



## **Cisco Nexus 5000 Series NX-OS Fundamentals Configuration Guide, Release 5.2(1)N1(1)**

**First Published:** 2012-07-02

**Last Modified:** 2017-10-30

### **Americas Headquarters**

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

Text Part Number: OL-27538-01



# CONTENTS

## PREFACE

### Preface xiii

Audience xiii

Document Conventions xiii

Documentation Feedback xiv

Communications, Services, and Additional Information xiv

## CHAPTER 1

### New and Changed Information for this Release 1

## CHAPTER 2

### Overview 3

Fibre Channel over Ethernet 3

Data Center I/O Consolidation 3

Virtual Interfaces 4

Typical Deployment Topologies 5

Ethernet Switching 5

FCoE and Fibre Channel Switching 5

QoS 5

Virtual Port Channels 6

Serviceability 6

Switched Port Analyzer 6

Ethalyzer 6

Call Home 6

Online Diagnostics 6

Switch Management 7

Simple Network Management Protocol 7

Role-Based Access Control 7

Configuration Methods	7
Network Security Features	7
Virtual Device Contexts	8
Licensing	8
Ethernet TOR Switch Topology	8
Fabric Extender Deployment Topology	9
Data Center I/O Consolidation Topology	9
Supported Standards	10

---

## CHAPTER 3

### Using the Cisco NX-OS Setup Utility 13

Configuring the Switch	13
Image Files on the Switch	13
Starting the Switch	13
Boot Sequence	13
Console Settings	14
Upgrading the Switch Software	15
Downgrading from a Higher Release	16
Initial Configuration	18
Configuration Prerequisites	18
Initial Setup	18
Preparing to Configure the Switch	19
Default Login	19
Configuring the Switch	19
Changing the Initial Configuration	24
Management Interface Configuration	24
About the mgmt0 Interface	24
Configuring the Management Interface	24
Displaying Management Interface Configuration	26
Shutting Down the Management Interface	26

---

## CHAPTER 4

### Using PowerOn Auto Provisioning 27

Guidelines and Limitations for POAP	27
Setting Up the Network Environment To Use POAP	28
Configuring a Switch Using POAP	29

Verifying the Device Configuration	29
Related Documents for POAP	30

---

**CHAPTER 5**

<b>Understanding the Command-Line Interface</b>	<b>31</b>
Finding Feature Information	31
Information About the CLI Prompt	32
Command Modes	32
EXEC Command Mode	32
Global Configuration Command Mode	33
Interface Configuration Command Mode	33
Subinterface Configuration Command Mode	34
Saving and Restoring a Command Mode	34
Exiting a Configuration Command Mode	35
Command Mode Summary	35
Special Characters	36
Keystroke Shortcuts	36
Abbreviating Commands	38
Completing a Partial Command Name	39
Identifying Your Location in the Command Hierarchy	39
Using the no Form of a Command	40
Configuring CLI Variables	41
About CLI Variables	41
Configuring CLI Session-Only Variables	42
Configuring Persistent CLI Variables	42
Command Aliases	43
About Command Aliases	43
Defining Command Aliases	44
Configuring Command Aliases for a User Session	44
Command Scripts	45
Running a Command Script	45
Echoing Information to the Terminal	45
Delaying Command Action	46
Context-Sensitive Help	47
Understanding Regular Expressions	48

Special Characters	48
Multiple-Character Patterns	49
Anchoring	49
Searching and Filtering show Command Output	50
Filtering and Searching Keywords	50
diff Utility	52
grep and egrep Utilities	52
less Utility	53
sed Utility	53
sort Utility	53
Searching and Filtering from the --More-- Prompt	54
Using the Command History	55
Recalling a Command	55
Controlling CLI History Recall	56
Configuring the CLI Edit Mode	56
Displaying the Command History	56
Enabling or Disabling the CLI Confirmation Prompts	57
Setting CLI Display Colors	57
Sending Commands to Modules	57
BIOS Loader Prompt	58
Examples Using the CLI	59
Defining Command Aliases	59
Using CLI Session Variables	59
Using the System-Defined Timestamp Variable	60
Running a Command Script	60
Additional References for the CLI	61
Related Documents for the CLI	61

---

## CHAPTER 6

### Configuring Terminal Settings and Sessions 63

Finding Feature Information	63
Information About Terminal Settings and Sessions	63
Terminal Session Settings	63
Console Port	64
COM1 Port	64

Virtual Terminals	64
Modem Support	65
Configuring the Console Port	65
Configuring the COM1 Port	67
Configuring Virtual Terminals	69
Configuring the Inactive Session Timeout	69
Configuring the Session Limit	70
Configuring Modem Connections	71
Enabling a Modem Connection	71
Downloading the Default Initialization String	72
Configuring and Downloading a User-Specified Initialization String	73
Initializing a Modem for a Powered-Up Cisco NX-OS Device	75
Clearing Terminal Sessions	75
Displaying Terminal and Session Information	76
Default Settings for File System Parameters	76
Additional References for Terminal Settings and Sessions	76
Related Documents for Terminal Settings and Sessions	76

---

**CHAPTER 7**
**Basic Device Management 77**

Finding Feature Information	77
Default Settings for Basic Device Parameters	77
Information About Basic Device Management	78
Device Hostname	78
Message-of-the-Day Banner	78
EXEC Banner	78
Device Clock	78
Clock Manager	78
Time Zone and Summer Time (Daylight Saving Time)	78
User Sessions	79
Changing the Device Hostname	79
Configuring the MOTD Banner	80
Configuring the EXEC Banner	81
Configuring the Time Zone	82
Configuring Summer Time (Daylight Saving Time)	83

Manually Setting the Device Clock	84
Setting the Clock Manager	85
Managing Users	85
Displaying Information about the User Sessions	86
Sending a Message to Users	86
Verifying the Device Configuration	86
Additional References for Basic Device Management	87
Related Documents for Basic Device Management	87

---

## CHAPTER 8

<b>Using the Device File Systems, Directories, and Files</b>	<b>89</b>
Finding Feature Information	89
Information About Device File Systems, Directories, Files, and External Storage Devices	89
File Systems	89
Directories	90
Files	90
Working with Directories	91
Identifying the Current Directory	91
Changing the Current Directory	91
Creating a Directory	91
Displaying Directory Contents	92
Deleting a Directory	92
Accessing the Directories on a Standby Supervisor Module	93
Working with Files	93
Moving Files	93
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
Working with Archive Files	98
Creating an Archive Files	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 a File System	101
Accessing Directories on a Standby Supervisor Module	101
Moving Files	102
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
Default Settings for File System Parameters	105
Additional References for File Systems	105
Related Documents for File Systems	105

---

**CHAPTER 9**

<b>Working with Configuration Files</b>	<b>107</b>
Finding Feature Information	107
Information About Configuration Files	107
Types of Configuration Files	107
Managing Configuration Files	108
Saving the Running Configuration to the Startup Configuration	108
Copying a Configuration File to a Remote Server	108
Downloading the Running Configuration From a Remote Server	109
Downloading the Startup Configuration From a Remote Server	110
Copying Configuration Files to an External Flash Memory Device	111
Copying the Running Configuration from an External Flash Memory Device	112
Copying the Startup Configuration from an External Flash Memory Device	113
Copying Configuration Files to an Internal File System	114
Rolling Back to a Previous Configuration	114
Removing the Configuration for a Missing Module	115
Erasing a Configuration	116
Clearing Inactive Configurations	117



Verifying the Device Configuration	118
Examples of Working with Configuration Files	118
Copying Configuration Files	118
Backing Up Configuration Files	118
Rolling Back to a Previous Configuration	119
Additional References for Configuration Files	119
Related Documents for Configuration Files	119



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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For 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 standards documentation, or language that is used by a referenced third-party product.

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

© 2012–2017 Cisco Systems, Inc. All rights reserved.





## Preface

The preface contains the following sections:

- [Audience, on page xiii](#)
- [Document Conventions, on page xiii](#)
- [Documentation Feedback, on page xiv](#)
- [Communications, Services, and Additional Information, on page xiv](#)

## Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices.

## Document Conventions



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

Command descriptions use the following conventions:

Convention	Description
<b>bold</b>	Bold text indicates the commands and keywords that you enter literally as shown.
<i>Italic</i>	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x   y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.

Convention	Description
[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.
<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 will include 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.
<b>boldface screen font</b>	Information 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.

This document uses the following conventions:



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



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

## Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to: .

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 for this Release

---

There are no new or changed features in this release.





## CHAPTER 2

# Overview

---

This chapter contains the following sections:

- [Fibre Channel over Ethernet, on page 3](#)
- [Data Center I/O Consolidation, on page 3](#)
- [Virtual Interfaces, on page 4](#)
- [Typical Deployment Topologies, on page 5](#)
- [Supported Standards, on page 10](#)

## Fibre Channel over Ethernet

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

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

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

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

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

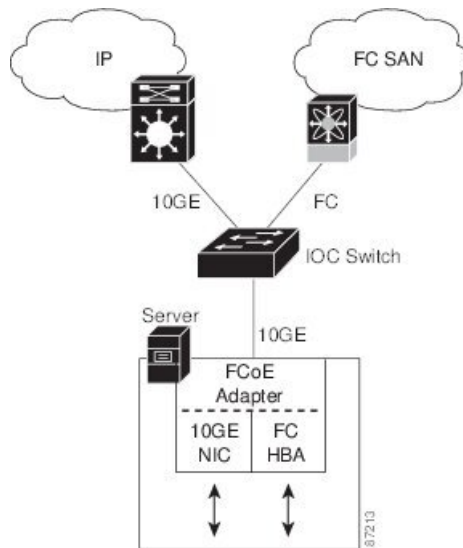
## Data Center I/O Consolidation

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

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

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

**Figure 1: I/O Consolidation**



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

## Virtual Interfaces

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

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

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

# Typical Deployment Topologies

## Ethernet Switching

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

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

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

## FCoE and Fibre Channel Switching

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

FCoE and Fibre Channel switching includes the following features:

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

## QoS

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

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

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

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

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



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

## Virtual Port Channels

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

## Serviceability

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

## Switched Port Analyzer

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

## Ethalyzer

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

## Call Home

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

## Online Diagnostics

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

# Switch Management

## Simple Network Management Protocol

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

## Role-Based Access Control

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

## Configuration Methods

### Configuring with CLI, XML Management Interface, or SNMP

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

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

### Configuring with Cisco Data Center Network Manager

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

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

### Configuring with Cisco MDS Fabric Manager

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

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

## Network Security Features

Cisco NX-OS includes the following security features:

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

## Virtual Device Contexts

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

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

## Licensing

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

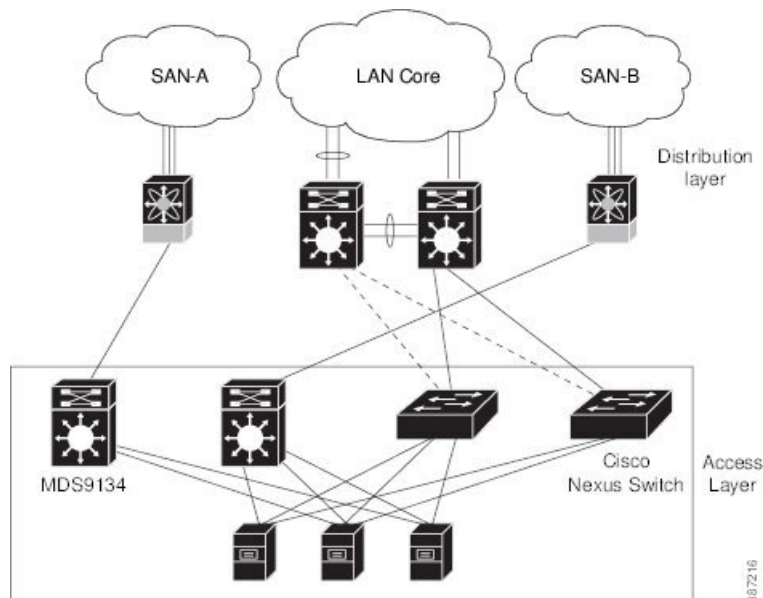
## Ethernet TOR Switch Topology

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

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

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

**Figure 2: Ethernet TOR Switch Topology**



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

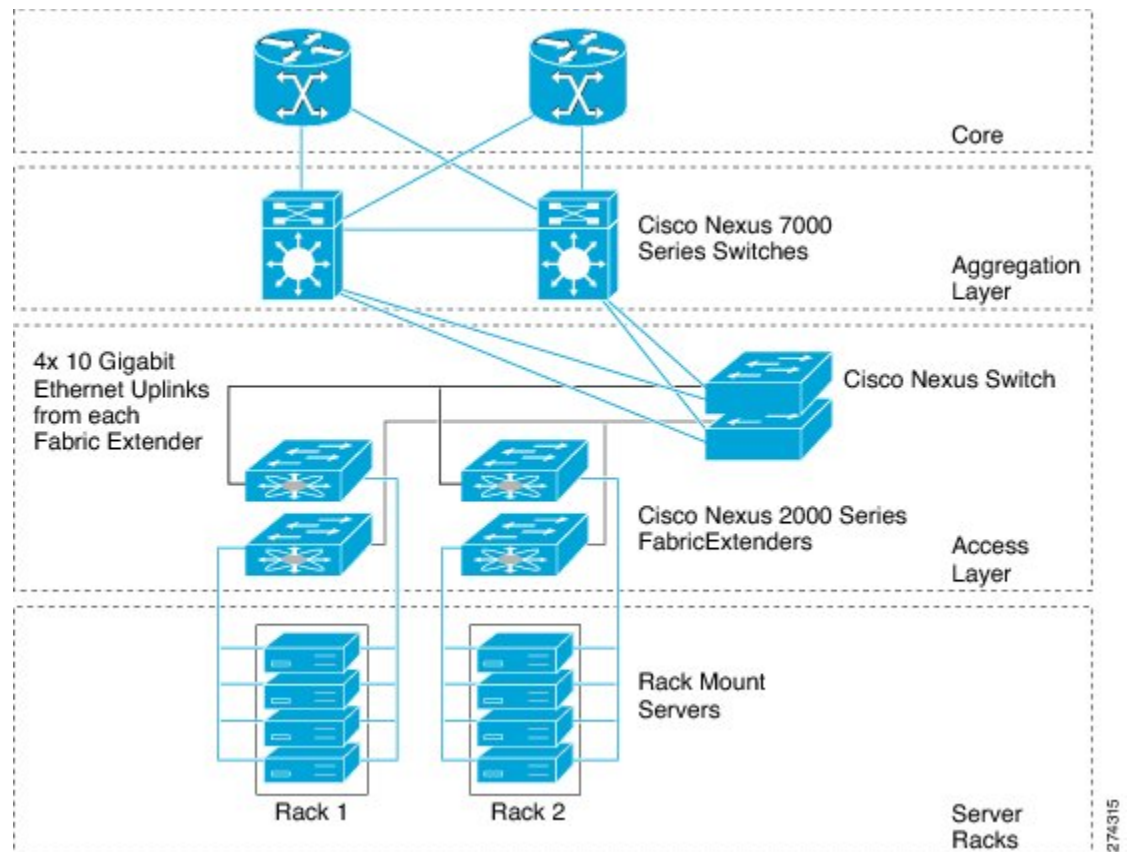
The servers are connected to the data center SAN through MDS 9134 SAN switches. The server Fibre Channel ports require standard Fibre Channel HBAs.



## Fabric Extender Deployment Topology

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

**Figure 3: Fabric Extender Deployment Topology**



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

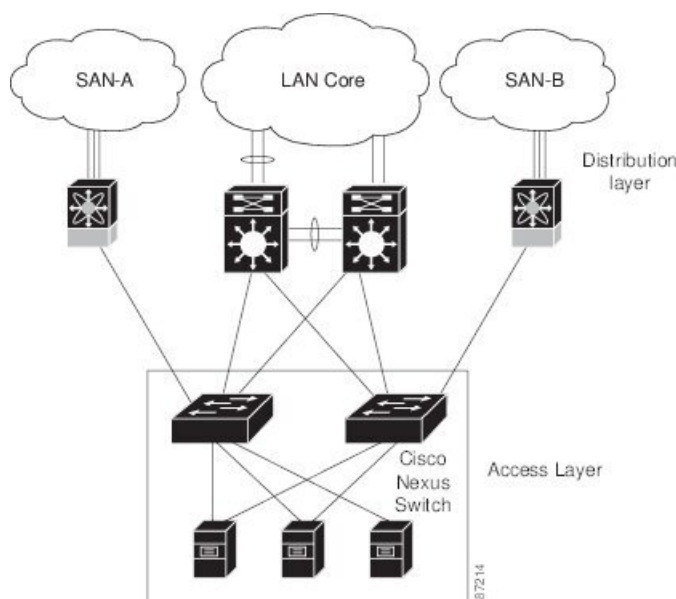
Each Fabric Extender acts as a Remote I/O Module on the parent Cisco Nexus device. All device configurations are managed on the Cisco Nexus device and configuration information is downloaded using inband communication to the Fabric Extender.

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

## Data Center I/O Consolidation Topology

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

Figure 4: I/O Consolidation Topology



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

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

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

## Supported Standards

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

Table 1: IEEE Compliance

Standard	Description
802.1D	MAC Bridges
802.1s	Multiple Spanning Tree Protocol
802.1w	Rapid Spanning Tree Protocol
802.3ad	Link aggregation with LACP
802.3ae	10-Gigabit Ethernet

Standard	Description
802.1Q	VLAN Tagging
802.1p	Class of Service Tagging for Ethernet frames





## CHAPTER 3

# Using the Cisco NX-OS Setup Utility

---

This chapter describes how to use the Cisco NX-OS setup utility.

- [Configuring the Switch, on page 13](#)

## Configuring the Switch

### Image Files on the Switch

The Cisco Nexus devices have the following images:

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

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

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

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

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

### Starting the Switch

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

### Boot Sequence

When the switch boots, the golden BIOS validates the checksum of the upgradeable BIOS. If the checksum is valid, then control is transferred to the upgradeable BIOS image. The upgradeable BIOS launches the

kickstart image, which then launches the system image. If the checksum of the upgradeable BIOS is not valid, then the golden BIOS launches the kickstart image, which then launches the system image.

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

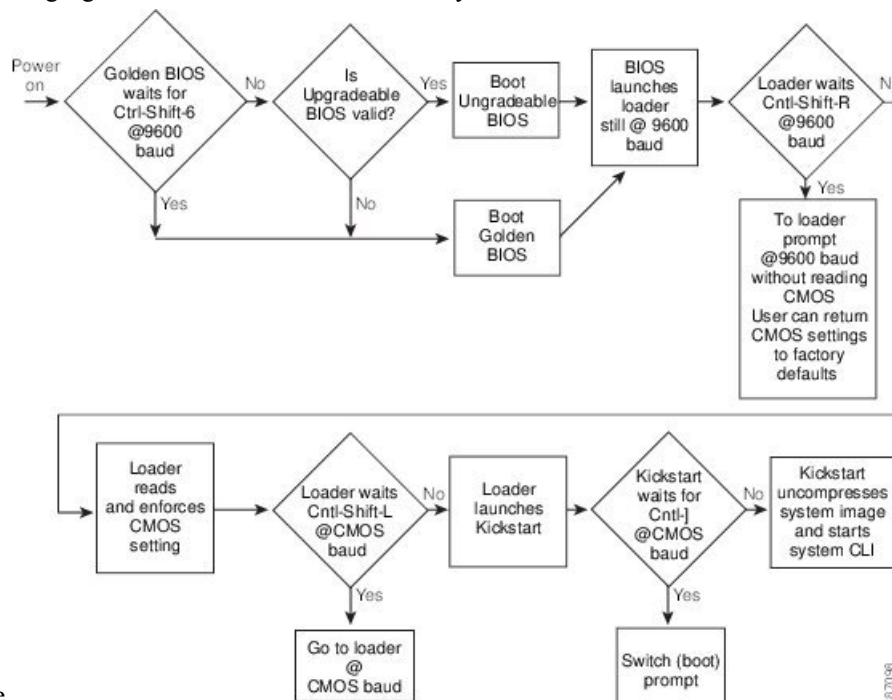


**Note** When you press **Ctrl-Shift-6**, the console settings must be set to their defaults: 9600 baud, 8 data bits, no parity, and 1 stop bit.

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

**Figure 5: Boot Sequence**

The following figure shows the normal and recovery boot



sequence.

For additional information, see *Troubleshooting*.

## Console Settings

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

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

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

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

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

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

## Upgrading the Switch Software



---

**Note** You must have the network-admin role before you can upgrade the software image on the switch. You must log in to the switch on its console port connection.

---

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

### SUMMARY STEPS

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

### DETAILED STEPS

---

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

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

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

**Step 3** Navigate to the software downloads for Cisco Nexus devices.

You see links to the download images for the switch.

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

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

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

**Example:**

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

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

**Example:**

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

**Example:**

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

**Example:**

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

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

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

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

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

**Example:**

## Downgrading from a Higher Release

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



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



## SUMMARY STEPS

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

## DETAILED STEPS

### Step 1

Locate the image files you will use for the downgrade by entering the **dir bootflash:** command.

If the image files are not stored on the bootflash memory, download the files from Cisco.com:

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

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

- b) Access the Software Download Center using this URL: <http://www.cisco.com/cisco/web/download/index.html>
- c) Navigate to the software downloads for Cisco Nexus Series switches.

You see links to the download images for the switch.

- d) Read the release notes for the related image file then select and download the kickstart and system software files to a local server
- e) Ensure that the required space is available in the bootflash: directory for the image file(s) to be copied.

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

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

### Step 2

Install the new images.

#### Example:

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

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

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

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

### Step 3

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

#### Example:

```
switch# show version
```

---

# Initial Configuration

## Configuration Prerequisites

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

### SUMMARY STEPS

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

### DETAILED STEPS

---

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

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

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

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

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

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

## Initial Setup

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



---

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

---

## Preparing to Configure the Switch

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

- Administrator password.



---

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

---

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

- SSH service on the switch (optional).

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

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

This is your switch prompt.

- An additional login account and password (optional).



---

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

---

## Default Login

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

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



---

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

---

## Configuring the Switch

This section describes how to initially configure the switch.



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



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

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

## SUMMARY STEPS

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

## DETAILED STEPS

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

**Step 2** Enter the new password for the administrator.

**Example:**

Enter the password for admin: *<password>*

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

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

**Step 3** Enter **yes** to enter the setup mode.

**Example:**

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

\*Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values.

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

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

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

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

**Example:**

Enter the password for admin: **admin**

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

**Example:**

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

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

a) Enter the user login ID.

**Example:**

Enter the user login ID: *user\_name*

b) Enter the user password.

**Example:**

Enter the password for user\_name: *user-password*

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

**Example:**

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

**Step 7** Enter a name for the switch.

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

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

**Example:**

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

Permits traffic flow to all members of the default zone.

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

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

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

**Example:**

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

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

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

**Example:**

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

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

**Example:**

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

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

---

## Changing the Initial Configuration

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

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

The setup utility guides you through the basic configuration process.

## Management Interface Configuration

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

### About the mgmt0 Interface

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




---

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

---

## Configuring the Management Interface

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

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface mgmt 0**



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

## DETAILED STEPS

---

- Step 1**     `switch# configure terminal`  
Enters configuration mode.
- Step 2**     `switch(config)# interface mgmt 0`  
Selects the management Ethernet interface on the switch and enters interface configuration submode.
- Step 3**     Configure the IP address for IPv4 or IPv6:  
a) `switch(config-if)# ip address ipv4-address [/ length]`  
Configures the IPv4 address and its subnet mask.  
b) `switch(config-if)# ip address ipv4-address [subnet-mask]`  
An alternative method that configures the IPv4 address and its subnet mask.  
c) `switch(config-if)# ipv6 address ipv6-address [/ length]`  
Configures the IPv6 address and its subnet mask.
- Step 4**     `switch(config-if)# no shutdown`  
Enables the interface.
- Step 5**     `switch(config-if)# exit`  
Returns to configuration mode.
- Step 6**     `switch(config)# vrf context management`  
Enters VRF context management configuration mode.
- Step 7**     Configure the IP address (IPv4 or IPv6) for the next hop:  
a) `switch(config-vrf)# ip route ipv4-prefix [/ length] ipv4-nexthop-address`  
Configures the IPv4 address of the next hop.  
b) `switch(config-vrf)# ipv6 route ipv6-prefix [/ length] ipv6-nexthop-address`  
Configures the IPv6 address of the next hop.
- Step 8**     `switch(config-vrf)# end`  
Returns to EXEC mode.
- Step 9**     (Optional) `switch# copy running-config startup-config`

Saves your configuration changes to the file system.

---

### Example

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

## Displaying Management Interface Configuration

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

```
switch# show interface mgmt0

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

## Shutting Down the Management Interface

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

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

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

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

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



## CHAPTER 4

# Using PowerOn Auto Provisioning

This chapter contains the following sections:

- [Guidelines and Limitations for POAP, on page 27](#)
- [Setting Up the Network Environment To Use POAP, on page 28](#)
- [Configuring a Switch Using POAP, on page 29](#)
- [Verifying the Device Configuration, on page 29](#)
- [Related Documents for POAP, on page 30](#)

## Guidelines and Limitations for POAP

- The Cisco Nexus switch software image must support POAP for this feature to function.
- POAP can be triggered even when the startup-config is present using the **boot poap enable** command.
- If a LACP Layer 3 port-channel is configured on an uplink device connected to the Cisco Nexus device that is being bootstrapped using POAP, the port-channel is not active because all the member links are in a suspended state. Therefore, the Cisco Nexus device that is being bootstrapped using POAP cannot reach the DHCP server or any other infrastructure device needed for POAP. To work around this issue, configure a static L3 port-channel on the uplink device connected to the Cisco Nexus device that is being bootstrapped using POAP.

- If you use POAP to bootstrap a Cisco Nexus device that is a part of a vPC pair using static port-channels on the VPC links, the Cisco Nexus device activates all of its links upon POAP startup. The dually connected device at the end of the VPC links might start sending some or all of its traffic to the port-channel member links connected to the Cisco Nexus device, and the traffic would be lost.

To work around this issue, you can configure LACP on the vPC links so that the links do not incorrectly start forwarding traffic to the Cisco Nexus device that is being bootstrapped using POAP.

- If you use POAP to bootstrap a Cisco Nexus device that is connected downstream to a Cisco Nexus Series 7000 device through a LACP port-channel, the Cisco Nexus 7000 Series device defaults to suspend its member port if it cannot bundle it as a part of a port-channel. To work around this issue, configure the Cisco Nexus 7000 Series device to not suspend its member ports using the **no lacp suspend-individual** command from interface configuration mode.
- Important POAP updates are logged in the syslog and are available from the serial console.

- Critical POAP errors are logged to the bootflash. The filename format is *date-time\_poap\_PID\_[init,1,2].log*, where *date-time* is in the YYYYMMDD\_hhmmss format and *PID* is the process ID.
- Script logs are saved in the bootflash directory. The filename format is *date-time\_poap\_PID\_script.log*, where *date-time* is in the YYYYMMDD\_hhmmss format and *PID* is the process ID.
- The Scheduler configuration cannot be replayed using POAP. The reason that the Scheduler configuration cannot be replayed is that it is associated with the user (for example "admin") that was logged in when the Scheduler configuration was created. Because the configuration replay using POAP is not associated with any specific user, the scheduler configuration cannot be replayed and fails.

Instead of configuring the Scheduler, configure the Embedded Event Manager (EEM). An EEM configuration can be downloaded and replayed using POAP.

- You can bypass password and basic POAP configuration by using the **skip** option at the POAP prompt. When you use the **skip** option, no password will be configured for the **admin** user. The **copy running-config startup-config** command will be blocked until a valid password is set for the **admin** user.
- DHCP for NX-OS will be successful, if the DHCP response is set to IP address 255.255.255.255. Since not all the DHCP server including IOS DHCP server sends the DHCP responses to 255.255.255.255, NX-OS is unable to get an IP address as a result POAP does not succeed.

## Setting Up the Network Environment To Use POAP

### SUMMARY STEPS

1. Modify the basic configuration script provided by Cisco or create your own script. For information, see the *Python Scripting and API Configuration Guide*.
2. (Optional) Put the POAP configuration script and any other desired software image and switch configuration files on a USB device accessible to the switch.
3. 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.)
4. Deploy a TFTP or HTTP server to host the configuration script.
5. Deploy one or more servers to host the software images and configuration files.

### DETAILED STEPS

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Modify the basic configuration script provided by Cisco or create your own script. For information, see the <i>Python Scripting and API Configuration Guide</i> .   |
| <b>Step 2</b> | (Optional) Put the POAP configuration script and any other desired software image and switch configuration files on a USB device accessible to the switch.  |
| <b>Step 3</b> | 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.) |

You do not need to deploy a DHCP server if all software image and switch configuration files are on the USB device.

- Step 4** Deploy a TFTP or HTTP server to host the configuration script.
- Step 5** Deploy one or more servers to host the software images and configuration files.
- 

## Configuring a Switch Using POAP

### Before you begin

Make sure that the network environment is set up to use POAP. For more information, refer to the "Setting up the Network Environment to use POAP" section immediately preceding this section.

### SUMMARY STEPS

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

### DETAILED STEPS

---

**Step 1** Install the switch in the network.

**Step 2** Power on the switch.

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

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

**Step 3** (Optional) If you want to exit POAP mode and enter the normal interactive setup script, enter **y** (yes).

The switch boots, and the POAP process begins. For more information, see the "POAP Process" section.

---

### What to do next

Verify the configuration.

## Verifying the Device Configuration

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

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

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

## Related Documents for POAP

Related Topic	Document Title
Configuration Script	<i>Cisco Nexus 3000 Series NX-OS Python API Reference Guide</i>
DHCP Options and BOOTP Vendor Extensions	RFC2132— <a href="http://tools.ietf.org/html/rfc2132">http://tools.ietf.org/html/rfc2132</a>
TFTP Server Address Option for DHCPv4	RFC5859— <a href="http://tools.ietf.org/html/rfc5859">http://tools.ietf.org/html/rfc5859</a>



## CHAPTER 5

# Understanding the Command-Line Interface

This chapter helps you understand the command-line interface.

- Finding Feature Information, on page 31
- Information About the CLI Prompt, on page 32
- Command Modes, on page 32
- Special Characters, on page 36
- Keystroke Shortcuts, on page 36
- Abbreviating Commands, on page 38
- Completing a Partial Command Name, on page 39
- Identifying Your Location in the Command Hierarchy, on page 39
- Using the no Form of a Command , on page 40
- Configuring CLI Variables, on page 41
- Command Aliases, on page 43
- Command Scripts, on page 45
- Context-Sensitive Help , on page 47
- Understanding Regular Expressions, on page 48
- Searching and Filtering show Command Output, on page 50
- Searching and Filtering from the --More-- Prompt, on page 54
- Using the Command History, on page 55
- Enabling or Disabling the CLI Confirmation Prompts, on page 57
- Setting CLI Display Colors, on page 57
- Sending Commands to Modules, on page 57
- BIOS Loader Prompt, on page 58
- Examples Using the CLI , on page 59
- Additional References for the CLI, on page 61

## Finding Feature Information

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

# Information About the CLI Prompt

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

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

You can change the default device hostname.

From the CLI prompt, you can do the following:

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



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

## Command Modes

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

## EXEC Command Mode

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



## Global Configuration Command Mode

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

### SUMMARY STEPS

1. **configure terminal**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.  <b>Note</b> The CLI prompt changes to indicate that you are in global configuration mode.

## Interface Configuration Command Mode

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

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

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

## Subinterface Configuration Command Mode

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

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

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>type number.subint</i>  <b>Example:</b> <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.  <b>Note</b> The CLI prompt changes to indicate that you are in global 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.

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

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

## Exiting a Configuration Command Mode

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>exit</b> <b>Example:</b> <pre>switch(config-if) # exit switch(config) #</pre>	Exits from the current configuration command mode and returns to the previous configuration command mode.
<b>Step 2</b>	<b>end</b> <b>Example:</b> <pre>switch(config-if) # end switch#</pre>	Exits from the current configuration command mode and returns to EXEC mode.
<b>Step 3</b>	(Optional) <b>Ctrl-Z</b> <b>Example:</b> <pre>switch(config-if) # ^z switch#</pre>	Exits the current configuration command mode and returns to EXEC mode.  <b>Caution</b> If you press <b>Ctrl-Z</b> 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 <b>exit</b> or <b>end</b> command.

## Command Mode Summary

This table summarizes information about the main command modes.

*Table 2: 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 <b>exit</b> command.
Global configuration	From EXEC mode, use the <b>configure terminal</b> command.	switch(config)#	To exit to EXEC mode, use the <b>end</b> or <b>exit</b> command or press <b>Ctrl-Z</b> .

Mode	Access Method	Prompt	Exit Method
Interface configuration	From global configuration mode, use an interface command and specify an interface with an <b>interface</b> command.	switch(config-if) #	To exit to global configuration mode, use the <b>exit</b> command. To exit to EXEC mode, use the <b>exit</b> command or press <b>Ctrl-Z</b> .
Subinterface configuration	From global configuration mode, specify a subinterface with an <b>interface</b> command.	switch(config-subif) #	To exit to global configuration mode, use the <b>exit</b> command. To exit to EXEC mode, use the <b>end</b> command or press <b>Ctrl-Z</b> .

## 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 3: 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 4: Keystroke Shortcuts**

Keystokes	Description
Ctrl-A	Moves the cursor to the beginning of the line.

Keystrokes	Description
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.
Ctrl-N	Displays the next command in the command history.
Ctrl-O	Clears the terminal screen.
Ctrl-P	Displays the previous command in the command history.
Ctrl-R	Redisplays the current command line.
Ctrl-T	Transposes the character under the cursor with the character located to the right of the cursor. The cursor is then moved one character to the right.
Ctrl-U	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-V	Removes any special meaning for the following keystroke. For example, press Ctrl-V before entering a question mark (?) in a regular expression.
Ctrl-W	Deletes the word to the left of the cursor.
Ctrl-X, H	Lists the history of commands you have entered.  When using this key combination, press and release the Ctrl and X keys together before pressing H.
Ctrl-Y	Recalls the most recent entry in the buffer (press keys simultaneously).
Ctrl-Z	Ends a configuration session, and returns you to EXEC mode.  When used at the end of a command line in which a valid command has been typed, the resulting configuration is first added to the running configuration file.
Up arrow key	Displays the previous command in the command history.
Down arrow key	Displays the next command in the command history.

Keystokes	Description
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.
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"> <li>• Command names</li> <li>• Scheme names in the file system</li> <li>• Server names in the file system</li> <li>• Filenames in the file system</li> </ul> <p><b>Example:</b></p> <pre>switch(config)# c&lt;Tab&gt; callhome class-map clock cts cdp cli control-plane switch(config)# cl&lt;Tab&gt; class-map cli clock switch(config)# cla&lt;Tab&gt; switch(config)# class-map</pre> <p><b>Example:</b></p> <pre>switch# cd bootflash:&lt;Tab&gt; bootflash: bootflash://sup-1/ bootflash:/// bootflash://sup-2/ bootflash://module-5/ bootflash://sup-active/ bootflash://module-6/ bootflash://sup-local/</pre> <p><b>Example:</b></p> <pre>switch# cd bootflash://mo&lt;Tab&gt; bootflash://module-5/ bootflash://module-6/cv switch# cd bootflash://module-</pre>

## 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 5: 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 this example, the CLI recognizes the unique string for **conf** in EXEC mode when you press the **Tab** key:

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

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

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

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

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

## Identifying Your Location in the Command Hierarchy

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

### SUMMARY STEPS

1. where detail

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>where detail</b> <b>Example:</b> <pre>switch# configure terminal switch(config)# interface mgmt0 switch(config-if)# where detail mode:                conf                     interface mgmt0 username:            admin</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. The Cisco NX-OS command reference publications describe the function of the **no** form of the command whenever a **no** form is available.

This example shows how to disable a feature:

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

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

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

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

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

```
switch# configure terminal
switch(config)# radius-server host 10.10.2.2
switch(config)# show radius-server
retransmission count:0
timeout value:1
deadtime value:1
total number of servers:1

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

switch(config)# no radius-server host 10.10.2.2
```



```
switch(config)# show radius-server
retransmission count:0
timeout value:1
deadtime value:1
total number of servers:1

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

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

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

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

## Configuring CLI Variables

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

### About CLI Variables

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

You can refer to CLI variables in the following ways:

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

CLI variables have the following characteristics:

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

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



---

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

---

## Configuring CLI Session-Only Variables

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>cli var name</b> <i>variable-name variable-text</i> <b>Example:</b> <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.
<b>Step 2</b>	(Optional) <b>show cli variables</b> <b>Example:</b> <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.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>cli var name</b> <i>variable-name variable-text</i> <b>Example:</b>	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
	<code>switch(config)# cli var name testinterface ethernet 2/1</code>	
Step 3	<b>exit</b> <b>Example:</b> <code>switch(config)# exit</code> <code>switch#</code>	Exits global configuration mode.
Step 4	(Optional) <b>show cli variables</b> <b>Example:</b> <code>switch# show cli variables</code>	Displays the CLI variable configuration.
Step 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Command Aliases

This section provides information about command aliases.

### About Command Aliases

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

Command alias support has the following characteristics:

- Command aliases are global for all user sessions.
- Command aliases persist across reboots if you save them to the startup configuration.
- Command alias translation always takes precedence over any keyword in any configuration mode or submode.
- Command alias configuration takes effect for other user sessions immediately.
- The Cisco NX-OS software provides one default alias, **alias**, which is the equivalent to the **show cli alias** command that displays all user-defined aliases.
- You cannot delete or change the default command alias **alias**.
- You can nest aliases to a maximum depth of 1. One command alias can refer to another command alias that must refer to a valid command, not to another command alias.
- A command alias always replaces the first command keyword on the command line.
- You can define command aliases for commands in any command mode.
- If you reference a CLI variable in a command alias, the current value of the variable appears in the alias, not the variable reference.

- You can use command aliases for **show** command searching and filtering.

## Defining Command Aliases

You can define command aliases for commonly used commands.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>cli alias name</b> <i>alias-name alias-text</i>  <b>Example:</b> <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.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
<b>Step 4</b>	(Optional) <b>alias</b>  <b>Example:</b> <pre>switch# alias</pre>	Displays the command alias configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <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.

## SUMMARY STEPS

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

## DETAILED STEPS

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

## Command Scripts

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

### Running a Command Script

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



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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>run-script [bootflash:   slot0:   volatile:]filename</b>  <b>Example:</b> <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 6: Formatting Options for the echo Command**

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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>echo</b> [backslash-interpret] [ <i>text</i> ]  <b>Example:</b> <pre>switch# echo This is a test. This is a test.</pre>	The <b>backslash-interpret</b> 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.

## SUMMARY STEPS

1. **sleep** *seconds*

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>sleep</b> <i>seconds</i> <b>Example:</b> switch# sleep 30	Causes a delay for a number of seconds. The range is from 0 to 2147483647.

## Context-Sensitive Help

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

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

This table shows example outputs of context sensitive help.

**Table 7: 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 <b>clock</b> command in EXEC mode.</p> <p>The switch output shows that the <b>set</b> keyword is required for using the <b>clock</b> 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&lt;CR&gt; % Incomplete command switch#</pre>	<p>Adds the current time.</p> <p>The CLI indicates the command is incomplete.</p>
<pre>switch# &lt;Ctrl-P&gt; switch# clock set 13:32:00</pre>	Displays the previous command that you entered.
<pre>switch# clock set 13:32:00 ?       &lt;1-31&gt;      Day of the month switch# clock set 13:32:00</pre>	Displays the additional arguments for the <b>clock set</b> command.

Example Outputs	Description
<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>	Displays the additional arguments for the <b>clock set</b> command.
<pre>switch# clock set 13:32:00 18 April 08&lt;CR&gt; % 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 08.</p>
<pre>switch# clock set 13:32:00 18 April ? &lt;2000-2030&gt; Enter the year (no abbreviation)  switch# clock set 13:32:00 18 April</pre>	Displays the correct arguments for the year.
<pre>switch# clock set 13:32:00 18 April 2008&lt;CR&gt; switch#</pre>	Enters the correct syntax for the <b>clock set</b> command.

## Understanding Regular Expressions

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

## Special Characters

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

This table lists the keyboard characters that have special meanings.

**Table 8: 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.



Character	Special Meaning
^	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.  <b>Note</b> 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 9: 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
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 10: Filtering and Searching Keywords**

Keyword Syntax	Description
<b>begin</b> <i>string</i> <b>Example:</b> <code>show version   begin Hardware</code>	Starts displaying at the line that contains the text that matches the search string. The search string is case sensitive.
<b>count</b> <b>Example:</b> <code>show running-config   count</code>	Displays the number of lines in the command output.
<b>cut</b> [- <i>d character</i> ] {- <i>b</i>   - <i>c</i>   - <i>f</i>   - <i>s</i> } <b>Example:</b> <code>show file testoutput   cut -b 1-10</code>	Displays only part of the output lines. You can display a number of bytes (- <i>b</i> ), characters (- <i>vcut</i> [- <i>d character</i> ] {- <i>b</i>   - <i>c</i>   - <i>f</i>   - <i>s</i> }), or fields (- <i>f</i> ). You can also use the - <i>d</i> keyword to define a field delimiter other than the tag character default. The - <i>s</i> keyword suppresses the display of the lines that do not contain the delimiter.
<b>end</b> <i>string</i> <b>Example:</b> <code>show running-config   end interface</code>	Displays all lines up to the last occurrence of the search string.
<b>exclude</b> <i>string</i> <b>Example:</b> <code>show interface brief   exclude down</code>	Displays all lines that do not include the search string. The search string is case sensitive.
<b>head</b> [ <i>lines lines</i> ] <b>Example:</b> <code>show logging logfile   head lines 50</code>	Displays the beginning of the output for the number of lines specified. The default number of lines is 10.
<b>include</b> <i>string</i> <b>Example:</b> <code>show interface brief   include up</code>	Displays all lines that include the search string. The search string is case sensitive.
<b>last</b> [ <i>lines</i> ] <b>Example:</b> <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.
<b>no-more</b> <b>Example:</b> <code>show interface brief   no-more</code>	Displays all the output without stopping at the end of the screen with the --More-- prompt.

Keyword Syntax	Description
<b>sscp</b> <i>SSH-connection-name filename</i> <b>Example:</b> <pre>show version   sscp MyConnection show_version_output</pre>	Redirects the output using streaming secure copy (sscp) to a named SSH connection. You can create the SSH named connection using the <b>ssh name</b> command.
<b>wc</b> [bytes   lines   words] <b>Example:</b> <pre>show file testoutput   wc bytes</pre>	Displays counts of characters, lines, or words. The default is to display the number of lines, words, and characters.

## diff Utility

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

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

This table describes the keywords for the diff utility.

Keyword	Description
<b>all-sessions</b>	Removes diff temporary files from all sessions (past and present sessions) of the current user.
<b>all-users</b>	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 11: grep and egrep Parameters**

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

## 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 12: sort Utility Parameters**

Parameter	Description
<b>-M</b>	Sorts by month.

Parameter	Description
<b>-b</b>	Ignores leading blanks (space characters). The default sort includes the leading blanks.
<b>-d</b>	Sorts by comparing only blanks and alphanumeric characters. The default sort includes all characters.
<b>-f</b>	Folds lowercase characters into uppercase characters.
<b>-g</b>	Sorts by comparing a general numeric value.
<b>-i</b>	Sorts only using printable characters. The default sort includes nonprintable characters.
<b>-k</b> <i>field-number</i> [ <i>,char-position</i> ][ <i>ordering</i> ]	Sorts according to a key value. There is no default key value.
<b>-n</b>	Sorts according to a numeric string value.
<b>-r</b>	Reverses order of the sort results. The default sort output is in ascending order.
<b>-t</b> <i>delimiter</i>	Sorts using a specified delimiter. The default delimiter is the space character.
<b>-u</b>	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 13: --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> ] <b>z</b>	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.

Commands	Description
[ <i>lines</i> ] <b>d</b> 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.
<b>q</b> or <b>Q</b> or Ctrl-C	Exits the --More-- prompt.
[ <i>lines</i> ] <b>s</b>	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> ] <b>f</b>	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> ] <b>n</b>	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.
{ <b>!</b>   <b>!!</b> [ <i>shell-cmd</i> ] }	Executes the command specified in the <i>shell-cmd</i> argument in a subshell.
.	Repeats the previous command.

## Using the Command History

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

### Recalling a Command

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

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

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

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

## Controlling CLI History Recall

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

## Configuring the CLI Edit Mode

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

## Displaying the Command History

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

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

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

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

```
switch# show cli history
```

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

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

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

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



# Enabling or Disabling the CLI Confirmation Prompts

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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>[no] terminal dont-ask [persist]</code>  <b>Example:</b> <code>switch# terminal dont-ask</code>	Disables the CLI confirmation prompt. The <b>persist</b> keyword makes the setting persistent across sessions for the current username. The default is enabled.  Use the <b>no</b> 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 those set by the terminal emulator software.

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>terminal color [evening] [persist]</code>  <b>Example:</b> <code>switch# terminal color</code>	Sets the CLI display colors for the terminal session. The <b>evening</b> keyword is not supported. The <b>persist</b> 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 2 show version | grep lc
```

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

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

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

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

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

## BIOS Loader Prompt

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

```
loader>
```

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

## Examples Using the CLI

This section includes examples of using the CLI.

### Defining Command Aliases

This example shows how to define command aliases:

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

This example shows how to use a command alias:

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

### Using CLI Session Variables

You can reference a variable using the syntax `$(variable-name)`.

This example shows how to reference a user-defined CLI session variable:

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

```

0 input error 0 short frame 0 watchdog
0 no buffer 0 runt 0 CRC 0 ecc
0 overrun 0 underrun 0 ignored 0 bad etype drop
0 bad proto drop 0 if down drop 0 input with dribble
0 input discard
0 output error 0 collision 0 deferred
0 late collision 0 lost carrier 0 no carrier
0 babble
0 Rx pause 0 Tx pause 0 reset

```

## Using the System-Defined Timestamp Variable

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

```

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

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

```

## Running a Command Script

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

```

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

```

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

```

switch# run-script testfile
`configure terminal`
`interface ethernet 2/1`
`no shutdown`
`end`
`show interface ethernet 2/1`
Ethernet2/1 is down (Link not connected)
  Hardware is 10/100/1000 Ethernet, address is 0019.076c.4dac (bia 0019.076c.4dac)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
  Last clearing of "show interface" counters 1d26.2uh
  5 minute input rate 0 bytes/sec, 0 packets/sec

```

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

## Additional References for the CLI

This section includes additional information related to the CLI.

### Related Documents for the CLI

Related Topic	Document Title
Cisco NX-OS Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	





## CHAPTER 6

# Configuring Terminal Settings and Sessions

This chapter describes how to configure terminal settings and sessions.

- [Finding Feature Information, on page 63](#)
- [Information About Terminal Settings and Sessions, on page 63](#)
- [Configuring the Console Port, on page 65](#)
- [Configuring the COM1 Port, on page 67](#)
- [Configuring Virtual Terminals , on page 69](#)
- [Configuring Modem Connections, on page 71](#)
- [Clearing Terminal Sessions, on page 75](#)
- [Displaying Terminal and Session Information, on page 76](#)
- [Default Settings for File System Parameters, on page 76](#)
- [Additional References for Terminal Settings and Sessions, on page 76](#)

## Finding Feature Information

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

## Information About Terminal Settings and Sessions

This section includes information about terminal settings and sessions.

### Terminal Session Settings

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

#### **Terminal type**

Name used by Telnet when communicating with remote hosts

#### **Length**

Number of lines of command output displayed before pausing

**Width**

Number of characters displayed before wrapping the line

**Inactive session timeout**

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

## Console Port

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

**Data bits**

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

**Inactive session timeout**

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

**Parity**

Specifies the odd or even parity for error detection.

**Speed**

Specifies the transmission speed for the connection.

**Stop bits**

Specifies the stop bits for an asynchronous line.

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

## COM1 Port

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

**Data bits**

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

**Hardware flowcontrol**

Enables the flow-control hardware.

**Parity**

Specifies the odd or even parity for error detection.

**Speed**

Specifies the transmission speed for the connection.

**Stop bits**

Specifies the stop bits for an asynchronous line.

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

## Virtual Terminals

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



## Modem Support

You can connect a modem to the COM1 or console ports only on the supervisor 1 module. The following modems were tested on devices running the Cisco NX-OS software:

- MultiTech MT2834BA
- Hayes Accura V.92



---

**Note** Do not connect a modem when the device is booting. Only connect the modem when the device is powered up.

---

The Cisco NX-OS software has the default initialization string (ATE0Q1&D2&C1S0=1\015) to detect connected modems. The default string is defined as follows:

**AT**

Attention

**E0 (required)**

No echo

**Q1**

Result code on

**&D2**

Normal data terminal ready (DTR) option

**&C1**

Enable tracking the state of the data carrier

**S0=1**

Pick up after one ring

**\015 (required)**

Carriage return in octal

## Configuring the Console Port

You can set the following characteristics for the console port:

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

### Before you begin

Log in to the console port.

### SUMMARY STEPS

1. **configure terminal**

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>line console</b>  <b>Example:</b> <pre>switch# line console switch(config-console)#</pre>	Enters console configuration mode.
<b>Step 3</b>	<b>databits</b> <i>bits</i>  <b>Example:</b> <pre>switch(config-console)# databits 7</pre>	Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.
<b>Step 4</b>	<b>exec-timeout</b> <i>minutes</i>  <b>Example:</b> <pre>switch(config-console)# exec-timeout 30</pre>	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.
<b>Step 5</b>	<b>parity</b> { <b>even</b>   <b>none</b>   <b>odd</b> }  <b>Example:</b> <pre>switch(config-console)# parity even</pre>	Configures the parity. The default is <b>none</b> .
<b>Step 6</b>	<b>speed</b> { <b>300</b>   <b>1200</b>   <b>2400</b>   <b>4800</b>   <b>9600</b>   <b>38400</b>   <b>57600</b>   <b>115200</b> }  <b>Example:</b> <pre>switch(config-console)# speed 115200</pre>	Configures the transmit and receive speed. The default is <b>9600</b> .
<b>Step 7</b>	<b>stopbits</b> { <b>1</b>   <b>2</b> }  <b>Example:</b> <pre>switch(config-console)# stopbits 2</pre>	Configures the stop bits. The default is <b>1</b> .
<b>Step 8</b>	<b>exit</b>  <b>Example:</b>	Exits console configuration mode.

	Command or Action	Purpose
	<code>switch(config-console)# exit</code> <code>switch(config)#</code>	
<b>Step 9</b>	(Optional) <b>show line console</b>  <b>Example:</b> <code>switch(config)# show line console</code>	Displays the console settings.
<b>Step 10</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Configuring the COM1 Port

You can set the following characteristics for the COM1 port:

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

### Before you begin

Log in to the console port or COM1 port.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
<b>Step 2</b>	<b>line com1</b>  <b>Example:</b> switch# line com1 switch(config-com1)#	Enters COM1 configuration mode.
<b>Step 3</b>	<b>databits <i>bits</i></b>  <b>Example:</b> switch(config-com1)# databits 7	Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.
<b>Step 4</b>	<b>flowcontrol hardware</b>  <b>Example:</b> switch(config-com1)# flowcontrol hardware	Enables flow control on the hardware. The default is enabled.  Use the <b>no flowcontrol hardware</b> command to disable flow control on the hardware.
<b>Step 5</b>	<b>parity {even   none   odd}</b>  <b>Example:</b> switch(config-com1)# parity even	Configures the parity. The default is <b>none</b> .
<b>Step 6</b>	<b>speed {300   1200   2400   4800   9600   38400   57600   115200}</b>  <b>Example:</b> switch(config-com1)# speed 115200	Configures the transmit and receive speed. The default is <b>9600</b> .
<b>Step 7</b>	<b>stopbits {1   2}</b>  <b>Example:</b> switch(config-com1)# stopbits 2	Configures the stop bits. The default is <b>1</b> .
<b>Step 8</b>	<b>exit</b>  <b>Example:</b> switch(config-com1)# exit switch(config)#	Exits COM1 configuration mode.
<b>Step 9</b>	(Optional) <b>show line com1</b>  <b>Example:</b> switch(config)# show line com1	Displays the COM1 port settings.
<b>Step 10</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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 a Cisco NX-OS device.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<b>line vty</b>  <b>Example:</b> <pre>switch# line vty switch(config-line)#</pre>	Enters line configuration mode.
Step 3	<ul style="list-style-type: none"> <li>• <b>exec-timeout</b> <i>minutes</i></li> <li>• <b>absolute-timeout</b> <i>minutes</i></li> </ul> <b>Example:</b> <pre>switch(config-line)# exec-timeout 30</pre> <b>Example:</b> <pre>switch(config-line)# absolute-timeout 30</pre>	<p>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.</p> <p>Sets a timeout interval on a virtual terminal (vty) line. The range is from 0 to 10000.</p> <p>The <b>absolute-timeout</b> command terminates the connection after the specified time period has elapsed, regardless of whether the connection is being used at the time of termination. You can specify an absolute-timeout value for each port. The user is given 20 seconds notice before the session is terminated. You can use this command along with the <b>logout-warning</b> command, which notifies the user of an impending logout.</p>

	Command or Action	Purpose
<b>Step 4</b>	<b>exit</b> <b>Example:</b> <pre>switch(config-line) # exit switch(config) #</pre>	Exits line configuration mode.
<b>Step 5</b>	(Optional) <b>show running-config all   begin vty</b> <b>Example:</b> <pre>switch(config) # show running-config all   begin vty</pre>	Displays the virtual terminal configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config) # copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## Configuring the Session Limit

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>line vty</b> <b>Example:</b> <pre>switch# line vty switch(config-line) #</pre>	Enters line configuration mode.
<b>Step 3</b>	<b>session-limit sessions</b> <b>Example:</b> <pre>switch(config-line) # session-limit 10</pre>	Configures the maximum number of virtual sessions for the Cisco NX-OS device. The range is from 1 to 60. The default is 32.

	Command or Action	Purpose
<b>Step 4</b>	<b>exit</b> <b>Example:</b> <pre>switch(config-line)# exit switch(config)#</pre>	Exits line configuration mode.
<b>Step 5</b>	(Optional) <b>show running-config all   begin vty</b> <b>Example:</b> <pre>switch(config)# show running-config all   begin vty</pre>	Displays the virtual terminal configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## Configuring Modem Connections

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

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

## Enabling a Modem Connection

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

### Before you begin

Log in to the console port.

### SUMMARY STEPS

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

### DETAILED STEPS

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

	Command or Action	Purpose
<b>Step 2</b>	Enter one of the following commands:	Enters COM1 configuration mode or console configuration mode.
	<b>Command</b>	
	<b>line com1</b>	
	<b>line console</b>	
	<b>Example:</b> switch# line com1 switch(config-com1) #	
<b>Step 3</b>	<b>modem in</b>  <b>Example:</b> switch(config-com1) # modem in	Enables modem input on the COM1 or console port.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> switch(config-com1) # exit switch(config) #	Exits COM1 or console configuration mode.
<b>Step 5</b>	(Optional) <b>show line</b>  <b>Example:</b> switch(config) # show line	Displays the console and COM1 settings.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config) # copy running-config startup-config	Copies the running configuration to the startup configuration.

## Downloading the Default Initialization String

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

### Before you begin

Log in to the console port.

### SUMMARY STEPS

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



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b>  switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	Enter one of the following commands:	
	<b>Option</b>	<b>Description</b>
	<b>line com1</b>	Enters COM1 configuration mode.
	<b>line console</b>	Enters console configuration mode.
	<b>Example:</b>  switch# line com1 switch(config-com1)#	
Step 3	<b>modem init-string default</b>  <b>Example:</b>  switch(config-com1)# modem init-string default	Writes the default initialization string to the modem.
Step 4	<b>exit</b>  <b>Example:</b>  switch(config-com1)# exit switch(config)#	Exits COM1 or console configuration mode.
Step 5	(Optional) <b>show line</b>  <b>Example:</b>  switch(config)# show line	Displays the COM1 and console settings.
Step 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b>  switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Configuring and Downloading a User-Specified Initialization String

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

### Before you begin

Log in to the console port.

## SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:

3. **modem set-string user-input** *string*
4. **modem init-string user-input**
5. **exit**
6. (Optional) **show line**
7. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose						
Step 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.						
Step 2	Enter one of the following commands:							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><b>line com1</b></td><td>Enters COM1 configuration mode.</td></tr><tr><td><b>line console</b></td><td>Enters console configuration mode.</td></tr></table>		Option	Description	<b>line com1</b>	Enters COM1 configuration mode.	<b>line console</b>	Enters console configuration mode.
	Option		Description					
	<b>line com1</b>		Enters COM1 configuration mode.					
	<b>line console</b>		Enters console configuration mode.					
<b>Example:</b> <pre>switch# line com1 switch(config-com1)#</pre>								
Step 3	<b>modem set-string user-input</b> <i>string</i>  <b>Example:</b> <pre>switch(config-com1)# modem set-string user-input ATE0Q1&amp;D2&amp;C1S0=3\015</pre>	Sets the user-specified initialization string for the COM1 or console port. The initialization string is alphanumeric and case sensitive, can contain special characters, and has a maximum of 100 characters.  <b>Note</b> You must first set the user-input string before initializing the string.						
Step 4	<b>modem init-string user-input</b>  <b>Example:</b> <pre>switch(config-com1)# modem init-string user-input</pre>	Writes the user-specified initialization string to the modem connected to the COM1 or console port.						
Step 5	<b>exit</b>  <b>Example:</b> <pre>switch(config-com1)# exit switch(config)#</pre>	Exits COM1 or console configuration mode.						
Step 6	(Optional) <b>show line</b>  <b>Example:</b> <pre>switch(config)# show line</pre>	Displays the COM1 and console settings.						
Step 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b>	Copies the running configuration to the startup configuration.						

	Command or Action	Purpose
	<code>switch(config)# copy running-config startup-config</code>	

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

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

### Before you begin

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

Enable the modem connection on the port.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>modem connect line {com1   console}</b>  <b>Example:</b> <code>switch# modem connect line com1</code>	Initializes the modem connected to the device.

### Related Topics

[Enabling a Modem Connection](#), on page 71

## Clearing Terminal Sessions

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>show users</b>  <b>Example:</b> <code>switch# show users</code>	Displays the user sessions on the device.

	Command or Action	Purpose
<b>Step 2</b>	<b>clear line</b> <i>name</i>  <b>Example:</b> switch# clear line pts/0	Clears a terminal session on a specific line. The line name is case sensitive.

## Displaying Terminal and Session Information

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

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

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

## Default Settings for File System Parameters

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

*Table 14: Default File System Settings*

Parameter	Default
Default filesystem	bootflash:

## Additional References for Terminal Settings and Sessions

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

## Related Documents for Terminal Settings and Sessions

Related Topic	Document Title
Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	



## CHAPTER 7

# Basic Device Management

This chapter describes how to configure, manage, and verify the basic setting on your Cisco NX-OS device.

- [Finding Feature Information, on page 77](#)
- [Default Settings for Basic Device Parameters, on page 77](#)
- [Information About Basic Device Management, on page 78](#)
- [Changing the Device Hostname, on page 79](#)
- [Configuring the MOTD Banner, on page 80](#)
- [Configuring the EXEC Banner, on page 81](#)
- [Configuring the Time Zone, on page 82](#)
- [Configuring Summer Time \(Daylight Saving Time\), on page 83](#)
- [Manually Setting the Device Clock, on page 84](#)
- [Setting the Clock Manager, on page 85](#)
- [Managing Users, on page 85](#)
- [Verifying the Device Configuration, on page 86](#)
- [Additional References for Basic Device Management, on page 87](#)

## Finding Feature Information

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

## Default Settings for Basic Device Parameters

This table lists the default settings for basic device parameters.

**Table 15: Default Basic Device Parameters**

Parameters	Default
MOTD banner text	User Access Verification

Parameters	Default
Clock time zone	UTC

## Information About Basic Device Management

This section provides information about basic device management.

### Device Hostname

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

### Message-of-the-Day Banner

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

### EXEC Banner

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

### Device Clock

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

### Clock Manager

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

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

### Time Zone and Summer Time (Daylight Saving Time)

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

## User Sessions

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

## Changing the Device Hostname

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>{hostname   switchname} name</b>  <b>Example:</b> Using the <b>hostname</b> command: <pre>switch(config)# hostname Engineering1 Engineering1(config)#</pre> Using the <b>switchname</b> command: <pre>Engineering1(config)# switchname Engineering2 Engineering2(config)#</pre>	<b>Note</b> The <b>switchname</b> command performs the same function as the <b>hostname</b> command.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>Engineering2(config)# exit Engineering2#</pre>	Exits global configuration mode.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <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 254 characters per line
- Maximum of 40 lines

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>banner motd</b> <i>delimiting-character message delimiting-character</i>  <b>Example:</b> <pre>switch(config)# banner motd #Welcome to the Switch# switch(config)#</pre>	Configures the MOTD banner. Do not use the <i>delimiting-character</i> in the <i>message</i> text.  <b>Note</b> Do not use " or % as a delimiting character.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
<b>Step 4</b>	(Optional) <b>show banner motd</b>  <b>Example:</b> <pre>switch# show banner motd</pre>	Displays the configured MOTD banner.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.



# Configuring the EXEC Banner

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

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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>banner exec</b> <i>delimiting-character message delimiting-character</i>  <b>Example:</b> <pre>switch(config)# banner exec #Welcome to the Test# switch(config)#</pre>	Configures the EXEC banner. Do not use the <i>delimiting-character</i> in the <i>message</i> text.
<b>Step 3</b>	(Optional) <b>no banner exec</b>  <b>Example:</b> <pre>switch(config)# no banner exec</pre>	Resets the value of EXEC banner to the default value.  <b>Note</b> The default value of the EXEC banner is blank.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
<b>Step 5</b>	(Optional) <b>show banner exec</b>  <b>Example:</b> <pre>switch# show banner exec</pre>	Displays the configured EXEC banner.

	Command or Action	Purpose
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

### Configuring the EXEC Banner

This example shows how to configure the EXEC banner.

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

## Configuring the Time Zone

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>clock timezone</b> <i>zone-name offset-hours offset-minutes</i>  <b>Example:</b> <pre>switch(config)# clock timezone EST -5 0</pre>	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.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.

	Command or Action	Purpose
<b>Step 4</b>	(Optional) <b>show clock</b>  <b>Example:</b> <code>switch# show clock</code>	Displays the time and time zone.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Configuring Summer Time (Daylight Saving Time)

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

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

## Manually Setting the Device Clock

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

### Before you begin

Configure the time zone.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>clock set</b> <i>time day month year</i> <b>Example:</b> <pre>switch# clock set 15:00:00 30 May 2008 Fri May 30 15:14:00 PDT 2008</pre>	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 <b>January, February, March, April, May, June, July, August, September, October, November, and December</b> . The range for the <i>year</i> argument is from 2000 to 2030.
<b>Step 2</b>	(Optional) <b>show clock</b> <b>Example:</b> <pre>switch(config)# show clock</pre>	Displays the current clock value.

### Related Topics

[Configuring the Time Zone](#), on page 82

# Setting the Clock Manager

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

## SUMMARY STEPS

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

## DETAILED STEPS

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

### SUMMARY STEPS

1. **show users**

### DETAILED STEPS

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

## Sending a Message to Users

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

## Verifying the Device Configuration

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

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

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

## Additional References for Basic Device Management

You can find additional information related to basic device management.

### Related Documents for Basic Device Management

Related Topic	Document Title
Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	<i>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference</i>







## CHAPTER 8

# Using the Device File Systems, Directories, and Files

---

This chapter describes how to use your device file systems, directories, and files.

- [Finding Feature Information, on page 89](#)
- [Information About Device File Systems, Directories, Files, and External Storage Devices, on page 89](#)
- [Working with Directories, on page 91](#)
- [Working with Files, on page 93](#)
- [Working with Archive Files, on page 98](#)
- [Examples of Using a File System, on page 101](#)
- [Default Settings for File System Parameters, on page 105](#)
- [Additional References for File Systems, on page 105](#)

## Finding Feature Information

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

## Information About Device File Systems, Directories, Files, and External Storage Devices

This section describes the file systems, directories, files, and support provided to the external storage devices on devices.

### File Systems

This topic provides information about the file system components supported on a Cisco MDS device. (The syntax for specifying a local file system is `filesystem:[//modules/]`.)



**Note** The default *filesystem* parameter is bootflash:.

This table describes the file system components that you can use on a Cisco MDS device.

**Table 16: File System Components**

File System Name	Module	Description
bootflash	sup-active sup-local	Internal CompactFlash memory located on an 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 a 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 an active supervisor module. Used for storing file statistics logs.
system	—	Memory on a supervisor module. Used for storing the running configuration file.
debug	—	Memory on a supervisor module. Used for storing the debug logs.

## Directories

You can create directories on bootflash: and external flash memory (slot0:, usb1:, and usb2:). You can create, store, and access files from directories.

## Files

You can create and access files from bootflash:, volatile:, slot0:, usb1:, and usb2: file systems. You can only access files from the system: file system. Use the debug: file system to store the debug log files specified using the **debug logfile** command.

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

## Working with Directories

### Identifying the Current Directory

You can display the directory name of your current directory.

#### SUMMARY STEPS

1. `pwd`

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>pwd</b>  <b>Example:</b> switch# pwd	Displays the name of your current directory.

### Changing the Current Directory

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

#### SUMMARY STEPS

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

#### DETAILED STEPS

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

### Creating a Directory

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

## SUMMARY STEPS

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

## DETAILED STEPS

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

## SUMMARY STEPS

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

## DETAILED STEPS

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

## Deleting a Directory

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

### Before you begin

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

## SUMMARY STEPS

1. (Optional) **pwd**

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) <b>pwd</b>  <b>Example:</b> switch# pwd	Displays the name of your current default directory.
Step 2	(Optional) <b>dir</b> [ <i>filesystem</i> :[// <i>module</i> ]/][ <i>directory</i> ]  <b>Example:</b> 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	<b>rmdir</b> [ <i>filesystem</i> :[// <i>module</i> ]/] <i>directory</i>  <b>Example:</b> switch# rmdir test	Deletes a directory. The file system and directory name are case sensitive.

## Accessing the Directories on a Standby Supervisor Module

You can access all the file systems on a standby supervisor module (remote) from a session on an active supervisor module. This feature is useful when copying files to the active supervisor module that requires similar files to exist, as in the standby supervisor module.

To access the file systems on the standby supervisor module from a session on the active supervisor module, specify the standby supervisor module in the path to the file using either the *filesystem://sup-remote/* command, or the *filesystem://sup-standby/* command.

## Working with Files

### Moving Files

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



#### Caution

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

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

## SUMMARY STEPS

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

3. **move** [*filesystem:[//module/][directory /] | directory/*]*source-filename* { [*filesystem:[//module/][directory /] | directory/*]*[target-filename]* | *target-filename*}

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>pwd</b>  <b>Example:</b> switch# pwd	Displays the name of your current default directory.
<b>Step 2</b>	(Optional) <b>dir</b> [ <i>filesystem:[//module/][directory]</i> ]  <b>Example:</b> switch# dir bootflash	Displays the contents of the current directory. The file system and directory name are case sensitive.
<b>Step 3</b>	<b>move</b> [ <i>filesystem:[//module/][directory /]   directory/</i> ] <i>source-filename</i> { [ <i>filesystem:[//module/][directory /]   directory/</i> ] <i>[target-filename]</i>   <i>target-filename</i> }  <b>Example:</b> 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.



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

## SUMMARY STEPS

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

## DETAILED STEPS

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

	Command or Action	Purpose
<b>Step 2</b>	(Optional) <b>dir</b> [ <i>filesystem:[//module/][directory]</i> ]  <b>Example:</b> switch# dir bootflash	Displays the contents of the current directory. The file system and directory name are case sensitive.
<b>Step 3</b>	<b>copy</b> [ <i>filesystem:[//module/][directory/]   directory/]source-filename   {filesystem:[//module/][directory/]   directory/}{target-filename}</i>  <b>Example:</b> 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.  The copy command supports ftp, scp, sftp, tftp and http protocols.

## Deleting Files

You can delete a file from a directory.

### SUMMARY STEPS

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

### DETAILED STEPS

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

## Displaying File Contents

You can display the contents of a file.

### SUMMARY STEPS

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

## DETAILED STEPS

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

## Displaying File Checksums

You can display checksums to check the file integrity.

## SUMMARY STEPS

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

## DETAILED STEPS

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

## Compressing and Uncompressing Files

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

## SUMMARY STEPS

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

## DETAILED STEPS

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



	Command or Action	Purpose
<b>Step 3</b>	<b>gunzip</b> <i>[filesystem:[//module/]][directory/]   directory/]filename .gz</i>  <b>Example:</b> switch# gunzip show_tech.gz	Uncompresses a file. The file to uncompress must have the .gz suffix. After the file is uncompressed, it does not have the .gz suffix.

## Displaying the Last Lines in a File

You can display the last lines of a file.

### SUMMARY STEPS

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

### DETAILED STEPS

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

## Redirecting show Command Output to a File

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

## Finding Files

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

### SUMMARY STEPS

1. (Optional) **pwd**

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

## DETAILED STEPS

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

# Working with Archive Files

## Creating an Archive Files

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

- bzip2
- gzip
- Uncompressed

The default is gzip.

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>tar create</b> {bootflash:   volatile:} archive-filename [absolute] [bz2-compress] [gz-compress] [remove] [uncompressed] [verbose] filename-list	Creates an archive file and adds files to it. The filename is alphanumeric, not case sensitive, and has a maximum length of 240 characters.  The <b>absolute</b> keyword specifies that the leading backslash characters (\) should not be removed from the names of the

	Command or Action	Purpose
		<p>files added to the archive file. By default, the leading backslash characters are removed.</p> <p>The <b>bz2-compress</b>, <b>gz-compress</b>, and <b>uncompressed</b> 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"> <li>• For <b>bz2-compress</b>, the extension is .tar.bz2.</li> <li>• For <b>gz-compress</b>, the extension is .tar.gz.</li> <li>• For <b>uncompressed</b>, the extension is .tar.</li> </ul> <p>The <b>remove</b> 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 <b>verbose</b> 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 create a gzip compressed archive file:

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

## Appending Files to an Archive File

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

### Before you begin

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>tar append</b> {bootflash:   volatile:} <i>archive-filename</i> [ <b>absolute</b> ] [ <b>remove</b> ] [ <b>verbose</b> ] <i>filename-list</i>	<p>Adds files to an existing archive file. The archive filename is not case sensitive.</p> <p>The <b>absolute</b> keyword specifies that the leading backslash characters (\) should not be removed from the names of the</p>

	Command or Action	Purpose
		<p>files added to the archive file. By default, the leading backslash characters are removed.</p> <p>The <b>remove</b> 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 <b>verbose</b> 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 Cisco NX-OS device.

### Before you begin

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

### SUMMARY STEPS

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

### DETAILED STEPS

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

	Command or Action	Purpose
		The <b>verbose</b> keyword specifies that the Cisco NX-OS software should display the names of the files as they are extracted.

### Example

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

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

## Displaying the Filenames in an Archive File



**Note** The archive filename is not case sensitive.

To display the file names in an archive file, run the following command:

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

Example:

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

## Examples of Using a File System

This section includes examples of using a file system on a device.

## Accessing Directories on a Standby Supervisor Module

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

```
switch# dir bootflash://sup-remote
12198912   Aug 27 16:29:18 2003  m9500-sflek9-kickstart-mzg.1.3.0.39a.bin
 1864931   Apr 29 12:41:59 2003  dplug2
   12288   Apr 18 20:23:11 2003  lost+found/
12097024   Nov 21 16:34:18 2003  m9500-sflek9-kickstart-mz.1.3.1.1.bin
41574014   Nov 21 16:34:47 2003  m9500-sflek9-mz.1.3.1.1.bin
```

```
Usage for bootflash://sup-remote
67747169 bytes used
116812447 bytes free
184559616 bytes total
```

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

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

## Moving Files

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

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

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

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

## Copying Files

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

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

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

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

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

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




---

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

---

## Deleting a Directory

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

### Before you begin

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

### SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>pwd</b>  <b>Example:</b> switch# pwd	Displays the name of your current default directory.
<b>Step 2</b>	(Optional) <b>dir</b> [ <i>filesystem</i> :[ <i>//module</i> ]][ <i>directory</i> ]  <b>Example:</b> 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.
<b>Step 3</b>	<b>rmdir</b> [ <i>filesystem</i> :[ <i>//module</i> ]][ <i>directory</i> ]  <b>Example:</b> switch# rmdir test	Deletes a directory. The file system and directory name are case sensitive.

## Displaying File Contents

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

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

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

```
switch# show file myfile
```

## Displaying File Checksums

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

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

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

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

## Compressing and Uncompressing Files

This example shows how to compress a file:

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

This example shows how to uncompress a compressed file:

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

## Redirecting show Command Output

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

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

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

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

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

```
switch# show interface > tftp://10.10.1.1/home/configs/switch-intf.cfg
Preparing to copy...done
```

This example shows how to direct the output of the **show tech-support** command to a file:

```
switch# show tech-support > Samplefile
Building Configuration ...
switch# dir
 1525859      Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
 1527808 bytes used
 19443712 bytes free
 20971520 bytes total
```

## Finding Files

This example shows how to find a file in the current default directory:

```
switch# find smm_shm.cfg
/usr/bin/find: ./lost+found: Permission denied
```



```
./smm_shm.cfg  
./newer-fs/isan/etc/routing-sw/smm_shm.cfg  
./newer-fs/isan/etc/smm_shm.cfg
```

## Default Settings for File System Parameters

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

**Table 17: Default File System Settings**

Parameter	Default
Default filesystem	bootflash:

## Additional References for File Systems

This section includes additional information related to the file systems.

### Related Documents for File Systems

Related Topic	Document Title
Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	<i>Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference</i>





## CHAPTER 9

# Working with Configuration Files

This chapter describes how to work with your device configuration files.

- [Finding Feature Information, on page 107](#)
- [Information About Configuration Files, on page 107](#)
- [Managing Configuration Files, on page 108](#)
- [Verifying the Device Configuration, on page 118](#)
- [Examples of Working with Configuration Files, on page 118](#)
- [Additional References for Configuration Files, on page 119](#)

## Finding Feature Information

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

## Information About Configuration Files

Configuration files contain the Cisco NX-OS software commands used to configure the features on a Cisco NX-OS device. Commands are parsed (translated and executed) by the Cisco NX-OS software when the system is booted (from the startup-config file) or when you enter commands at the CLI in a configuration mode.

To change the startup configuration file, you can either save the running-configuration file to the startup configuration using the **copy running-config startup-config** command or copy a configuration file from a file server to the startup configuration.

## Types of Configuration Files

The Cisco NX-OS software has two types of configuration files, running configuration and startup configuration. The device uses the startup configuration (startup-config) during device startup to configure the software features. The running configuration (running-config) contains the current changes that you make to the startup-configuration file. The two configuration files can be different. You might want to change the device configuration for a short time period rather than permanently. In this case, you would change the running

configuration by using commands in global configuration mode but not save the changes to the startup configuration.

To change the running configuration, use the **configure terminal** command to enter global configuration mode. As you use the Cisco NX-OS configuration modes, commands generally are executed immediately and are saved to the running configuration file either immediately after you enter them or when you exit a configuration mode.

To change the startup-configuration file, you can either save the running configuration file to the startup configuration or download a configuration file from a file server to the startup configuration.

#### Related Topics

[Saving the Running Configuration to the Startup Configuration](#), on page 108

[Downloading the Startup Configuration From a Remote Server](#), on page 110

## Managing Configuration Files

This section describes how to manage configuration files.

### Saving the Running Configuration to the Startup Configuration

You can save the running configuration to the startup configuration to save your changes for the next time you that reload the device.

#### SUMMARY STEPS

1. (Optional) **show running-config**
2. **copy running-config startup-config**

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>show running-config</b>  <b>Example:</b> switch# show running-config	Displays the running configuration.
<b>Step 2</b>	<b>copy running-config startup-config</b>  <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

### Copying a Configuration File to a Remote Server

You can copy a configuration file stored in the internal memory to a remote server as a backup or to use for configuring other Cisco NX-OS devices.

#### SUMMARY STEPS

1. **copy running-config** *scheme://server/[url /]filename*

## 2. `copy startup-config scheme://server/[url /]filename`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b><code>copy running-config scheme://server/[url /]filename</code></b> <b>Example:</b> <pre>switch# copy running-config tftp://10.10.1.1/sw1-run-config.bak</pre>	<p>Copies the running-configuration file to a remote server.</p> <p>For the <i>scheme</i> argument, you can enter <b>tftp:</b>, <b>ftp:</b>, <b>scp:</b>, or <b>sftp:</b>. 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>
Step 2	<b><code>copy startup-config scheme://server/[url /]filename</code></b> <b>Example:</b> <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 <b>tftp:</b>, <b>ftp:</b>, <b>scp:</b>, or <b>sftp:</b>. 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

## Downloading the Running Configuration From a Remote Server

You can configure your Cisco NX-OS device by using configuration files that you created on another Cisco NX-OS device and uploaded to a remote server. You then download the file from the remote server to your device using TFTP, FTP, Secure Copy (SCP), or Secure Shell FTP (SFTP) to the running configuration.

### Before you begin

Ensure that the configuration file that you want to download is in the correct directory on the remote server.

Ensure that the permissions on the file are set correctly. Permissions on the file should be set to world-read.

Ensure that your Cisco NX-OS device has a route to the remote server. The Cisco NX-OS device and the remote server must be in the same subnetwork if you do not have a router or a default gateway to route traffic between subnets.

Check connectivity to the remote server using the **ping** or **ping6** command.

### SUMMARY STEPS

1. **`copy scheme://server/[url /]filename running-config`**
2. (Optional) **`show running-config`**
3. (Optional) **`copy running-config startup-config`**
4. (Optional) **`show startup-config`**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>copy</b> <i>scheme://server/[url]/filename</i> <b>running-config</b> <b>Example:</b> <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 <b>tftp:</b> , <b>ftp:</b> , <b>scp:</b> , or <b>sftp:</b> . 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.
<b>Step 2</b>	(Optional) <b>show running-config</b> <b>Example:</b> <pre>switch# show running-config</pre>	Displays the running configuration.
<b>Step 3</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.
<b>Step 4</b>	(Optional) <b>show startup-config</b> <b>Example:</b> <pre>switch# show startup-config</pre>	Displays the startup configuration.

## Downloading the Startup Configuration From a Remote Server

You can configure your Cisco NX-OS device by using configuration files that you created on another Cisco NX-OS device and uploaded to a remote server. You then download the file from the remote server to your device using TFTP, FTP, Secure Copy (SCP), or Secure Shell FTP (SFTP) to the startup configuration.



**Caution** This procedure disrupts all traffic on the Cisco NX-OS device.

### Before you begin

Log in to a session on the console port.

Ensure that the configuration file that you want to download is in the correct directory on the remote server.

Ensure that the permissions on the file are set correctly. Permissions on the file should be set to world-read.

Ensure that your Cisco NX-OS device has a route to the remote server. The Cisco NX-OS device and the remote server must be in the same subnetwork if you do not have a router or a default gateway to route traffic between subnets.

Check connectivity to the remote server using the **ping** or **ping6** command.

## SUMMARY STEPS

1. write erase

2. **reload**
3. **copy *scheme://server/[url /]filename* running-config**
4. **copy running-config startup-config**
5. (Optional) **show startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>write erase</b>  <b>Example:</b> <pre>switch# write erase</pre>	Erases the startup configuration file.
<b>Step 2</b>	<b>reload</b>  <b>Example:</b> <pre>switch# reload This command will reboot the system. (y/n)? [n] y ... Enter the password for "admin": &lt;password&gt; Confirm the password for "admin": &lt;password&gt; ... Would you like to enter the basic configuration dialog (yes/no): n switch#</pre>	Reloads the Cisco NX-OS device.  <b>Note</b> Do not use the setup utility to configure the device.
<b>Step 3</b>	<b>copy <i>scheme://server/[url /]filename</i> running-config</b>  <b>Example:</b> <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 <b>tftp:</b> , <b>ftp:</b> , <b>scp:</b> , or <b>sftp:</b> . 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.
<b>Step 4</b>	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Saves the running configuration file to the startup configuration file.
<b>Step 5</b>	(Optional) <b>show startup-config</b>  <b>Example:</b> <pre>switch# show startup-config</pre>	Displays the running configuration.

## Copying Configuration Files to an External Flash Memory Device

You can copy configuration files to an external flash memory device as a backup for later use.

### Before you begin

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

## SUMMARY STEPS

1. (Optional) **dir** {slot0: | usb1: | usb2:}[directory/]
2. **copy running-config** {slot0: | usb1: | usb2:}[directory/]filename
3. **copy startup-config** {slot0: | usb1: | usb2:}[directory/]filename

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>dir</b> {slot0:   usb1:   usb2:}[directory/]  <b>Example:</b> switch# dir slot0:	Displays the files on the external flash memory device.
<b>Step 2</b>	<b>copy running-config</b> {slot0:   usb1:   usb2:}[directory/]filename  <b>Example:</b> switch# copy running-config slot0:dsn-running-config.cfg	Copies the running configuration to an external flash memory device. The <i>filename</i> argument is case sensitive.
<b>Step 3</b>	<b>copy startup-config</b> {slot0:   usb1:   usb2:}[directory/]filename  <b>Example:</b> switch# copy startup-config slot0:dsn-startup-config.cfg	Copies the startup configuration to an external flash memory device. The <i>filename</i> argument is case sensitive.

## Copying the Running Configuration from an External Flash Memory Device

You can configure your Cisco NX-OS device by copying configuration files created on another Cisco NX-OS device and saved to an external flash memory device.

### Before you begin

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

## SUMMARY STEPS

1. (Optional) **dir** {slot0: | usb1: | usb2:}[directory/]
2. **copy** {slot0: | usb1: | usb2:}[directory/]filename **running-config**
3. (Optional) **show running-config**
4. (Optional) **copy running-config startup-config**
5. (Optional) **show startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>dir</b> {slot0:   usb1:   usb2:}[directory/]  <b>Example:</b>	Displays the files on the external flash memory device.



	Command or Action	Purpose
	switch# dir slot0:	
<b>Step 2</b>	<b>copy {slot0:   usb1:   usb2:}[directory/]filename running-config</b> <b>Example:</b> switch# copy slot0:dsn-config.cfg running-config	Copies the running configuration from an external flash memory device. The <i>filename</i> argument is case sensitive.
<b>Step 3</b>	(Optional) <b>show running-config</b> <b>Example:</b> switch# show running-config	Displays the running configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.
<b>Step 5</b>	(Optional) <b>show startup-config</b> <b>Example:</b> switch# show startup-config	Displays the startup configuration.

## Copying the Startup Configuration from an External Flash Memory Device

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

### Before you begin

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

### SUMMARY STEPS

1. (Optional) **dir {slot0: | usb1: | usb2:}[directory/]**
2. **copy {slot0: | usb1: | usb2:}[directory/]filename startup-config**
3. (Optional) **show startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>dir {slot0:   usb1:   usb2:}[directory/]</b> <b>Example:</b> switch# dir slot0:	Displays the files on the external flash memory device.
<b>Step 2</b>	<b>copy {slot0:   usb1:   usb2:}[directory/]filename startup-config</b> <b>Example:</b> switch# copy slot0:dsn-config.cfg startup-config	Copies the startup configuration from an external flash memory device. The <i>filename</i> argument is case sensitive.

	Command or Action	Purpose
<b>Step 3</b>	(Optional) <b>show startup-config</b>  <b>Example:</b> switch# show startup-config	Displays the startup configuration.

## Copying Configuration Files to an Internal File System

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

### SUMMARY STEPS

1. **copy running-config** [*filesystem:*][*directory/*] | [*directory/*]*filename*
2. **copy startup-config** [*filesystem:*][*directory/*] | [*directory/*]*filename*

### DETAILED STEPS

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

## SUMMARY STEPS

1. **write erase**
2. **reload**
3. **copy *configuration\_file* running-configuration**
4. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>write erase</b> <b>Example:</b> <pre>switch# write erase</pre>	Clears the current configuration of the switch.
<b>Step 2</b>	<b>reload</b> <b>Example:</b> <pre>switch# reload</pre>	Restarts the device. You will be prompted to provide a kickstart and system image file for the device to boot and run.  <b>Note</b> By default, the <b>reload</b> command reloads the device from a binary version of the startup configuration.  Beginning with Cisco NX-OS 6.2(2), you can use the <b>reload ascii</b> command to copy an ASCII version of the configuration to the start up configuration when reloading the device.
<b>Step 3</b>	<b>copy <i>configuration_file</i> running-configuration</b> <b>Example:</b> <pre>switch# copy bootflash:start-config.bak running-configuration</pre>	Copies a previously saved configuration file to the running configuration.  <b>Note</b> The <i>configuration_file</i> filename argument is case sensitive.
<b>Step 4</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the start-up configuration.

## Removing the Configuration for a Missing Module

When you remove an I/O module from the chassis, you can also remove the configuration for that module from the running configuration.



**Note** You can only remove the configuration for an empty slot in the chassis.

### Before you begin

Remove the I/O module from the chassis.

**SUMMARY STEPS**

1. (Optional) **show hardware**
2. **purge module slot running-config**
3. (Optional) **copy running-config startup-config**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>show hardware</b>  <b>Example:</b> switch# show hardware	Displays the installed hardware for the device.
<b>Step 2</b>	<b>purge module slot running-config</b>  <b>Example:</b> switch# purge module 3 running-config	Removes the configuration for a missing module from the running configuration.
<b>Step 3</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Erasing a Configuration

You can erase the configuration on your device to return to the factory defaults.

You can erase the following configuration files saved in the persistent memory on the device:

- Startup
- Boot
- Debug

The **write erase** command erases the entire startup configuration, except for the following:

- Boot variable definitions
- The IPv4 configuration on the mgmt0 interface, including the following:
  - Address
  - Subnet mask

To remove the boot variable definitions follow step-1 and step-2.

To remove the boot variables, running configuration, and the IP configuration on the management interface follow step-3 to step-5.

**SUMMARY STEPS**

1. **write erase boot**
2. **reload**

3. **write erase**
4. **write erase boot**
5. **reload**

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>write erase boot</b> <b>Example:</b> <pre>switch# write erase boot</pre>	Erases the boot variable definitions.
<b>Step 2</b>	<b>reload</b> <b>Example:</b> <pre>switch# reload</pre>	Restarts the device. You will be prompted to provide a kickstart and system image file for the device to boot and run. By default, the reload command reloads the device from a binary version of the startup configuration.
<b>Step 3</b>	<b>write erase</b> <b>Example:</b> <pre>switch# write erase</pre>	Erases the boot variable definitions.
<b>Step 4</b>	<b>write erase boot</b> <b>Example:</b> <pre>switch# write erase boot</pre>	Erases the boot variable definitions and the IPv4 configuration on the management interface.
<b>Step 5</b>	<b>reload</b> <b>Example:</b> <pre>switch# reload</pre>	Restarts the device. You will be prompted to provide a kickstart and system image file for the device to boot and run. By default, the reload command reloads the device from a binary version of the startup configuration.

## Clearing Inactive Configurations

You can clear inactive Quality of Service (QoS) and/or access control list (ACL) configurations.

#### SUMMARY STEPS

1. (Optional) **show running-config type inactive-if-config**
2. **clear inactive-config policy**
3. (Optional) **show inactive-if-config log**

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>show running-config type inactive-if-config</b> <b>Example:</b>	Displays any inactive ACL or QoS configurations. The values for the <i>type</i> argument are <b>aclmgr</b> and <b>ipqos</b> .

	Command or Action	Purpose
	# show running-config ipqos inactive-if-config	<ul style="list-style-type: none"> <li>• <b>aclmgr</b>—Displays any inactive configurations for aclmgr.</li> <li>• <b>ipqos</b>—Displays any inactive configurations for qosmgr.</li> </ul>
<b>Step 2</b>	<b>clear inactive-config policy</b>  <b>Example:</b> <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 &amp; for other than default vdc: /bootflash/vdc_x/qos_inactive_if_config.cfg (where x is vdc number) 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 <b>qos</b> and <b>acl</b>.</p> <p>The following describes the values:</p> <ul style="list-style-type: none"> <li>• <b>qos</b>—Clears inactive QoS configurations.</li> <li>• <b>acl</b>—Clears inactive ACL configurations.</li> <li>• <b>acl qos</b>—Clears inactive ACL configurations and inactive QoS configurations.</li> </ul>
<b>Step 3</b>	<b>(Optional) show inactive-if-config log</b>  <b>Example:</b> <pre># show inactive-if-config log</pre>	Displays the commands that were used to clear the inactive configurations.

## Verifying the Device Configuration

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

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

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

## Examples of Working with Configuration Files

This section includes examples of working with configuration files.

### Copying Configuration Files

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

### Backing Up Configuration Files

This example shows how to back up the startup configuration to the bootflash: file system (ASCII file):

```
switch# copy startup-config bootflash:my-config
```

This example shows how to back up the startup configuration to the TFTP server (ASCII file):

```
switch# copy startup-config tftp://172.16.10.100/my-config
```

This example shows how to back up the running configuration to the bootflash: file system (ASCII file):

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

## Rolling Back to a Previous Configuration

To roll back your configuration to a snapshot copy of a previously saved configuration, you need to perform the following steps:

1. Clear the current running image with the **write erase** command.
2. Restart the device with the **reload** command.



---

**Note** By default, the **reload** command reloads the device from a binary version of the startup configuration.

---

3. Copy the previously saved configuration file to the running configuration with the **copy configuration\_file running-configuration** command.
4. Copy the running configuration to the start-up configuration with the **copy running-config startup-config** command.

## Additional References for Configuration Files

This section includes additional information related to managing configuration files.

### Related Documents for Configuration Files

Related Topic	Document Title
Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	

