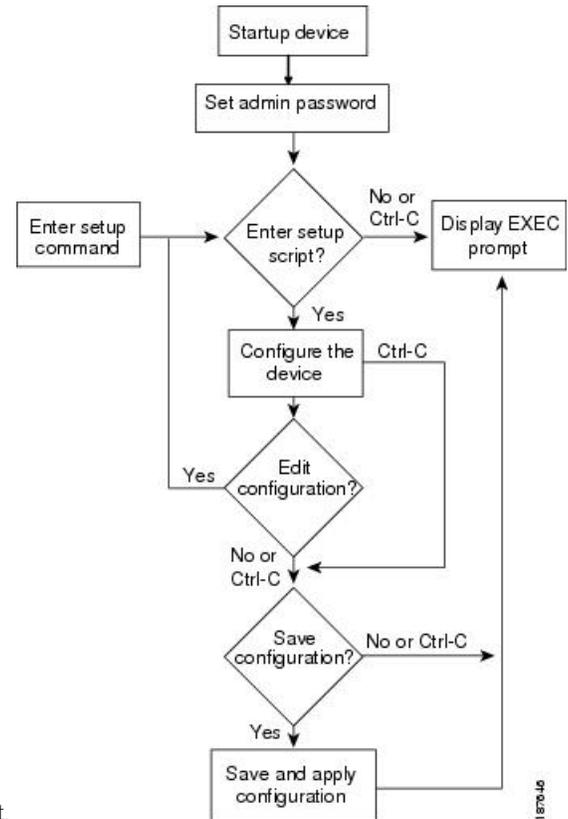
About the Cisco NX-OS Setup Utility

The Cisco NX-OS setup utility is an interactive command-line interface (CLI) mode that guides you through a basic (also called a startup) configuration of the system. The setup utility allows you to configure only enough connectivity for system management.

The setup utility allows you to build an initial configuration file using the System Configuration Dialog. The setup starts automatically when a device has no configuration file in NVRAM. The dialog guides you through initial configuration. After the file is created, you can use the CLI to perform additional configuration.

You can press **Ctrl-C** at any prompt to skip the remaining configuration options and proceed with what you have configured up to that point, except for the administrator password. If you want to skip answers to any questions, press **Enter**. If a default answer is not available (for example, the device hostname), the device uses what was previously configured and skips to the next question.

Figure 2: Setup Script Flow



This figure shows how to enter and exit the setup script.

You use the setup utility mainly for configuring the system initially, when no configuration is present. However, you can use the setup utility at any time for basic device configuration. The setup utility keeps the configured values when you skip steps in the script. For example, if you have already configured the mgmt0 interface, the setup utility does not change that configuration if you skip that step. However, if there is a default value for the step, the setup utility changes to the configuration using that default, not the configured value. Be sure to carefully check the configuration changes before you save the configuration.



Note Be sure to configure the IPv4 route, the default network IPv4 address, and the default gateway IPv4 address to enable SNMP access. If you enable IPv4 routing, the device uses the IPv4 route and the default network IPv4 address. If IPv4 routing is disabled, the device uses the default gateway IPv4 address.



Note The setup script only supports IPv4.

Prerequisites for the Setup Utility

The setup utility has the following prerequisites:

- Have a password strategy for your network environment.
- Connect the console port on the supervisor module to the network. If you have dual supervisor modules, connect the console ports on both supervisor modules to the network.
- Connect the Ethernet management port on the supervisor module to the network. If you have dual supervisor modules, connect the Ethernet management ports on both supervisor modules to the network.

Setting Up Your Cisco NX-OS Device

To configure basic management of the Cisco NX-OS device using the setup utility, follow these steps:

Procedure

Step 1 Power on the device.

Step 2 Enable or disable password-strength checking.

A strong password has the following characteristics:

- At least eight characters long
- Does not contain many consecutive characters (such as "abcd")
- Does not contain many repeating characters (such as "aaabbb")
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Example:

```
---- System Admin Account Setup ----  
Do you want to enforce secure password standard (yes/no) [y]: y
```

Step 3 Enter the new password for the administrator.

Note If a password is trivial (such as a short, easy-to-decipher password), your password configuration is rejected. Passwords are case sensitive. Be sure to configure a strong password that has at least eight characters, both uppercase and lowercase letters, and numbers.

Example:

```
Enter the password for "admin": <password>  
Confirm the password for "admin": <password>  
---- 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.

Please register Cisco Nexus 9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus devices must be registered to receive entitled support services.

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

Step 4 Enter the setup mode by entering **yes**.

Example:

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

Step 5 Create additional accounts by entering **yes** (**no** is the default).

Example:

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

a) Enter the user login ID.

Example:

Enter the User login Id : *user_login*

Caution Usernames must begin with an alphanumeric character and can contain only these special characters: (+ = . _ \ -). The # and ! symbols are not supported. If the username contains characters that are not allowed, the specified user is unable to log in.

b) Enter the user password.

Example:

Enter the password for "user1": *user_password*
Confirm the password for "user1": *user_password*

c) Enter the default user role.

Example:

Enter the user role (network-operator|network-admin) [network-operator]: *default_user_role*

For information on the default user roles, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Step 6 Configure an SNMP community string by entering **yes**.

Example:

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

```
SNMP community string : snmp_community_string
```

For information on SNMP, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Step 7 Enter a name for the device (the default name is switch).

Example:

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

Step 8 Configure out-of-band management by entering **yes**. You can then enter the mgmt0 IPv4 address and subnet mask.

Note You can only configure IPv4 address in the setup utility. For information on configuring IPv6, see the *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*.

Example:

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes  
Mgmt0 IPv4 address: mgmt0_ip_address  
Mgmt0 IPv4 netmask: mgmt0_subnet_mask
```

Step 9 Configure the IPv4 default gateway (recommended) by entering **yes**. You can then enter its IP address.

Example:

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

Step 10 Configure advanced IP options such as the static routes, default network, DNS, and domain name by entering **yes**.

Example:

```
Configure Advanced IP options (yes/no)? [n]: yes
```

Step 11 Configure a static route (recommended) by entering **yes**. You can then enter its destination prefix, destination prefix mask, and next hop IP address.

Example:

```
Configure static route: (yes/no) [y]: yes  
Destination prefix: dest_prefix  
Destination prefix mask: dest_mask  
Next hop ip address: next_hop_address
```

Step 12 Configure the default network (recommended) by entering **yes**. You can then enter its IPv4 address.

Note The default network IPv4 address is the same as the destination prefix in the static route configuration.

Example:

```
Configure the default network: (yes/no) [y]: yes
Default network IP address [dest_prefix]: dest_prefix
```

Step 13 Configure the DNS IPv4 address by entering **yes**. You can then enter the address.

Example:

```
Configure the DNS IP address? (yes/no) [y]: yes
DNS IP address: ipv4_address
```

Step 14 Configure the default domain name by entering **yes**. You can then enter the name.

Example:

```
Configure the DNS IP address? (yes/no) [y]: yes
DNS IP address: ipv4_address
```

Step 15 Enable the Telnet service by entering **yes**.

Example:

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

Step 16 Enable the SSH service by entering **yes**. You can then enter the key type and number of key bits. For more information, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Example:

```
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) : key_type
Number of key bits <768-2048> : number_of_bits
```

Step 17 Configure the NTP server by entering **yes**. You can then enter its IP address. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Example:

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

Step 18 Specify a default interface layer (L2 or L3).

Example:

```
Configure default interface layer (L3/L2) [L3]: interface_layer
```

Step 19 Enter the default switchport interface state (shutdown or no shutdown). A shutdown interface is in an administratively down state. For more information, see the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*.

Example:

```
Configure default switchport interface state (shut/noshut) [shut]: default_state
```

- Step 20** Enter the best practices profile for control plane policing (CoPP). For more information, see the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Example:

```
Configure best practices CoPP profile (strict/moderate/lenient/none) [strict]: moderate
```

The system now summarizes the complete configuration and asks if you want to edit it.

- Step 21** Continue to the next step by entering **no**. If you enter **yes**, the setup utility returns to the beginning of the setup and repeats each step.

Example:

```
Would you like to edit the configuration? (yes/no) [y]: yes
```

- Step 22** Use and save this configuration by entering **yes**. If you do not save the configuration at this point, none of your changes are part of the configuration the next time the device reboots. Enter **yes** to save the new configuration. This step ensures that the boot variables for the nx-os image are also automatically configured.

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 part of the configuration the next time that the device reboots. Enter **yes** to save the new configuration to ensure that the boot variables for the nx-os image are also automatically configured.

Additional References for the Setup Utility

This section includes additional information related to using the setup utility.

Related Documents for the Setup Utility

Related Topic	Document Title
Licensing	<i>Cisco NX-OS Licensing Guide</i>
SSH and Telnet	<i>Cisco Nexus 9000 Series NX-OS Security Configuration Guide</i>
User roles	<i>Cisco Nexus 9000 Series NX-OS Security Configuration Guide</i>
IPv4 and IPv6	<i>Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</i>

Related Topic	Document Title
SNMP and NTP	<i>Cisco Nexus 9000 Series NX-OS System Management Configuration Guide</i>



CHAPTER 4

Using PowerOn Auto Provisioning

This chapter contains the following sections:

- [About PowerOn Auto Provisioning, on page 23](#)
- [Guidelines and Limitations for POAP, on page 32](#)
- [Setting Up the Network Environment to Use POAP, on page 33](#)
- [Configuring a Switch Using POAP, on page 34](#)
- [Creating md5 Files, on page 34](#)
- [Verifying the Device Configuration, on page 36](#)
- [Troubleshooting for POAP, on page 36](#)
- [Managing the POAP Personality, on page 37](#)

About PowerOn Auto Provisioning

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

When a device with the POAP feature boots and does not find the startup configuration, the device enters POAP mode, locates a DHCP server, and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. The device also obtains the IP address of a TFTP server and downloads a configuration script that enables the switch to download and install the appropriate software image and configuration file.



Note The DHCP information is used only during the POAP process.



Note Checking for a USB device containing the configuration script file in POAP mode is not supported on the Cisco Nexus 9000 Series switches.

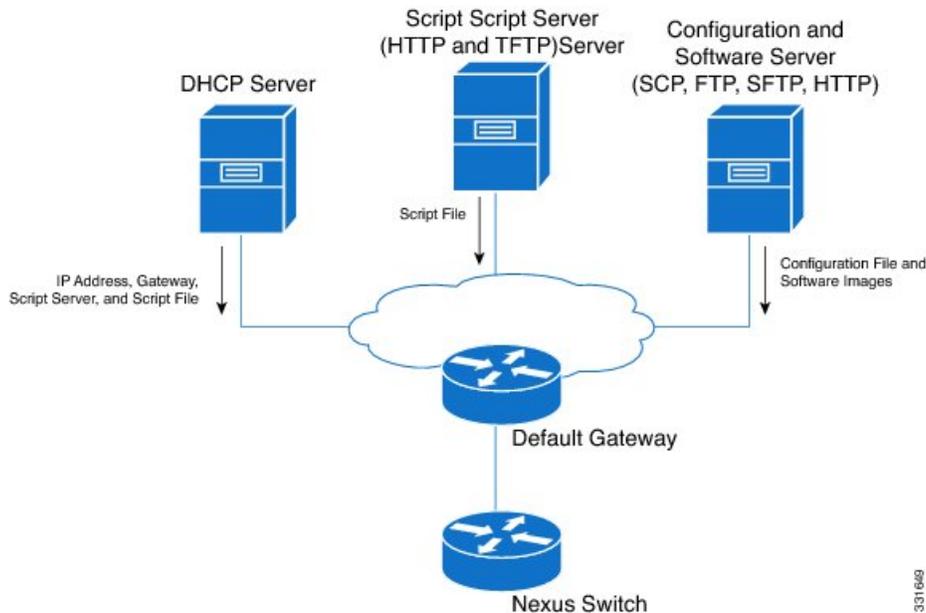
Network Requirements for POAP

POAP requires the following network infrastructure:

- A DHCP server to bootstrap the interface IP address, gateway address, and Domain Name System (DNS) server.

- A TFTP server that contains the configuration script used to automate the software image installation and configuration process.
- One or more servers that contains the desired software images and configuration files.
- If you use USB, then no DHCP server or TFTP server are required for POAP.

Figure 3: POAP Network Infrastructure



POAP Configuration Script

We provide a sample configuration script that is developed using the Python programming language. We recommend using the provided script and modifying it to meet the requirements of your network environment. The POAP script can be found at <https://github.com/datacenter/nexus9000/blob/master/nx-os/poap/poap.py>. To modify the script using Python, see the *Cisco NX-OS Python API Reference Guide* for your platform.

Using the POAP Script and POAP Script Options

Before using the POAP script, perform the following actions:

1. Edit the options dictionary at the top of the script to ensure that all relevant options for your setup are included in the script. Do not change the defaults (in the default options function) directly.
2. Update the MD5 checksum of the POAP script as shown using shell commands.

```
f=poap_nexus_script.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i
"s/^#md5sum=.*/#md5sum=\"$(md5sum $f.md5 | sed 's/ .*//')\"/" $f
```

3. If the device has a startup configuration, perform a write erase and reload the device.

The following POAP script options can be specified to alter the POAP script behavior. When you download files from a server, the hostname, username, and password options are required. For every mode except personality, the target_system_image is also required. Required parameters are enforced by the script, and the script aborts if the required parameters are not present. Every option except hostname, username, and password has a default option. If you do not specify the option in the options dictionary, the default is used.

- **username**

The username to use when downloading files from the server.

- **password**

The password to use when downloading files from the server.

- **hostname**

The name or address of the server from which to download files.

- **mode**

The default is **serial_number**.

Use one of the following options:

- **personality**

A method to restore the switch from a tarball.

- **serial_number**

The serial number of the switch to determine the configuration filename. The format for the serial number in the configuration file is `conf.serialnumber`. Example: `conf.FOC123456`

- **hostname**

The hostname as received in the DHCP options to determine the configuration filename. The format for the hostname in the configuration file is `conf_hostname.cfg`. Example: `conf_3164-RS.cfg`

- **mac**

The interface MAC address to determine the configuration filename. The format for the hostname in the configuration file is `conf_macaddress.cfg`. Example: `conf_7426CC5C9180.cfg`

- **raw**

The configuration filename is used exactly as provided in the options. The filename is not altered in any way.

- **location**

The CDP neighbors are used to determine the configuration filename. The format for the location in the configuration file is `conf_host_intf.cfg`, where *host* is the host connected to the device over the POAP interface, and *intf* is the remote interface to which the POAP interface is connected. Example: `conf_remote-switch_Eth1_8.cfg`

- **required_space**

The required space in KB for that particular iteration of POAP. The default is 100,000. For multi-step upgrades, specify the size of the last image in the upgrade path of the target image.

- **transfer_protocol**

Any transfer protocol such as http, https, ftp, scp, sftp, or tftp that is supported by VSH. The default is scp.

- **config_path**

The path to the configuration file on the server. Example: /tftpboot. The default is /var/lib/tftpboot.

- **target_system_image**

The name of the image to download from the remote server. This is the image you get after POAP completes. This option is a required parameter for every mode except personality. The default is "".

- **target_image_path**

The path to the image on the server. Example: /tftpboot. The default is /var/lib/tftpboot.

- **destination_path**

The path to which to download images and MD5 sums. The default is /bootflash.

- **destination_system_image**

The name for the destination image filename. If not specified, the default will be the target_system_image name.

- **user_app_path**

The path on the server where the user scripts, agents, and user data are located. The default is /var/lib/tftpboot.

- **disable_md5**

This is True if MD5 checking should be disabled. The default is False.

- **midway_system_image**

The name of the image to use for the midway system upgrade. By default, the POAP script finds the name of any required midway images in the upgrade path and uses them. Set this option if you prefer to pick a different midway image for a two-step upgrade. The default is "".

- **source_config_file**

The name of the configuration file when raw mode is used. The default is poap.cfg.

- **vrf**

The VRF to use for downloads and so on. The VRF is automatically set by the POAP process. The default is the POAP_VRF environment variable.

- **destination_config**

The name to use for the downloaded configuration. The default is poap_replay.cfg.

- **split_config_first**

The name to use for the first configuration portion if the configuration needs to be split. It is applicable only when the configuration requires a reload to take effect. The default is poap_1.cfg.

- **split_config_second**

The name to use for the second configuration portion if the configuration is split. The default is poap_2.cfg.

- **timeout_config**

The timeout in seconds for copying the configuration file. The default is 120. For non-legacy images, this option is not used, and the POAP process times out. For legacy images, FTP uses this timeout for the login process and not for the copy process, while scp and other protocols use this timeout for the copy process.

- **timeout_copy_system**

The timeout in seconds for copying the system image. The default is 2100. For non-legacy images, this option is not used, and the POAP process times out. For legacy images, FTP uses this timeout for the login process and not for the copy process, while scp and other protocols use this timeout for the copy process.

- **timeout_copy_personality**

The timeout in seconds for copying the personality tarball. The default is 900. For non-legacy images, this option is not used, and the POAP process times out. For legacy images, FTP uses this timeout for the login process and not for the copy process, while scp and other protocols use this timeout for the copy process.

- **timeout_copy_user**

The timeout in seconds for copying any user scripts and agents. The default is 900. For non-legacy images, this option is not used, and the POAP process times out. For legacy images, FTP uses this timeout for the login process and not for the copy process, while scp and other protocols use this timeout for the copy process.

- **personality_path**

The remote path from which to download the personality tarball. Once the tarball is downloaded and the personality process is started, the personality will download all files in the future from locations specified inside the tarball configuration. The default is /var/lib/tftpboot.

- **source_tarball**

The name of the personality tarball to download. The default is personality.tar.

- **destination_tarball**

The name for the downloaded personality tarball after it is downloaded. The default is personality.tar.

Setting up the DHCP Server without DNS for POAP

Beginning with Cisco NX-OS Release 7.0(3)I6(1), the tftp-server-name can be used without the DNS option. To enable POAP functionality without DNS on earlier releases, a custom option of 150 must be used to specify the tftp-server-address.

To use the tftp-server-address option, specify the following at the start of your dhcpd.conf file.

```
option tftp-server-address code 150 = ip-address;
```

For example:

```
host MyDevice {
    option dhcp-client-identifier "\000SAL12345678";
    fixed-address 2.1.1.10;
    option routers 2.1.1.1;
    option host-name "MyDevice";
    option bootfile-name "poap_nexus_script.py";
}
```

```
option tftp-server-address 2.1.1.1;
}
```

Downloading and Using User Data, Agents, and Scripts as part of POAP

Under the options dictionary, you can find the **download_scripts_and_agents** function. If you choose to download user scripts and data, uncomment the first **poap_log** line and then use a series of **download_user_app** function calls to download each application. Since older Cisco NX-OS versions do not support recursive copy of directories, such directories must be put into a tarball (TAR archive) and then unpacked once on the switch. The parameters for the **download_scripts_and_agents** function are as follows:

- **source_path** - The path to where the file or tarball is located. This is a required parameter. Example: `/var/lib/tftpboot`.
- **source_file** - The name of the file to download. This is a required parameter. Example: `agents.tar`, `script.py`, and so on.
- **dest_path** - The location to download the file on the switch. Any directories that do not exist earlier will be created. This is an optional parameter. The default is `/bootflash`.
- **dest_file** - The name to give the downloaded file. This is an optional parameter. The default is unchanged `source_file`.
- **unpack** - Indicates whether a tarball exists for unpacking. Unpacking is done with `tar -xf tarfile -C /bootflash`. This is an optional parameter. The default is `False`.
- **delete_after_unpack** - Indicates whether to delete the downloaded tarball after unpack is successful. There is no effect if `unpack` is `False`. The default is `False`.

Using the download functionality, you can download all the agents and files needed to run POAP. To start the agents, you should have the configuration present in the running configuration downloaded by POAP. Then the agents, scheduler, and cron entry, along with EEM, can be used.

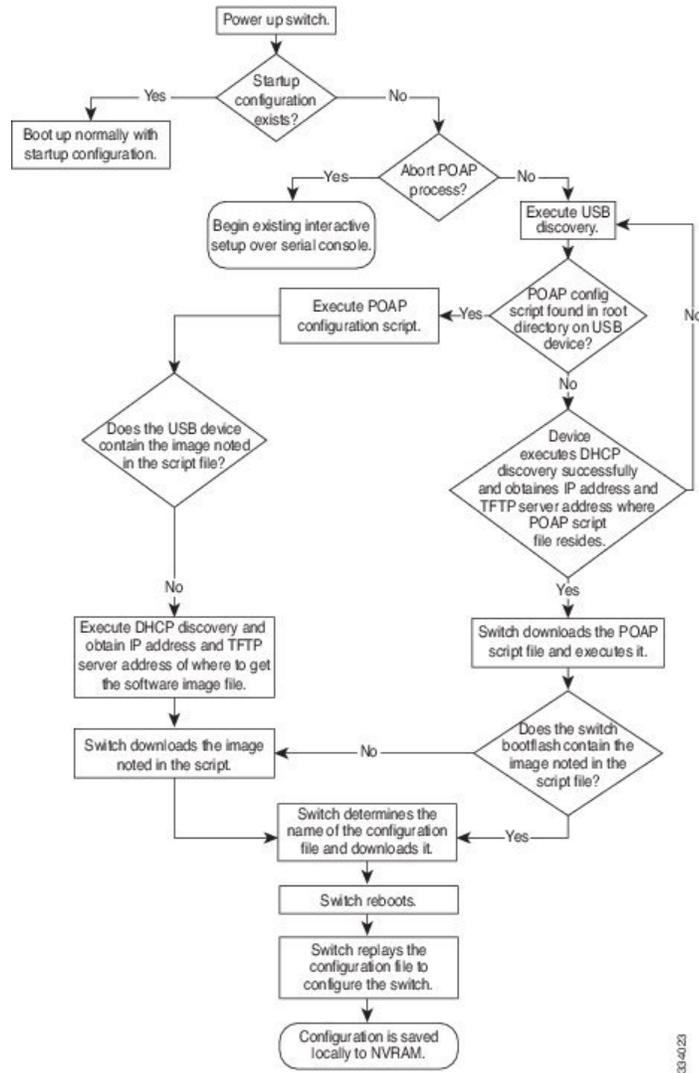
POAP Process

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 4: POAP Process



Power-Up Phase

When you powerup the device for the first time, it loads the software image that is installed at manufacturing and tries to find a configuration file from which to boot. When a configuration file is not found, POAP mode starts.

During startup, a prompt appears asking if you want to abort POAP and continue with a 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 the default configuration.

DHCP Discovery Phase

The switch sends out DHCP discover messages on the front-panel interfaces or the MGMT interface that solicit DHCP offers from the DHCP server or servers. (See the following figure.) The DHCP client on the Cisco Nexus switch uses the switch serial number 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 filename, 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 the DHCP negotiation.

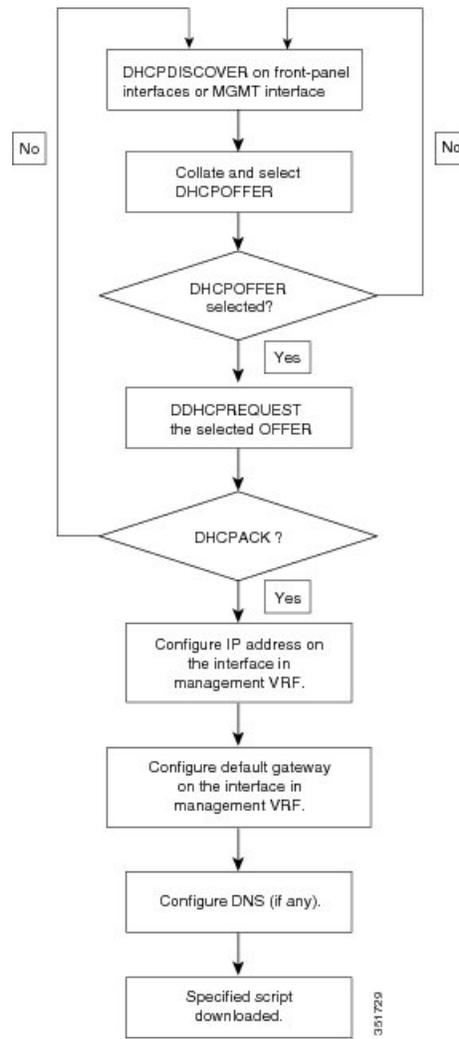
The DHCP discover message also solicits the following options from the DHCP server:

- TFTP server name or 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.
- 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, the one arriving first is honored and the POAP process moves to next stage. 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 a failure occurs 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.

Figure 5: DHCP Discovery Process



POAP Dynamic Breakout

Beginning with Cisco NX-OS Release 7.0(3)I4(1), POAP dynamically breaks out ports in an effort to detect a DHCP server behind one of the broken-out ports. Previously, the DHCP server used for POAP had to be directly connected to a normal cable because breakout cables were not supported.

POAP determines which breakout map (for example, 10gx4, 50gx2, 25gx4, or 10gx2) will bring up the link connected to the DHCP server. If breakout is not supported on any of the ports, POAP skips the dynamic breakout process. After the breakout loop completes, POAP proceeds with the DHCP discovery phase as normal.



Note For more information on dynamic breakout, see the interfaces configuration guide for your device.

Script Execution Phase

After the device bootstraps itself using the information in the DHCP acknowledgement, the script file is downloaded from the TFTP 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 that currently runs 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 an image 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.

Guidelines and Limitations for POAP

POAP configuration guidelines and limitations are as follows:

- The 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 virtual port channel (vPC) pair using static port channels on the vPC links, the Cisco Nexus device activates all of its links when POAP starts up. 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 that are connected to the Cisco Nexus device, which causes traffic to get lost.

To work around this issue, you can configure Link Aggregation Control Protocol (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 9000 Series switch through a LACP port channel, the Cisco Nexus 9000 Series switch 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 9000 Series switch to not suspend its member ports by 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.

- You can bypass the password and the basic POAP configuration by using the **skip** option at the POAP prompt. When you use the **skip** option, no password is configured for the admin user. The **copy running-config startup-config** command is blocked until a valid password is set for the admin user.
- If the **boot poap enable** command (perpetual POAP) is enabled on the switch, on a reload, a POAP boot is triggered even if there is a startup configuration present. If you do not want to use POAP in this scenario, remove the boot poap enable configuration by using the **no boot poap enable** command.
- 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.

You can configure the format of the script log file. Script file log formats are specified in the script. The template of the script log file has a default format; however, you can choose a different format for the script execution log file.
- You must clear the temporary POAP configurations from POAP script after successful provisioning. If you don't clear them there might be a configuration leak when you reload. Make sure you include "no-reload" and "write erase" in POAP scripts so that previous configurations are cleared before importing a new configuration through POAP.
- The POAP feature does not require a license and is enabled by default. However for the POAP feature to function, appropriate licenses must be installed on the devices in the network before the deployment of the network.
- Beginning with NX-OS 7.0(3)I7(4), RFC 3004 (User Class Option for DHCP) is supported. This enables POAP to support user-class option 77 for DHCPv4 and user-class option 15 for DHCPv6. The text displayed for the user class option for both DHCPv4 and DHCPv6 is "Cisco-POAP".
 - With RFC 3004 (User Class Option for DHCP) support, POAP over IPv6 is supported on Nexus 9000 switches. The POAP over IPv6 feature enables the POAP process to use IPv6 when IPv4 fails. The feature is designed to cycle between IPv4 and IPv6 protocols when a connection failure occurs.
- For secure POAP, ensure that DHCP snooping is enabled.
- To support POAP, set firewall rules to block unintended or malicious DHCP servers.
- To maintain system security and make POAP more secure, configure the following:
 - Enable DHCP snooping.
 - Set firewall rules to block unintended or malicious DHCP servers.
- POAP is supported on both MGMT ports and in-band ports.

Setting Up the Network Environment to Use POAP

Procedure

-
- Step 1** Modify the configuration script provided as necessary.
- 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 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.

Procedure

- 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.
-

What to do next

Verify the configuration.

Creating md5 Files

Every time you make a change to the configuration script, ensure that you recalculate the MD5 checksum by running `# f=poap_fabric.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i "s/^#md5sum=.*/#md5sum=\"$ (md5sum $f.md5 | sed 's/ .*//')\"/" $f` using a bash shell.

This procedure replaces `md5sum` in `poap_fabric.py` with a new value if there was any change in that file.



- Note** Steps 1-4 and 7-8 are needed only if you are using the BASH shell. If you have access to any other Linux server, these steps are not required.
-

Before you begin

Access to the BASH shell.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# <code>configure terminal</code> switch(config)#	Enters global configuration mode.
Step 2	feature bash-shell Example: switch(config)# <code>feature bash-shell</code>	Enable BASH shell feature.
Step 3	exit Example: switch(config)# <code>exit</code>	Exit configuration mode.
Step 4	run bash Example: switch# <code>run bash</code>	Open Linux BASH.
Step 5	md5sum /bootflash/nxos.release_number.bin > /bootflash/nxos.release_number.bin.md5 Example: bash-4.2\$ <code>md5sum</code> <code>/bootflash/nxos.7.0.3.I6.1.bin ></code> <code>/bootflash/nxos.7.0.3.I6.1.bin.md5</code>	Creates md5sum for the .bin file.
Step 6	md5sum /bootflash/poap.cfg > /bootflash/poap.cfg.md5 Example: bash-4.2\$ <code>md5sum /bootflash/poap.cfg ></code> <code>/bootflash/poap.cfg.md5</code>	Creates md5sum for the .cfg file.
Step 7	exit Example: switch(config)# <code>exit</code>	Exit the BASH shell.
Step 8	dir i .md5 Example: switch# <code>dir i .md5</code> 65 Jun 09 12:38:48 2017 nxos.7.0.3.I6.1.bin.md5 54 Jun 09 12:39:36 2017 poap.cfg.md5 67299 Jun 09 12:48:58 2017 poap.py.md5	Display the .md5 files.

	Command or Action	Purpose
Step 9	<pre>copy bootflash:poap.cfg.md5 scp://ip_address/ Example: copy bootflash:poap.cfg.md5 scp://10.1.100.3/ Enter vrf (If no input, current vrf 'default' is considered): management Enter username: root root@10.1.100.3's password: poap.cfg.md5 100% 54 0.1KB/s 00:00 Copy complete.</pre>	Uploads the files to the Configuration and Software Server.

Verifying the Device Configuration

To verify the configuration, use one of the following commands:

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

This option masks the sensitive words in running configuration output with <removed> keyword.

Troubleshooting for POAP

The following is a list of known issues and suggestions while using POAP:

- Issue: POAP script execution fails immediately with no syslogs or output except for a "Script execution failed" statement.

Suggestion: Use the **python** *script-name* command on the server and make sure there are no syntax errors. The options dictionary is a Python dictionary so each entry must be comma separated and have the key or option and the value separated by a colon.

- Issue: A TypeError exception occurs at various places depending on the incorrectly used option.

Suggestion: Some options use integers (for example, timeouts and other numeric values). Check the options dictionary for numeric values that are enclosed in quotes. Refer to the options list for the correct usage.

Managing the POAP Personality

POAP Personality

The POAP personality feature, which is introduced in Cisco NX-OS Release 7.0(3)I4(1), enables user data, Cisco NX-OS and third-party patches, and configuration files to be backed up and restored. In previous releases, POAP can restore only the configuration.

The POAP personality is defined by tracked files on the switch. The configuration and package list in the personality file are ASCII files.

Binary versions are recorded in the personality file, but the actual binary files are not included. Because binary files are typically large, they are accessed from a specified repository.

The personality file is a .tar file, which would typically be extracted into a temporary folder. Here is an example:

```
switch# dir bootflash: 042516182843personality # timestamp name
46985 Dec 06 23:12:56 2015 running-config Same as "show running-configuration" command.
20512 Dec 06 23:12:56 2015 host-package-list Package/Patches list
58056 Dec 06 23:12:56 2015 data.tar User Data
25 Dec 06 23:12:56 2015 IMAGEFILE Tracked image metadata
```

Backing Up the POAP Personality

You can create a backup of the POAP personality either locally on the switch or remotely on the server. The personality backup taken from the switch should be restored only on a switch of the same model.



Note If you are using the Cisco scheduler feature for backups, you can configure it to also back up the POAP personality, as shown in the following example. For more information on the scheduler, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

```
switch(config)# scheduler schedule name weeklybkup
switch(config-schedule)# time weekly mon:07:00
switch(config-schedule)# job name personalitybkup
switch(config-schedule)# exit
switch(config)# scheduler job name personalitybkup
switch(config-job)# personality backup bootflash:/personality-file ; copy
bootflash:/personality-file tftp://10.1.1.1/ vrf management
```

Procedure

	Command or Action	Purpose
Step 1	Required: personality backup [bootflash:uri scp:uri] Example: <pre>switch# personality backup bootflash:personality1.tar</pre> Example:	Creates a backup of the POAP personality.

	Command or Action	Purpose
	switch# personality backup scp://root@2.1.1.1/var/lib/tftpboot/backup.tar	

Configuring the POAP Personality

You can specify whether the POAP personality should be derived from the running state of the system or the committed (startup) state.

Procedure

	Command or Action	Purpose
Step 1	Required: configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	Required: personality Example: switch# personality switch(config-personality)#	Enters personality configuration mode.
Step 3	Required: track [running-state startup-state data local-directories-or-files] Example: switch(config-personality)# track data bootflash:myfile1 Example: switch(config-personality)# track data bootflash:user_scripts/*.py Example: switch(config-personality)# track data bootflash:basedir/*/backup_data	Specifies how the POAP personality is derived. The following options are available: <ul style="list-style-type: none"> • running-state—Captures the following information: the running configuration (as shown in the show running-config command), active Cisco NX-OS patches and third-party packages in the host system, and the image name (as shown in the show version command). This is the default option. • startup-state—Captures the following information: the startup configuration (as shown in the show startup-config command), committed Cisco NX-OS patches and third-party packages in the host system, and the image name (as shown in the show version command). • data local-directories-or-files—Specifies a directory or file to be backed up. You can enter this command multiple times to back up multiple directories and files. UNIX-style wildcard characters are supported. In the example, one folder and two directories are specified.

	Command or Action	Purpose
		<p>Note Do not use this command to backup binary files in the bootflash and do not point to the entire bootflash.</p> <p>Note Guest Shell packages are not tracked.</p> <p>Note Signed RPMs (which require a key) are not supported. The POAP personality feature does not work with signed RPMs.</p>
Step 4	Required: binary-location <i>source-uri-folder</i> Example: <pre>switch(config-personality) # binary-location scp://remote-dir1/nxos_patches/</pre>	Specifies the local or remote directory from which to pick up binary files when the POAP personality is restored. You can enter this command multiple times (in order of priority) to specify multiple locations.

Restoring the POAP Personality

During the POAP script execution phase, the personality module in the script restores the POAP personality, provided that the currently booted switch image is Cisco NX-OS Release 7.0(3)I4(1) or later. If necessary, upgrade the switch to the correct software image.



Note A personality restore is done with the same software image used for the personality backup. Upgrading to a newer image is not supported through the POAP personality feature. To upgrade to a newer image, use the regular POAP script.



Note If the personality script fails to execute for any reason (such as not enough space in the bootflash or a script execution failure), the POAP process returns to the DHCP discovery phase.

The restore process performs the following actions:

1. Untars and unzips the personality file in the bootflash.
2. Validates the personality file.
3. Reads the configuration and package list files from the personality file to make a list of the binaries to be downloaded.
4. If the current image or patches are not the same as specified in the personality file, downloads the binaries to the bootflash (if not present) and reboots with the correct image and then applies the packages or patches.
5. Unzips or untars the user data files relative to "/".

6. Copies the configuration file in the POAP personality to the startup configuration.
7. Reboots the switch.

POAP Personality Sample Script

The following sample POAP script (poap.py) includes the personality feature:

```
#md5sum="b00a7fffb305d13a1e02cd0d342afca3"
# The above is the (embedded) md5sum of this file taken without this line, # can be # created
this way:
# f=poap.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i "s/^#md5sum=.*/#md5sum=$(md5sum
$f.md5 | sed 's/ .*//')/" $f # This way this script's integrity can be checked in case you
do not trust # tftp's ip checksum. This integrity check is done by /isan/bin/poap.bin).
# The integrity of the files downloaded later (images, config) is checked # by downloading
the corresponding file with the .md5 extension and is # done by this script itself.

from poap.personality import POAPPersonality import os

# Location to download system image files, checksums, etc.
download_path = "/var/lib/tftpboot"
# The path to the personality tarball used for restoration personality_tarball =
"/var/lib/tftpboot/foo.tar"
# The protocol to use to download images/config protocol = "scp"
# The username to download images, the personality tarball, and the # patches and RPMs
during restoration username = "root"
# The password for the above username
password = "passwd754"
# The hostname or IP address of the file server server = "2.1.1.1"

# The VRF to use for downloading and restoration vrf = "default"
if os.environ.has_key('POAP_VRF'):
    vrf = os.environ['POAP_VRF']

# Initialize housekeeping stuff (logs, temp dirs, etc.) p = POAPPersonality(download_path,
personality_tarball, protocol, username, password, server, vrf)

p.get_personality()
p.apply_personality()

sys.exit(0)
```



CHAPTER 5

Understanding the Command-Line Interface

This chapter contains the following sections:

- About the CLI Prompt, on page 41
- Command Modes, on page 42
- Special Characters, on page 46
- Keystroke Shortcuts, on page 46
- Abbreviating Commands, on page 49
- Completing a Partial Command Name, on page 49
- Identifying Your Location in the Command Hierarchy, on page 50
- Using the no Form of a Command, on page 50
- Configuring CLI Variables, on page 51
- Command Aliases, on page 53
- Command Scripts, on page 55
- Context-Sensitive Help, on page 56
- Understanding Regular Expressions, on page 58
- Searching and Filtering show Command Output, on page 59
- Searching and Filtering from the --More-- Prompt, on page 64
- Using the Command History, on page 65
- Enabling or Disabling the CLI Confirmation Prompts, on page 66
- Setting CLI Display Colors, on page 67
- Sending Commands to Modules, on page 67
- Sending Command Output in Email, on page 68
- BIOS Loader Prompt, on page 70
- Examples Using the CLI, on page 70

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) 2002-2013, 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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	<pre>switch# configure terminal switch(config)#</pre>	<p>Note The CLI prompt changes to indicate that you are in global configuration mode.</p>

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 9000 Series NX-OS Interfaces Configuration Guide*.

Procedure

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>interface type number</p> <p>Example:</p> <pre>switch(config)# interface ethernet 2/2 switch(config-if)#</pre>	<p>Specifies the interface that you want to configure.</p> <p>The CLI places you into interface configuration mode for the specified interface.</p> <p>Note The CLI prompt changes to indicate that you are in interface configuration mode.</p>

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 9000 Series NX-OS Interfaces Configuration Guide*.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	interface <i>type number.subint</i> Example: <pre>switch(config)# interface ethernet 2/2.1 switch(config-subif)#</pre>	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 subinterface configuration mode.

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.

The following 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

Procedure

	Command or Action	Purpose
Step 1	exit Example: <pre>switch(config-if)# exit switch(config)#</pre>	Exits from the current configuration command mode and returns to the previous configuration command mode.
Step 2	end Example:	Exits from the current configuration command mode and returns to EXEC mode.

	Command or Action	Purpose
	switch(config-if)# end switch#	
Step 3	(Optional) Ctrl-Z Example: switch(config-if)# ^z switch#	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 4: 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, 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 .
VRF configuration	From global configuration mode, use the vrf command and specify a routing protocol.	switch(config-vrf)#	To exit to global configuration mode, use the exit command. To exit to EXEC mode, use the end command or press Ctrl-Z .
EXEC for a nondefault VRF	From EXEC mode, use the routing-context vrf command and specify a VRF.	switch-red#	To exit to the default VRF, use the routing-context vrf default command.

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 5: 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 6: Keystroke Shortcuts

Keystrokes	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.
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.

Keystrokes	Description
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 to the right one character.
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.
Down arrow key	Displays the next command in the command history.
Right arrow key Left arrow key	Moves your cursor through the command string, either forward or backward, allowing you to edit the current command.
?	Displays a list of available commands.

Keystrokes	Description
Tab	<p>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.</p> <p>Use tabs to complete the following items:</p> <ul style="list-style-type: none"> • Command names • Scheme names in the file system • Server names in the file system • Filenames in the file system <p>Example:</p> <pre>switch(config)# xm<Tab> switch(config)# xml<Tab> switch(config)# xml server</pre>
	<p>Example:</p> <pre>switch(config)# c<Tab> callhome class-map clock cdp cli control-plane switch(config)# cl<Tab> class-map cli clock switch(config)# cla<Tab> switch(config)# class-map</pre>
	<p>Example:</p> <pre>switch# cd bootflash:<Tab> bootflash:/// bootflash://sup-1/ bootflash://sup-active/ bootflash://sup-local/ bootflash://module-27/ bootflash://module-28/</pre>
	<p>Example:</p> <pre>switch# cd bootflash://mo<Tab> bootflash://module-27/ bootflash://module-28/ switch# cd bootflash://module-2</pre> <p>Note You cannot access remote machines using the cd command. If you are on slot 27 and enter the cd bootflash://module-28 command, the following message appears: "Changing directory to a non-local server is not allowed."</p>

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 7: 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).

Procedure

	Command or Action	Purpose
Step 1	where detail Example: <pre>switch# configure terminal switch(config)# interface mgmt0 switch(config-if)# where detail mode: conf interface mgmt0 username: admin routing-context vrf: default</pre>	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.

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="2013-05-12-13.43.13"
testinterface="ethernet1/2"

switch# cli no var name testinterface
switch# show cli variables
SWITCHNAME="switch"
TIMESTAMP="2013-05-12-13.43.13"

```

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)`.

Procedure

	Command or Action	Purpose
Step 1	cli var name <i>variable-name variable-text</i> Example: <pre>switch# cli var name testinterface ethernet 2/1</pre>	Configures the CLI session variable. The <i>variable-name</i> argument is alphanumeric, case sensitive, and has a maximum length of 31 characters. The <i>variable-text</i> argument is alphanumeric, case sensitive, can contain spaces, and has a maximum length of 200 characters. Note Beginning with Cisco NX-OS Release 7.0(3)I4(1), variables can include hyphens (-) and underscores (_).
Step 2	(Optional) show cli variables Example: <pre>switch# show cli variables</pre>	Displays the CLI variable configuration.

Configuring Persistent CLI Variables

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

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	cli var name <i>variable-name variable-text</i> Example: <pre>switch(config)# cli var name testinterface ethernet 2/1</pre>	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.

	Command or Action	Purpose
		Note Beginning with Cisco NX-OS Release 7.0(3)I4(1), variables can include hyphens (-) and underscores (_).
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	(Optional) show cli variables Example: switch# show cli variables	Displays the CLI variable configuration.
Step 5	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	cli alias name <i>alias-name alias-text</i> Example: <pre>switch(config)# cli alias name ethint interface ethernet</pre>	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: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	(Optional) alias Example: <pre>switch# alias</pre>	Displays the command alias configuration.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

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.

Procedure

	Command or Action	Purpose
Step 1	terminal alias [persist] <i>alias-name</i> <i>command-string</i> Example: <pre>switch# terminal alias shintbr show interface brief</pre>	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: or volatile: directory on the Cisco NX-OS device.

Procedure

	Command or Action	Purpose
Step 1	run-script [bootflash: volatile:] <i>filename</i> Example: <pre>switch# run-script testfile</pre>	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 8: 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.

Formatting Option	Description
\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.

Procedure

	Command or Action	Purpose
Step 1	echo [backslash-interpret] [text] Example: <pre>switch# echo This is a test. This is a test.</pre>	The backslash-interpret keyword indicates that the text string contains formatting options. The <i>text</i> 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.

Procedure

	Command or Action	Purpose
Step 1	sleep seconds Example: <pre>switch# sleep 30</pre>	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 9: Context-Sensitive Help Example

Example Outputs	Description
<pre>switch# clock ? set HH:MM:SS Current Time switch# clock</pre>	<p>Displays the command syntax for the clock command in EXEC mode.</p> <p>The switch output shows that the set keyword is required for using the clock command.</p>
<pre>switch# clock set ? WORD HH:MM:SS Current Time switch# clock set</pre>	<p>Displays the command syntax for setting the time.</p> <p>The help output shows that the current time is required for setting the clock and how to format the time.</p>
<pre>switch# clock set 13:32:00<CR> % Incomplete command switch#</pre>	<p>Adds the current time.</p> <p>The CLI indicates the command is incomplete.</p>
<pre>switch# <Ctrl-P> switch# clock set 13:32:00</pre>	<p>Displays the previous command that you entered.</p>
<pre>switch# clock set 13:32:00 ? <1-31> Day of the month switch# clock set 13:32:00</pre>	<p>Displays the additional arguments for the clock set command.</p>
<pre>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</pre>	<p>Displays the additional arguments for the clock set command.</p>
<pre>switch# clock set 13:32:00 18 April 13<CR> % Invalid input detected at '^' marker.</pre>	<p>Adds the date to the clock setting.</p> <p>The CLI indicates an error with the caret symbol (^) at 13.</p>
<pre>switch# clock set 13:32:00 18 April ? <2000-2030> Enter the year (no abbreviation) switch# clock set 13:32:00 18 April</pre>	<p>Displays the correct arguments for the year.</p>
<pre>switch# clock set 13:32:00 18 April 2013<CR> switch#</pre>	<p>Enters the correct syntax for the clock set command.</p>

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 10: 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 11: 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 12: Filtering and Searching Keywords

Keyword Syntax	Description
begin <i>string</i> Example: <pre>show version begin Hardware</pre>	Starts displaying at the line that contains the text that matches the search string. The search string is case sensitive.
count Example: <pre>show running-config count</pre>	Displays the number of lines in the command output.
cut [- d <i>character</i>] {- b - c - f - s } Example: <pre>show file testoutput cut -b 1-10</pre>	Displays only part of the output lines. You can display a number of bytes (- b), characters (- vcut [- d <i>character</i>] {- 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 line that does not contain the delimiter.
end <i>string</i> Example: <pre>show running-config end interface</pre>	Displays all lines up to the last occurrence of the search string.
exclude <i>string</i> Example: <pre>show interface brief exclude down</pre>	Displays all lines that do not include the search string. The search string is case sensitive.
head [<i>lines lines</i>] Example: <pre>show logging logfile head lines 50</pre>	Displays the beginning of the output for the number of lines specified. The default number of lines is 10.
human Example: <pre>show version human</pre>	Displays the output in normal format if you have previously set the output format to XML using the terminal output xml command.

Keyword Syntax	Description
include <i>string</i> Example: <code>show interface brief include up</code>	Displays all lines that include the search string. The search string is case sensitive.
last [<i>lines</i>] Example: <code>show logging logfile last 50</code>	Displays the end of the output for the number of lines specified. The default number of lines is 10.
no-more Example: <code>show interface brief no-more</code>	Displays all the output without stopping at the end of the screen with the <code>--More--</code> prompt.
sscp <i>SSH-connection-name filename</i> Example: <code>show version sscp MyConnection</code> <code>show_version_output</code>	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 [<i>bytes lines words</i>] Example: <code>show file testoutput wc bytes</code>	Displays counts of characters, lines, or words. The default is to display the number of lines, words, and characters.
xml Example: <code>show version xml</code>	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-sessions**] [**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 13: 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.
word-exp	Displays only lines that match a complete word.
<i>expression</i>	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.

Mini AWK Utility

AWK is a simple but powerful utility to summarize text output. You can use this utility after a pipe (`|`) to further process the text output of a command. Cisco NX-OS supports a mini AWK, which takes an inline program as an argument.

This example shows how the mini AWK utility can be used to summarize the text output of the **show ip route summary vrf all** command:

```

switch# show ip route summary vrf all | grep "Total number of routes"
Total number of routes: 3
Total number of routes: 10

switch# show ip route summary vrf all | grep "Total number of routes" | awk '{ x = x + $5}
END { print x }'
13

```

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 14: 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.
-k <i>field-number</i> [<i>.char-position</i>][<i>ordering</i>]	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 <i>delimiter</i>	Sorts using a specified delimiter. The default delimiter is the space character.

Parameter	Description
-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 15: --More-- Prompt Commands

Commands	Description
[<i>lines</i>]<space>	Displays output lines for either the specified number of lines or the current screen size.
[<i>lines</i>] z	Displays output lines for either the specified number of lines or the current screen size. If you use the <i>lines</i> argument, that value becomes the new default screen size.
[<i>lines</i>]<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 <i>lines</i> argument, that value becomes the new default number of lines to display for this command.
[<i>lines</i>] d or [<i>lines</i>]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 <i>lines</i> 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.
[<i>lines</i>] 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.
[<i>lines</i>] 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.
[<i>count</i>]/ <i>expression</i>	Skips to the line that matches the regular expression and displays a screen of output lines. Use the optional <i>count</i> 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.
[<i>count</i>] n	Skips to the next line that matches the current regular expression and displays a screen of output lines. Use the optional <i>count</i> argument to skip past matches.
{ ! !: [<i>shell-cmd</i>]}	Executes the command specified in the <i>shell-cmd</i> argument in a subshell.

Commands	Description
.	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.

Procedure

	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:

```
show cli history [lines] [config-mode | exec-mode | this-mode-only] [unformatted]
```

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

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

```
switch# show cli history
```

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

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

This example shows how to display only the configuration commands in the command history:

```
switch(config)# show cli history config-mode
```

This example shows how to display only the EXEC commands in the command history:

```
switch(config)# show cli history exec-mode
```

This example shows how to display only the commands in the command history for the current command mode:

```
switch(config-if)# show cli history this-mode-only
```

This 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.

Procedure

	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.

	Command or Action	Purpose
		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 if the previous command failed.
- The user input displays in blue.
- The command output displays in the default color.

The default colors are sent by the terminal emulator software.

Procedure

	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.

This example shows how to display and filter module information:

```
switch# slot 27 show version | grep lc
```

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

```
switch# slot 27 quoted "show version" | diff
switch# slot 28 quoted "show version" | diff -c
*** /volatile/vsh_diff_1_root_8430_slot__quoted_show_version.old      Wed Apr 29 20:10:41
```

```

2013
--- - Wed Apr 29 20:10:41 2013
*****
*** 1,5 ****
! RAM 1036860 kB
! lc27
  Software
    BIOS:      version 6.20
    system:    version 6.1(2)I1(1) [build 6.1(2)]
--- 1,5 ----
! RAM 516692 kB
! lc28
  Software
    BIOS:      version 6.20
    system:    version 6.1(2)I1(1) [build 6.1(2)]
*****
*** 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)

```

Sending Command Output in Email

You can use the CLI to send the output of a **show** command to an email address using the pipe operator (`|`).



Note The email configuration remains persistent for all **show** command output until it is reconfigured.

When you upgrade from a release before Cisco NX-OS Release 9.3(3) to Cisco NX-OS Release 9.3(3) or later releases, email configuration will be missing. This is due to enabling DME functionality for this feature. To resolve this, you need to execute "no email" and reapply the entire email configuration.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	email Example: <pre>switch(config)# email switch(config-email)#</pre>	Enters email configuration mode.

	Command or Action	Purpose
Step 3	smtp-host <i>ip-address</i> smtp-port <i>port</i> Example: <pre>switch(config-email)# smtp-host 198.51.100.1 smtp-port 25</pre>	Specifies the SMTP host IP address and the SMTP port number.
Step 4	vrf management Example: <pre>switch(config-email)# vrf management</pre>	Specifies a VRF for the email transmission.
Step 5	from <i>email-address</i> Example: <pre>switch(config-email)# from admin@Mycompany.com</pre>	Specifies the sender's email address.
Step 6	reply-to <i>email-address</i> Example: <pre>switch(config-email)# reply-to admin@Mycompany.com</pre>	Specifies the recipient's email address.
Step 7	exit Example: <pre>switch(config-email)# exit switch(config)#</pre>	Exits email configuration mode.
Step 8	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 9	show email Example: <pre>switch# show email</pre>	Displays the email configuration.
Step 10	<i>show-command</i> email subject <i>subject</i> <i>email-address</i> Example: <pre>switch# show interface brief email subject show-interface admin@Mycompany.com Email sent</pre>	Uses the pipe operator () to send the output of the specified show command with a subject to an email address.

BIOS Loader Prompt

When the supervisor modules power up, a specialized BIOS image automatically loads and tries to locate a valid nx-os image for booting the system. If a valid nx-os 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 9000 Series NX-OS Troubleshooting Guide*.

Examples Using the CLI

This section includes examples of using the CLI.

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 2013  rcfg.2013-05-01-12.27.59

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

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

```

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)#

```

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

```

Sending Command Output in Email

This example shows how to send the output of the **show interface brief** command to an email address using the pipe operator (**|**):

```

switch<config># email
switch(config-email)# smtp-host 198.51.100.1 smtp-port 25
switch(config-email)# vrf management
switch(config-email)# from admin@Mycompany.com
switch(config-email)# reply-to admin@Mycompany.com
switch(config-email)# exit
switch(config)# exit
switch# show email
SMTP host: 198.51.100.1
SMTP port: 25
Reply to: admin@Mycompany.com
From: admin@Mycompany.com
VRF: management
switch# show interface brief | email subject show-interface admin@Mycompany.com

Email sent

```

The email sent to **admin@Mycompany.com** with the subject "show-interface" shows the output of the command:

<snip>

```
Ethernet  VLAN Type Mode   Status Reason           Speed   Port
Interface                                     -----
Eth1/1    --  eth  trunk  up    none                10G (D)  --
Eth1/2    --  eth  routed down  Link not connected auto (D)  --
Eth1/3    --  eth  routed up   none                10G (D)  --
Eth1/4    --  eth  routed down  Link not connected auto (D)  --
Eth1/5    --  eth  routed down  Link not connected auto (D)  --
Eth1/6    --  eth  routed down  Link not connected auto (D)  --
Eth1/7    --  eth  routed down  Link not connected auto (D)  --
Eth1/8    --  eth  routed down  Link not connected auto (D)  --
Eth1/9    --  eth  routed down  Link not connected auto (D)  --
Eth1/10   --  eth  routed down  Link not connected auto (D)  --
<snip>
```




CHAPTER 6

Configuring Terminal Settings and Sessions

This chapter contains the following sections:

- [About Terminal Settings and Sessions, on page 75](#)
- [Default Settings for File System Parameters, on page 76](#)
- [Configuring the Console Port, on page 76](#)
- [Configuring Virtual Terminals, on page 78](#)
- [Clearing Terminal Sessions, on page 79](#)
- [Displaying Terminal and Session Information, on page 80](#)

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.

Virtual Terminals

You can use virtual terminal lines to connect to your 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.

Default Settings for File System Parameters

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

Table 16: Default File System Settings

Parameters	Default
Default filesystem	bootflash:

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
Step 2	line console Example: switch# line console switch(config-console)#	Enters console configuration mode.
Step 3	databits <i>bits</i> 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 <i>minutes</i> 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 9600.
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	(Optional) show line console Example: switch(config)# show line console	Displays the console settings.
Step 10	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	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 the device.

Procedure

	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 <i>minutes</i> 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	(Optional) show running-config all begin vty Example: switch(config)# show running-config all begin vty	Displays the virtual terminal configuration.
Step 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring the Session Limit

You can limit the number of virtual terminal sessions on your device.

Procedure

	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 your device. The range is from 1 to 64. The default is 32.
Step 4	exit Example: switch(config-line)# exit switch(config)#	Exits line configuration mode.
Step 5	(Optional) show running-config all being vty Example: switch(config)# show running-config all begin vty	Displays the virtual terminal configuration.
Step 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Clearing Terminal Sessions

You can clear terminal sessions on your device.

Procedure

	Command or Action	Purpose
Step 1	(Optional) show users Example: switch# show users	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.

	Command or Action	Purpose
--	-------------------	---------

Displaying Terminal and Session Information

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

Command	Purpose
show terminal	Displays terminal settings.
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.



CHAPTER 7

Basic Device Management

This chapter contains the following sections:

- [About Basic Device Management, on page 81](#)
- [Default Settings for Basic Device Parameters, on page 82](#)
- [Changing the Device Hostname, on page 82](#)
- [Configuring the MOTD Banner, on page 83](#)
- [Configuring the Time Zone, on page 84](#)
- [Configuring Summer Time \(Daylight Saving Time\), on page 85](#)
- [Manually Setting the Device Clock, on page 86](#)
- [Setting the Clock Manager, on page 86](#)
- [Managing Users, on page 87](#)
- [Verifying the Device Configuration, on page 88](#)

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.

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 NX-OS device might contain clocks of different types that might need to be synchronized. These clocks are a part of various components (such as the supervisor, line card processors, or line cards), and each might 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 9000 Series NX-OS Security Configuration Guide*.

Default Settings for Basic Device Parameters

This table lists the default settings for basic device parameters.

Table 17: Default Basic Device Parameters

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

Changing the Device Hostname

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

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	<p>{ hostname switchname } <i>name</i></p> <p>Example:</p> <p>Using the hostname command:</p> <pre>switch(config)# hostname Engineering1 Engineering1(config)#</pre> <p>Using the switchname command:</p> <pre>Engineering1(config)# switchname Engineering2 Engineering2(config)#</pre>	<p>Changes the device hostname. The <i>name</i> argument is alphanumeric and case sensitive. The default is switch.</p> <p>Note The switchname command performs the same function as the hostname command. Beginning with Cisco NX-OS Release 7.0(3)I7(3), a maximum length of 63 characters for the switchname is supported.</p>
Step 3	<p>exit</p> <p>Example:</p> <pre>Engineering2(config)# exit Engineering2#</pre>	Exits global configuration mode.
Step 4	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>Engineering2# copy running-config startup-config</pre>	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

Procedure

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>banner motd <i>delimiting-character message delimiting-character</i></p> <p>Example:</p> <pre>switch(config)# banner motd #Welcome to the Switch# switch(config)#</pre>	<p>Configures the MOTD banner. Do not use the <i>delimiting-character</i> in the <i>message</i> text.</p> <p>Note Do not use " or % as a delimiting character.</p>

	Command or Action	Purpose
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	(Optional) show banner motd Example: switch# show banner motd	Displays the configured MOTD banner.
Step 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring the Time Zone

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

Procedure

	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 <i>zone-name</i> argument is a 3-character string for the time zone acronym (for example, PST or EST). The <i>offset-hours</i> argument is the offset from the UTC and the range is from -23 to 23 hours. The range for the <i>offset-minutes</i> argument is from 0 to 59 minutes.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	(Optional) show clock Example: switch# show clock	Displays the time and time zone.
Step 5	(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	switch# copy running-config startup-config	

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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: <pre>switch(config)# clock summer-time PDT 1 Sunday March 02:00 1 Sunday November 02:00 60</pre>	<p>Configures summer time or daylight saving time.</p> <p>The <i>zone-name</i> argument is a three character string for the time zone acronym (for example, PST and EST).</p> <p>The values for the <i>start-day</i> and <i>end-day</i> arguments are Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.</p> <p>The values for the <i>start-month</i> and <i>end-month</i> arguments are January, February, March, April, May, June, July, August, September, October, November, and December.</p> <p>The value for the <i>start-time</i> and <i>end-time</i> arguments are in the format <i>hh:mm</i>.</p> <p>The range for the <i>offset-minutes</i> argument is from 0 to 1440 minutes.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	(Optional) show clock detail Example: <pre>switch(config)# show clock detail</pre>	Displays the configured MOTD banner.
Step 5	(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	switch# copy running-config startup-config	

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.

Procedure

	Command or Action	Purpose
Step 1	clock set <i>time day month year</i> Example: switch# clock set 15:00:00 30 May 2013 Fri May 30 15:14:00 PDT 2013	Configures the device clock. The format for the <i>time</i> argument is <i>hh:mm:ss</i> . The range for the <i>day</i> argument is from 1 to 31. The values for the <i>month</i> argument are January, February, March, April, May, June, July, August, September, October, November, and December . The range for the <i>year</i> argument is from 2000 to 2030.
Step 2	(Optional) show clock Example: switch(config)# show clock	Displays the current clock value.

Setting the Clock Manager

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

Procedure

	Command or Action	Purpose
Step 1	clock protocol <i>protocol</i> Example: switch# clock protocol ntp	Configures the clock manager. The values for the <i>protocol</i> argument are ntp , ptp , and none . The following describes the values:

	Command or Action	Purpose
		<ul style="list-style-type: none"> • ntp—Synchronizes clocks with Network Time Protocol (NTP). • ptp—Synchronizes clocks with Precision Time Protocol (PTP) as described by IEEE 1588. • none—Uses clock set HH:MM:SS to set the supervisor clock. <p>Note When none is used, the clock must be configured.</p> <p>Note Once the protocol is configured, the clock must use that protocol.</p>
Step 2	(Optional) show run clock_manager Example: <pre>switch# show run clock_manager</pre>	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.

Procedure

	Command or Action	Purpose
Step 1	show users Example: <pre>switch# show users</pre>	Displays the user sessions.

Sending a Message to Users

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

Procedure

	Command or Action	Purpose
Step 1	(Optional) show users Example: switch# show users	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, use one of the following commands:

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

This option masks the sensitive words in running configuration output with <removed> keyword.



CHAPTER 8

Using the Device File Systems, Directories, and Files

This chapter contains the following sections:

- [About the Device File Systems, Directories, and Files, on page 89](#)
- [Default Settings for File System Parameters, on page 91](#)
- [Configuring the FTP, HTTP, or TFTP Source Interface, on page 91](#)
- [Working with Directories, on page 91](#)
- [Working with Files, on page 94](#)
- [Working with Archive Files, on page 98](#)
- [Examples of Using the File System, on page 101](#)

About the 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 18: 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 (usb1: and usb2:). You can navigate through these directories and use them for files.

Files

You create and access files on bootflash:, volatile:, usb1:, and usb2: filesystems. You can only access files on the system: filesystem. You can use the log: filesystem for debug log files.

You can download files, such as the nx-os image file, 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.

Default Settings for File System Parameters

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

Table 19: Default File System Settings

Parameters	Default
Default filesystem	bootflash:

Configuring the FTP, HTTP, or TFTP Source Interface

You can configure the source interface for the File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), or Trivial File Transfer Protocol (TFTP). This configuration allows you to use the IP address associated with the configured source interface when copy packets are transferred.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] ip {ftp http tftp} source-interface {ethernet slot/port loopback number} Example: <pre>switch(config)# ip tftp source-interface ethernet 2/1</pre>	Configures the source interface for all FTP, HTTP, or TFTP packets.
Step 3	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

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.

Procedure

	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:.

Procedure

	Command or Action	Purpose
Step 1	(Optional) pwd Example: switch# pwd	Displays the name of your current default directory.
Step 2	cd { <i>directory</i> <i>filesystem:[//module/][directory]</i> } Example: switch# cd usb1:	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.

Procedure

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

Displaying Directory Contents

You can display the contents of a directory.

Procedure

	Command or Action	Purpose
Step 1	dir [<i>directory</i> <i>filesystem</i> : <i>[/module/][directory]</i>] 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.

Procedure

	Command or Action	Purpose
Step 1	(Optional) pwd Example: switch# pwd	Displays the name of your current default directory.
Step 2	(Optional) dir [<i>filesystem</i> : <i>[/module/][directory]</i>] Example: switch# dir bootflash:test	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 [<i>filesystem</i> : <i>[/module/]</i>] <i>directory</i> 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.

Procedure

	Command or Action	Purpose
Step 1	(Optional) pwd Example: switch# pwd	Displays the name of your current default directory.
Step 2	(Optional) dir [filesystem:[/module/][directory]] Example: switch# dir bootflash	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 <i>target-filename</i> argument is alphanumeric, case sensitive, and has a maximum of 64 characters. If the <i>target-filename</i> argument is not specified, the filename defaults to the <i>source-filename</i> argument value.

Copying Files

You can make copies of files, either within the same directory or on another directory. For more information, see the *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*.



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.

Procedure

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

Deleting Files

You can delete a file from a directory.

Procedure

	Command or Action	Purpose
Step 1	(Optional) dir [<i>filesystem:[//module][directory]</i>] Example: switch# dir bootflash:	Displays the contents of the current directory. The file system and directory name are case sensitive.
Step 2	delete { <i>filesystem:[//module][directory]</i> } [<i>directory</i>]} <i>filename</i> Example: switch# delete bootflash:old_config.cfg	Deletes a file. The file system, module, and directory names are case sensitive. The <i>source-filename</i> 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.

Procedure

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

Displaying File Checksums

You can display checksums to check the file integrity.

Procedure

	Command or Action	Purpose
Step 1	show file <i>[filesystem:[//module/]][directory/]filename</i> {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 device using Lempel-Ziv 1977 (LZ77) coding.

Procedure

	Command or Action	Purpose
Step 1	(Optional) dir <i>[filesystem:[//module/]directory]</i> Example: switch# dir bootflash:	Displays the contents of the current directory. The file system and directory name are case sensitive.
Step 2	gzip <i>[filesystem:[//module/]][directory/] directory/]filename</i> Example: switch# gzip show_tech	Compresses a file. After the file is compressed, it has a .gz suffix.
Step 3	gunzip <i>[filesystem:[//module/]][directory/] directory/]filename .gz</i> 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.

Procedure

	Command or Action	Purpose
Step 1	tail [<i>filesystem:[//module/]</i>][<i>directory/</i>] <i>filename</i> [<i>lines</i>] 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:, volatile:, or a remote server. You can also specify the format for the command output.

Procedure

	Command or Action	Purpose
Step 1	(Optional) terminal redirection-mode { ascii zipped } Example: switch# terminal redirection-mode zipped	Sets the redirection mode for the show command output for the user session. The default mode is ascii .
Step 2	show-command > <i>[filesystem:[//module/]</i> [<i>directory</i>] [<i>directory</i> <i>/</i>] <i>filename</i> 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.

Procedure

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

	Command or Action	Purpose
Step 2	(Optional) <code>cd {filesystem:[//module/][directory] directory}</code> Example: switch# cd bootflash:test_scripts	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.

Formatting the Bootflash

Use the **format bootflash:** CLI command to format the onboard flash memory (bootflash:). If the command errors out due to the `Deactivate all virtual-services and try again` error message, destroy the Guest Shell using the **guestshell destroy** CLI command and rerun the **format bootflash:** command, for example,

```
switch# sh virtual-service list
Virtual Service List:

Name                               Status           Package Name
-----
guestshell+                         Activated        guestshell.ova

switch#

switch# guestshell destroy
You are about to destroy the guest shell and all of its contents. Be sure to save your
work. Are you sure you want to continue? (y/n) [n] y

switch# 2018 Jan 17 18:42:24 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Deactivating
virtual service 'guestshell+'

switch#format bootflash:
```

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 File

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`.

Procedure

	Command or Action	Purpose
Step 1	<p>tar create {bootflash: volatile:} <i>archive-filename</i> [absolute] [bz2-compress] [gz-compress] [remove] [uncompressed] [verbose] <i>filename-list</i></p> <p>Example:</p> <pre>switch# tar create bootflash:config-archive gz-compress bootflash:config-file</pre>	<p>Creates an archive file and adds files to it. The filename is alphanumeric, not case sensitive, and has a maximum length of 240 characters.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • For bz2-compress, the extension is <code>.tar.bz2</code>. • For gz-compress, the extension is <code>.tar.gz</code>. • For uncompressed, the extension is <code>.tar</code>. <p>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.</p> <p>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.</p>

Appending Files to an Archive File

You can append files to an existing archive file on your device.

Before you begin

You have created an archive file on your device.

Procedure

	Command or Action	Purpose
Step 1	tar append {bootflash: volatile:}archive-filename [absolute] [remove] [verbose]filename-list	<p>Adds files to an existing archive file. The archive filename is not case sensitive.</p> <p>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.</p> <p>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.</p> <p>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.</p>

Example

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 device.

Before you begin

You have created an archive file on your device.

Procedure

	Command or Action	Purpose
Step 1	tar extract {bootflash: volatile:}archive-filename [keep-old] [screen] [to {bootflash: volatile:}[/directory-name]] [verbose] Example: <pre>switch# tar extract bootflash:config-archive.tar.gz</pre>	<p>Extracts files from an existing archive file. The archive filename is not case sensitive.</p> <p>The keep-old keyword indicates that the Cisco NX-OS software should not overwrite files with the same name as the files being extracted.</p> <p>The screen keyword indicates that the Cisco NX-OS software should not overwrite files with the same name as the files being extracted.</p> <p>The to keyword specifies the target filesystem. You can include a directory name. The directory</p>

	Command or Action	Purpose
		<p>name is alphanumeric, case sensitive, and has a maximum length of 240 characters.</p> <p>The verbose keyword specifies that the Cisco NX-OS software should display the names of the files as they are extracted.</p>

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 examples of how to use 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
 4096   Oct 03 23:55:55 2013  .patch/
...
 16384   Jan 01 13:23:30 2011  lost+found/
297054208 Oct 21 18:55:36 2013  n9000-dk9.6.1.2.I1.1.bin
...
```

```
Usage for bootflash://sup-remote
1903616000 bytes used
19234234368 bytes free
21137850368 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 usb1:samplefile usb1: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 usb1: file system to the mystorage directory:

```
switch# copy usb1:samplefile usb1: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:nx-os-image bootflash://sup-2/nx-os-image
```

This example shows how to overwrite the contents of an existing configuration in NVRAM:

```
switch# copy nvram:snapshot-config nvram:startup-config
```

```
Warning: this command is going to overwrite your current startup-config:
Do you wish to continue? {y/n} [y] y
```

You can also use the **copy** command to upload and download files from the 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.

Procedure

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

	Command or Action	Purpose
Step 2	(Optional) dir [<i>filesystem</i> : <i>//module</i>][<i>directory</i>] Example: switch# dir bootflash:test	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 [<i>filesystem</i> : <i>//module</i>][<i>directory</i>] 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 usb1: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 2013 Samplefile
...
switch# gzip volatile:Samplefile
switch# dir
```

```

    266069      Jul 04 00:51:03 2013 Samplefile.gz
...

```

This example shows how to uncompress a compressed file:

```

switch# dir
    266069      Jul 04 00:51:03 2013 Samplefile.gz
...
switch# gunzip samplefile
switch# dir
    1525859     Jul 04 00:51:03 2013 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 > usb1: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 2013 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

```



CHAPTER 9

Working with Configuration Files

This chapter contains the following sections:

- [About Configuration Files, on page 105](#)
- [Guidelines and Limitations for Configuration Files, on page 106](#)
- [Managing Configuration Files, on page 106](#)
- [Configuration Archive and Configuration Log, on page 115](#)
- [Verifying the Device Configuration, on page 119](#)
- [Examples of Working with Configuration Files, on page 119](#)

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 106

[Downloading the Startup Configuration From a Remote Server](#), on page 108

Guidelines and Limitations for Configuration Files

Configuration file guidelines and limitations are as follows:

- Beginning with NX-OS 7.0(3)I7(4), the **reload timer** command is supported to enable a reboot after a delay of 5 -60 seconds.

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.

Procedure

	Command or Action	Purpose
Step 1	(Optional) show running-config Example: switch# show running-config	Displays the running configuration.
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.

Procedure

	Command or Action	Purpose
Step 1	copy running-config <i>scheme://server</i>[<i>url</i> /]<i>filename</i> Example:	Copies the running-configuration file to a remote server. For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the

	Command or Action	Purpose
	<pre>switch# copy running-config tftp://10.10.1.1/sw1-run-config.bak</pre>	<p>address or name of the remote server, and the <i>url</i> argument is the path to the source file on the remote server.</p> <p>The <i>server</i>, <i>url</i>, and <i>filename</i> arguments are case sensitive.</p>
Step 2	<p>copy startup-config <i>scheme://server/[url]/filename</i></p> <p>Example:</p> <pre>switch# copy startup-config tftp://10.10.1.1/sw1-start-config.bak</pre>	<p>Copies the startup-configuration file to a remote server.</p> <p>For the <i>scheme</i> argument, you can enter tftp:, ftp:, scp:, or sftp:. The <i>server</i> argument is the address or name of the remote server, and the <i>url</i> argument is the path to the source file on the remote server.</p> <p>The <i>server</i>, <i>url</i>, and <i>filename</i> arguments are case sensitive.</p>

Example

This example shows how to copy the configuration file to a remote server:

```
switch# copy running-config
tftp://10.10.1.1/sw1-run-config.bak
switch# copy startup-config
tftp://10.10.1.1/sw1-start-config.bak
```

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 device has a route to the remote server. Your 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.

Procedure

	Command or Action	Purpose
Step 1	<pre>copy scheme://server/[url]/filename running-config</pre>	Downloads the running-configuration file from a remote server.

	Command or Action	Purpose
	Example: <pre>switch# copy tftp://10.10.1.1/my-config running-config</pre>	For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the address or name of the remote server, and the <i>url</i> argument is the path to the source file on the remote server. The <i>server</i> , <i>url</i> , and <i>filename</i> arguments are case sensitive.
Step 2	(Optional) show running-config Example: <pre>switch# show running-config</pre>	Displays the running configuration.
Step 3	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.
Step 4	(Optional) show startup-config Example: <pre>switch# show startup-config</pre>	Displays the startup configuration.

Related Topics

[Copying Files](#), on page 102

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 device has a route to the remote server. Your 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.

Procedure

	Command or Action	Purpose
Step 1	write erase Example: <pre>switch# write erase</pre>	Erases the startup configuration file.
Step 2	reload Example: <pre>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#</pre>	Reloads the Cisco NX-OS device. Note Do not use the setup utility to configure the device.
Step 3	copy <i>scheme://server/[url /]filename</i> running-config Example: <pre>switch# copy tftp://10.10.1.1/my-config running-config</pre>	Downloads the running configuration file from a remote server. For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the address or name of the remote server, and the <i>url</i> argument is the path to the source file on the remote server. The <i>server</i> , <i>url</i> , and <i>filename</i> arguments are case sensitive.
Step 4	copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Saves the running configuration file to the startup configuration file.
Step 5	(Optional) show startup-config Example: <pre>switch# show startup-config</pre>	Displays the running configuration.

Related Topics

[Copying Files](#), on page 102

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.

Procedure

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

Related Topics

[Copying Files](#), on page 102

Copying the Running Configuration from an External Flash Memory Device

You can configure your 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.

Procedure

	Command or Action	Purpose
Step 1	(Optional) dir {usb1: usb2:}[<i>directory/</i>] Example: switch# dir usb1:	Displays the files on the external flash memory device.
Step 2	copy {usb1: usb2:}[<i>directory/</i>] <i>filename</i> running-config Example: switch# copy usb1:dsn-config.cfg running-config	Copies the running configuration from an external flash memory device. The <i>filename</i> argument is case sensitive.

	Command or Action	Purpose
Step 3	(Optional) show running-config Example: switch# show running-config	Displays the running configuration.
Step 4	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.
Step 5	(Optional) show startup-config Example: switch# show startup-config	Displays the startup configuration.

Related Topics

[Copying Files](#), on page 102

Copying the Startup Configuration From an External Flash Memory Device

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

Before you begin

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

Procedure

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

Related Topics

[Copying Files](#), on page 102

Copying Configuration Files to an Internal File System

You can copy configuration files to the internal memory as a backup for later use.

Procedure

	Command or Action	Purpose
Step 1	copy running-config [<i>filesystem:</i>][<i>directory/</i>] [<i>directory/</i>] <i>filename</i> Example: <pre>switch# copy running-config bootflash:sw1-run-config.bak</pre>	Copies the running-configuration file to internal memory. The <i>filesystem</i> , <i>directory</i> , and <i>filename</i> arguments are case sensitive.
Step 2	copy startup-config [<i>filesystem:</i>][<i>directory/</i>] [<i>directory/</i>] <i>filename</i> Example: <pre>switch# copy startup-config bootflash:sw1-start-config.bak</pre>	Copies the startup-configuration file to internal memory. The <i>filesystem</i> , <i>directory</i> , and <i>filename</i> arguments are case sensitive.

Related Topics

[Copying Files](#), on page 94

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.

Procedure

	Command or Action	Purpose
Step 1	write erase Example: <pre>switch# write erase</pre>	Clears the current configuration of the switch.
Step 2	reload Example: <pre>switch# reload</pre>	Restarts the device. You will be prompted to provide an nx-os image file for the device to boot and run.
Step 3	copy configuration-file running-configuration	Copies a previously saved configuration file to the running configuration.

	Command or Action	Purpose
	Example: switch# copy bootflash:start-config.bak running-configuration	Note The <i>configuration-file</i> 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.

Procedure

	Command or Action	Purpose
Step 1	(Optional) show hardware Example: switch# show hardware	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	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Erasing a Configuration

Procedure

	Command or Action	Purpose
Step 1	<p>write erase [boot debug]</p> <p>Example:</p> <pre>switch# write erase Warning: This command will erase the startup-configuration. Do you wish to proceed anyway? (y/n) [n] y</pre>	<p>Erases configurations in persistent memory. The default action erases the startup configuration.</p> <p>The boot option erases the boot variable definitions and the IPv4 configuration on the mgmt0 interface.</p> <p>The debug option erases the debugging configuration.</p> <p>Note The running-configuration file is not affected by this command.</p>

Clearing Inactive Configurations

You can clear inactive QoS and/or ACL configurations.

Procedure

	Command or Action	Purpose
Step 1	<p>(Optional) show running-config <i>type</i> inactive-if-config</p> <p>Example:</p> <pre># show running-config ipqos inactive-if-config</pre>	<p>Displays any inactive access control list (ACL) or quality of service (QoS) configurations.</p> <p>The values for the <i>type</i> argument are acmgr and ipqos.</p> <ul style="list-style-type: none"> • acmgr—Displays any inactive configurations for acmgr. • ipqos—Displays any inactive configurations for qosmgr.
Step 2	<p>clear inactive-config <i>policy</i></p> <p>Example:</p> <pre># 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 you can see the log file @ show inactive-if-config log</pre>	<p>Clears inactive configurations.</p> <p>The values for the <i>policy</i> argument are qos and acl.</p> <p>The following describes the values:</p> <ul style="list-style-type: none"> • qos—Clears inactive QoS configurations. • acl—Clears inactive ACL configurations. • acl qos—Clears inactive ACL configurations and inactive QoS configurations.

	Command or Action	Purpose
Step 3	(Optional) show inactive-if-config log Example: <code># show inactive-if-config log</code>	Displays the commands that were used to clear the inactive configurations.

Configuration Archive and Configuration Log

This section contains information on configuration archive and configuration log.

Information About Configuration Archive

The configuration archive is intended to provide a mechanism to store, organize, and manage an archive of the configuration files to enhance the configuration rollback capability provided by the **configure replace** command. Before configuration archiving was introduced, you could save copies of the running configuration using the **copy running-config destination-url** command, storing the replacement file either locally or remotely. However, this method lacked any automated file management. The configuration replace and configuration rollback provides the capability to automatically save copies of the running configuration to the configuration archive. These archived files serve as checkpoint configuration references and can be used by the **configure replace** command to revert to the previous configuration states.

The **archive config** command allows you to save configurations in the configuration archive using a standard location and filename prefix that is automatically appended with an incremental version number (and optional timestamp) as each consecutive file is saved. This functionality provides a means for consistent identification of saved configuration files. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved in the archive, the oldest file is automatically deleted when the next, most recent file is saved. The **show archive** command displays information for all configuration files saved in the configuration archive.

The configuration archive, wherein the configuration files are stored and are available for use with the **configure replace** command, can be located on the following file systems: bootflash, FTP, and TFTP.



Note The TFTP and FTP for this feature use VRF management.

Configuring the Characteristics of the Configuration Archive

Before using the **archive config** command, the configuration archive must be configured. Complete the following steps to configure the characteristics of the configuration archive:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example:	Enters the global configuration mode.

	Command or Action	Purpose
	<code>switch# configure terminal</code>	
Step 2	archive Example: <code>switch(config)# archive</code>	Enters the archive configuration mode. Note This command does not apply to Cisco Nexus 9300-EX, -FX, and -R Series switches.
Step 3	path <i>url</i> Example: <code>switch(config-archive)# path bootflash:myconfig</code>	Specifies the location and the filename prefix for the files in the configuration archive. <ul style="list-style-type: none"> Depending on your hardware platform, the name of your file system can be different than the one displayed in the example. Note If a directory is specified in the path instead of the file, the directory name must be followed by a forward slash as follows: <code>path flash:/directory/</code> . The forward slash is not necessary after a filename; it is necessary only when specifying a directory.
Step 4	maximum <i>number</i> Example: <code>switch(config-archive)# maximum 14</code>	(Optional) Sets the maximum number of archive files of the running configuration to be saved in the configuration archive. <ul style="list-style-type: none"> The <i>number</i> is the maximum number of the archive files of the running configuration that can be saved in the configuration archive. The range is 1 to 14. The default is 10. Note Before using this command, you must configure the path to specify the location and filename prefix for the files in the configuration archive.
Step 5	time-period <i>minutes</i> Example: <code>switch(config-archive)# time-period 10</code>	(Optional) Sets the time increment for automatically saving an archive file of the current running configuration in the configuration archive. <ul style="list-style-type: none"> The <i>minutes</i> argument specifies how often, in minutes, to automatically save an archive file of the current running configuration in the configuration archive.

	Command or Action	Purpose
		<p>Note Before using this command, you must configure the path command to specify the location and filename prefix for the files in the configuration archive.</p>
Step 6	<p>write-memory</p> <p>Example:</p> <pre>switch(config-archive)# write-memory</pre>	Enables the command. It is disabled by default. Entering this command causes an archive to occur when the command copy r s is performed.
Step 7	<p>archive config</p> <p>Example:</p> <pre>switch(config-archive)# archive config</pre>	<p>Saves the current running configuration file to the configuration archive.</p> <p>Note You must configure the path before using the archive config command.</p>
Step 8	<p>(Optional) show archive log config all</p> <p>Example:</p> <pre>switch# show archive log config all</pre>	Displays the configuration log entries for all the users.

Information About Configuration Log

The configuration change logging tracks the changes that are made to the running configuration by using the data in the accounting log. This configuration log tracks the changes that are initiated only through the CLI. Only complete commands that result in the invocation of action routines are logged. The following types of entries are not logged:

- Commands that result in a syntax error message
- Partial commands that invoke the device help system

The configuration log tracks the changes that are initiated only through the CLI. For each configuration command that is executed, the following information is logged:

- A configuration change sequence number
- The line from which the command was executed
- The name of the user that executed the command
- The command that was executed

You can display the information from the configuration log by using the **show archive log config all** command. For each configuration command that is executed, the following information is logged:

- The command that was executed
- The name of the user that executed the command
- A configuration change sequence number

You can display the information from the configuration log by using the **show archive log config** command.

Displaying Configuration Log Entries

To display the configuration log entries, the configuration change logging provides the **show archive log config all** command.

Procedure

Step 1 switch# show archive log config all

Displays the configuration log entries for all users

Example:

```
switch# show archive log config all
```

INDEX	LINE	USER	LOGGED COMMAND
1	console0	user01	logging console 1
2	console0	user01	logging monitor 2
3	console0	user02	system default switchport shutdown
4	console0	user02	interface mgmt0
5	console0	user02	no shutdown

Step 2 switch# show archive log config user *username*

Displays the configuration log entries for the specified username.

Example:

The following example displays the configuration log entries for a specified username.

```
switch# show archive log config user user02
```

INDEX	LINE	USER	LOGGED COMMAND
3	console0	user02	system default switchport shutdown
4	console0	user02	interface mgmt0
5	console0	user02	no shutdown

Step 3 switch# show archive log config user *username* first-index *start-number* [last-index *end-number*]

Displays the configuration log entries by the index numbers. If you specify a number for the optional last-index, all the log entries with the index numbers in the range from the value entered for the start-number through the end-number for the specified user are displayed.

Example:

The following example displays the configuration log entry numbers 4 and 5 for a user with the username, user02. The range for the first-index and last-index is 1 to 2000000000.

```
switch# show archive log config user user02 first-index 4 last-index 5
Last Log cleared/wrapped time is : Wed Oct 19 00:53:08 2016
```

INDEX	LINE	USER	LOGGED COMMAND
4	console0	user02	interface mgmt0
5	console0	user02	no shutdown

Verifying the Device Configuration

To verify the configuration, use one of the following commands:

Command	Purpose
<code>show running-config</code>	Displays the running configuration.
<code>show startup-config</code>	Displays the startup configuration.

This option masks the sensitive words in running configuration output with <removed> keyword.

Examples of Working with Configuration Files

This section includes examples of working with configuration files.

Copying Configuration Files

This example shows how to overwrite the contents of an existing configuration in NVRAM:

```
switch# copy nvram:snapshot-config nvram:startup-config
Warning: this command is going to overwrite your current startup-config.
Do you wish to continue? {y/n} [y] y
```



Note This command does not apply to Cisco Nexus 9300-EX Series switches.

This example shows how to copy a running configuration to the bootflash: file system:

```
switch# copy system:running-config bootflash:my-config
```

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.
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.



INDEX

A

alias [54](#)

B

banner motd [83](#)
binary-location [39](#)
bootflash [90](#)

C

cd [92, 98](#)
clear inactive-config [114](#)
clear line [79](#)
cli alias name [54](#)
cli var name [52](#)
clock [57](#)
clock protocol none [86](#)
clock protocol ntp [86](#)
clock protocol ptp [86](#)
clock set [57, 86–87](#)
clock summer-time [85](#)
clock timezone [84](#)
configure [49](#)
copy [95, 109, 112](#)
copy {usb1 | usb2} [111](#)
copy ftp [108–109](#)
copy nvram [119](#)
copy running-config [112](#)
copy running-config {usb1 | usb2} [110](#)
copy running-config ftp [106](#)
copy running-config scp [106](#)
copy running-config sftp [106](#)
copy running-config tftp [106](#)
copy scp [108–109](#)
copy sftp [108–109](#)
copy startup-config [112](#)
copy startup-config {usb1 | usb2} [110](#)
copy startup-config ftp [107](#)
copy startup-config scp [107](#)
copy startup-config sftp [107](#)
copy startup-config tftp [107](#)
copy system [119](#)
copy tftp [108–109](#)

copy usb1 | usb2 [110](#)

D

databits [77](#)
debug [90](#)
diff-clean [61](#)
diff-clean all-sessions [61](#)
diff-clean all-users [61](#)
dir [94–96](#)
dir usb1 [110–111](#)
dir usb2 [110–111](#)

E

echo [56](#)
echo backslash-interpret [56](#)
egrep [62](#)
email [68](#)
end [44](#)
exec-timeout [77–78](#)

F

find [98](#)
from [69](#)

G

grep [62](#)
gunzip [96](#)
gzip [96](#)

H

hostname [83](#)

I

interface [43–44](#)
ip {ftp | http | tftp} source-interface {ethernet | loopback} [91](#)

L

less [62](#)
 line console [77](#)
 line vty [78–79](#)
 log [90](#)

M

mkdir [92](#)
 move [94](#)

P

parity {even | none | odd} [77](#)
 persist [66](#)
 personality [38](#)
 personality backup [37](#)
 ping [107–108](#)
 ping6 [107–108](#)
 pop [44](#)
 purge module [113](#)
 push [44](#)
 pwd [92, 95, 97](#)

R

reload [109, 112, 120](#)
 reply-to [69](#)
 rmdir [93, 103](#)
 run-script [55](#)

S

sed [63](#)
 send [88](#)
 session-limit [79](#)
 set [57](#)
 show [58–59, 61, 63–64, 70](#)
 show banner motd [84](#)
 show cli history [65–66](#)
 show cli variables [52–53](#)
 show clock [84, 86](#)
 show clock detail [85](#)
 show email [69](#)
 show file [96](#)
 show hardware [113](#)
 show inactive-if-config log [115](#)
 show interface brief [72](#)

show line [80](#)
 show line console [77](#)
 show run clock_manager [87](#)
 show running-config [36, 88, 106, 108, 111, 114, 119](#)
 show startup-config [36, 88, 109, 111, 119](#)
 show terminal [80](#)
 show users [79–80, 87–88](#)
 sleep [56](#)
 slot [67](#)
 smtp-host [69](#)
 smtp-port [69](#)
 sort [63](#)
 speed [77](#)
 ssh name [61](#)
 stopbits [77](#)
 switchname [83](#)
 system [90](#)

T

tail [97](#)
 tar append bootflash [100](#)
 tar append volatile [100](#)
 tar create bootflash [99](#)
 tar create volatile [99](#)
 tar extract {bootflash | volatile} [100](#)
 tar list bootflash [101](#)
 tar list volatile [101](#)
 terminal alias [55](#)
 terminal color [67](#)
 terminal dont-ask [66](#)
 terminal edit-mode vi [65](#)
 terminal output xml [60](#)
 terminal redirection-mode ascii [97](#)
 terminal redirection-mode zipped [97](#)
 track [38](#)

V

volatile [90](#)
 vrf management [69](#)

W

where detail [50](#)
 write erase [109, 112, 120](#)
 write erase boot [114](#)
 write erase debug [114](#)