



Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide, Release 6.x

First Published: April 09, 2013

Last Modified: April 09, 2013

Americas Headquarters

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

Text Part Number: OL-29291-02



CONTENTS

Preface

Preface **xiii**

Audience **xiii**

Document Conventions **xiii**

Related Documentation **xiv**

Obtaining Documentation and Submitting a Service Request **xvi**

CHAPTER 1

Overview **1**

Software Compatibility **1**

Modular Software Design **1**

Serviceability **1**

Switched Port Analyzer **2**

Call Home **2**

Online Diagnostics **2**

Embedded Event Manager **2**

Manageability **2**

Simple Network Management Protocol **2**

Role-Based Access Control **3**

Cisco NX-OS Software Configuration **3**

Tools for Software Configuration **3**

CLI **3**

NTP **4**

Licensing **5**

Quality of Service **5**

CHAPTER 2

Using the Cisco NX-OS Setup Utility **7**

Information About the Cisco NX-OS Setup Utility **7**

Prerequisites for the Setup Utility **9**

Initial Setup Routine	9
Configuring Out-of-Band Management	9
Configuring In-Band Management	15
Where to Go Next	21

CHAPTER 3

Using PowerOn Auto Provisioning	23
Network Requirements for POAP	23
POAP Configuration Script	24
POAP Process	25
Power-Up Phase	26
DHCP Discovery Phase	27
Script Execution Phase	28
Post-Installation Reload Phase	29
Guidelines and Limitations for POAP	29
Setting Up the Network Environment to Use POAP	29
Configuring a Switch Using POAP	30
Verifying the Device Configuration	30

CHAPTER 4

Understanding the Command-Line Interface	33
Information About the CLI Prompt	34
Command Modes	34
EXEC Command Mode	34
Global Configuration Command Mode	34
Interface Configuration Command Mode	35
Subinterface Configuration Command Mode	36
Saving and Restoring a Command Mode	36
Command Mode Summary	37
Special Characters	37
Keystroke Shortcuts	38
Abbreviating Commands	40
Completing a Partial Command Name	41
Identifying Your Location in the Command Hierarchy	41
Using the no Form of a Command	42
Configuring CLI Variables	43
About CLI Variables	43

Configuring CLI Session-Only Variables	43
Configuring Persistent CLI Variables	44
Command Aliases	45
About Command Aliases	45
Defining Command Aliases	46
Configuring Command Aliases for a User Session	47
Command Scripts	47
Running a Command Script	47
Echoing Information to the Terminal	48
Delaying Command Action	49
Context-Sensitive Help	49
Understanding Regular Expressions	51
Special Characters	51
Multiple-Character Patterns	51
Anchoring	52
Searching and Filtering show Command Output	52
Filtering and Searching Keywords	53
diff Utility	54
grep and egrep Utilities	55
less Utility	56
sed Utility	56
sort Utility	56
Redirecting show Command Output Using sscp	57
Searching and Filtering from the --More-- Prompt	57
Using the Command History	58
Recalling a Command	59
Configuring the CLI Edit Mode	59
Controlling CLI History Recall	59
Displaying the Command History	60
Enabling or Disabling the CLI Confirmation Prompts	60
Setting CLI Display Colors	61
Sending Commands to Modules	61
BIOS Loader Prompt	62
Examples Using the CLI	63
Defining Command Aliases	63

Using CLI Session Variables	63
Using the System-Defined Timestamp Variable	64
Running a Command Script	64
Using the sscp Utility to Redirect show Command Output	65

CHAPTER 5**Configuring Terminal Settings and Sessions 67**

Information About Terminal Settings and Sessions	67
Terminal Session Settings	67
Console Port	68
COM1 Port	68
Virtual Terminals	69
Modem Support	69
Configuring the Console Port	69
Configuring the COM1 Port	71
Configuring Virtual Terminals	73
Configuring the Inactive Session Timeout	73
Configuring the Session Limit	74
Configuring Modem Connections	75
Enabling a Modem Connection	75
Downloading the Default Initialization String	77
Configuring and Downloading a User-Specified Initialization String	78
Initializing a Modem for a Powered-Up Cisco NX-OS Device	79
Clearing Terminal Sessions	80
Displaying Terminal and Session Information	80
Default Settings for Terminal Display and Session Parameters	81

CHAPTER 6**Basic Device Management 83**

Information About Basic Device Management	83
Device Hostname	83
Management Interface	84
Default Gateway	84
Message-of-the-Day Banner	84
Device Clock	85
Time Zone and Summer Time (Daylight Saving Time)	85
User Sessions	85

Telnet Server Connection	85
Changing the Device Hostname	85
Configuring the Management Interface	86
Configuring the Default Gateway	88
Configuring the MOTD Banner	88
Configuring the Time Zone	89
Configuring Summer Time (Daylight Saving Time)	90
Manually Setting the Device Clock	92
Managing Users	92
Displaying Information about the User Sessions	92
Sending a Message to Users	93
Enabling or Disabling a Telnet Server Connection	93
Verifying the Device Configuration	94
Default Settings for Basic Device Parameters	95

CHAPTER 7**Using the Device File Systems, Directories, and Files 97**

Information About the Device File Systems, Directories, and Files	97
File Systems	97
Directories	99
Files	99
Formatting External Flash Devices	99
Working with Directories	100
Identifying the Current Directory	100
Changing the Current Directory	100
Creating a Directory	101
Displaying Directory Contents	102
Deleting a Directory	102
Accessing Directories on the Standby Supervisor Module	103
Working with Files	103
Moving Files	103
Copying Files	104
Deleting Files	105
Displaying File Contents	105
Displaying File Checksums	106
Compressing and Uncompressing Files	106

Displaying the Last Lines in a File	107
Redirecting show Command Output to a File	107
Finding Files	108
Working with Archive Files	109
Creating an Archive Files	109
Appending Files to an Archive File	110
Extracting Files from an Archive File	111
Displaying the Filenames in an Archive File	111
Examples of Using the File System	112
Accessing Directories on Standby Supervisor Modules	112
Moving Files	112
Copying Files	112
Deleting a Directory	113
Displaying File Contents	113
Displaying File Checksums	114
Compressing and Uncompressing Files	114
Redirecting show Command Output	114
Finding Files	115
Default Settings for File System Parameters	115

CHAPTER 8

Working with Configuration Files	117
Information About Configuration Files	117
Types of Configuration Files	117
Managing Configuration Files	118
Saving the Running Configuration to the Startup Configuration	118
Copying a Configuration File to a Remote Server	118
Downloading the Running Configuration From a Remote Server	119
Downloading the Startup Configuration From a Remote Server	120
Copying Configuration Files to an External Flash Memory Device	122
Copying the Running Configuration from an External Flash Memory Device	122
Copying the Startup Configuration from an External Flash Memory Device	123
Copying Configuration Files to an Internal File System	124
Rolling Back to a Previous Configuration	125
Removing the Configuration for a Missing Module	126
Erasing a Configuration	127

Verifying the Device Configuration	128
Examples of Working with Configuration Files	128
Copying Configuration Files	128
Backing Up Configuration Files	129
Rolling Back to a Previous Configuration	129

CHAPTER 9**Configuring CDP 131**

Information About CDP	131
CDP Overview	131
High Availability for CDP	132
Configuring CDP	132
Enabling or Disabling CDP Globally	132
Enabling or Disabling CDP on an Interface	133
Configuring Optional CDP Parameters	134
Verifying the CDP Configuration	134
Clearing CDP Counters and Tables	135
CDP Example Configuration	135
Default Settings for CDP	135

CHAPTER 10**Configuring NTP 137**

Information About NTP	137
NTP	137
NTP Configuration Distribution Using CFS	139
High Availability for NTP	139
Prerequisites for NTP	139
Guidelines and Limitations for NTP	139
Configuring NTP	139
Enabling or Disabling the NTP Protocol	140
Configuring an NTP Server and Peer	140
Displaying and Clearing NTP Statistics	141
Distributing the NTP Configuration Using CFS	142
Enabling NTP Configuration Distribution	142
Committing NTP Configuration Changes	143
Discarding NTP Configuration Changes	144
Releasing Fabric Session Lock on the NTP Configuration	145

Verifying NTP Configuration	145
NTP Example Configuration	145
Default Settings for NTP	146

CHAPTER 11**Managing System Hardware 147**

Displaying Switch Hardware Inventory	147
Running CompactFlash Tests	149
Running the CompactFlash CRC Checksum Test On Demand	150
Enabling and Disabling Automatic CompactFlash Firmware Update	150
Setting the CompactFlash CRC Checksum Test Interval	151
Enabling and Disabling Failure Action for a CompactFlash Checksum Test	152
Running the CompactFlash CRC Checksum Test On Demand	153
Updating the CompactFlash Firmware On Demand	153
Enabling and Disabling the Automatic CompactFlash CRC Checksum Test	153
Setting the CompactFlash Firmware Update Interval	154
Enabling and Disabling Failure Action for CompactFlash Firmware Updates	155
Displaying CompactFlash Firmware Update Configuration	156
Displaying CompactFlash CRC Test and Firmware Update Statistics	156
Displaying the Switch Serial Number	157
Displaying Power Usage Information	157
Power Supply Modes	158
Configuration Guidelines for Power Supplies	158
Configuring the Power Supply Mode	161
About Crossbar Management	162
Operational Considerations when Removing Crossbars	163
Gracefully Shutting Down a Crossbar	164
Providing Backward Compatibility for Generation 1 Modules in Cisco MDS 9513 Directors	164
About Module Temperature Monitoring	165
Displaying Module Temperatures	166
About Fan Modules	166
About Clock Modules	168
Displaying Environment Information	169
Default Settings	170

CHAPTER 12**Managing Modules 171**

About Modules 171

Supervisor Modules 172

Switching Modules 174

Services Modules 174

Maintaining Supervisor Modules 174

Replacing Supervisor Modules 174

Standby Supervisor Module Boot Variable Version 175

Standby Supervisor Module Bootflash Memory 175

Standby Supervisor Module Boot Alert 175

Verifying the Status of a Module 175

Checking the State of a Module 176

Connecting to a Module 177

Reloading Modules 178

Reloading a Switch 178

Power Cycling Modules 178

Reloading Switching Modules 179

Saving the Module Configuration 180

Purging Module Configurations 181

Powering Off Switching Modules 181

Identifying Module LEDs 182

EPLD Images 188

Upgrading EPLD Images 188

Displaying EPLD Image Versions 192

SSI Boot Images 193

Installing the SSI Boot Image 193

Upgrading or Downgrading the SSI Boot Image 195

SSI Boot Image Upgrade Considerations for the SSM 195

Verifying the SSI Boot Image 196

Using the install ssi Command 200

Managing SSMs and Supervisor Modules 202

Configuring SSM and MSM Global Upgrade Delay 202

Guidelines for Replacing SSMs and Supervisor Modules 203

Recovering an SSM After Replacing Corrupted CompactFlash Memory 203

Guidelines for Upgrading and Downgrading Cisco MDS NX-OS Releases 204
Default Settings 206



Preface

This preface describes the audience, organization, and conventions of the *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*. It also provides information on how to obtain related documentation.

- [Audience, page xiii](#)
- [Document Conventions, page xiii](#)
- [Related Documentation, page xiv](#)
- [Obtaining Documentation and Submitting a Service Request, page xvi](#)

Audience

This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco MDS 9000 Family of multilayer directors and fabric switches.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
<i>Italic</i>	Italic text indicates arguments for which 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.
<code>boldface screen font</code>	Information you must enter is in boldface screen font.
<i><code>italic screen font</code></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.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS NX-OS Documentation Locator at:

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocator.htm

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*
- *Release Notes for Cisco MDS 9000 Family Fabric Manager*

Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

Compatibility Information

- *Cisco Data Center Interoperability Support Matrix*
- *Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*
- *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*
- *Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*

Hardware Installation

- *Cisco MDS 9710 Director Hardware Installation Guide*
- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9250i Multiservice Switch Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*

Software Installation and Upgrade

- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*
- *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*

Cisco NX-OS

- *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*

- *Cisco MDS 9000 Family NX-OS Licensing Guide*
- *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Security Configuration Guide*
- *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*

Command-Line Interface

- *Cisco MDS 9000 Family Command Reference*

Intelligent Storage Networking Services Configuration Guides

- *Cisco MDS 9000 I/O Acceleration Configuration Guide*
- *Cisco MDS 9000 Family SANTap Deployment Guide*
- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*
- *Cisco MDS 9000 Family Secure Erase Configuration Guide*
- *Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*

Troubleshooting and Reference

- *Cisco NX-OS System Messages Reference*
- *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*
- *Cisco MDS 9000 Family NX-OS MIB Quick Reference*
- *Cisco MDS 9000 Family NX-OS SMI-S Programming Reference*
- *Cisco MDS 9000 Family Fabric Manager Server Database Schema*

Obtaining Documentation and Submitting a Service Request

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

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER

1

Overview

This chapter provides an overview of the Cisco NX-OS software.

- [Software Compatibility, page 1](#)
- [Serviceability, page 1](#)
- [Manageability, page 2](#)
- [Cisco NX-OS Software Configuration, page 3](#)
- [Licensing, page 5](#)
- [Quality of Service, page 5](#)

Software Compatibility

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

Modular Software Design

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

Serviceability

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

Switched Port Analyzer

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

Call Home

The Call Home feature continuously monitors hardware and software components to provide e-mail-based notification of critical system events. A versatile range of message formats is available for optimal compatibility with pager services, standard e-mail, and XML-based automated parsing applications. It offers alert grouping capabilities and customizable destination profiles. You can use this feature, for example, to directly page a network support engineer, send an e-mail message to a network operations center (NOC), and employ Cisco AutoNotify services to directly generate a case with the Cisco Technical Assistance Center (TAC). For more information about Call Home, see the [Cisco MDS 9000 Family NX-OS System Management Configuration Guide](#).

Online Diagnostics

Cisco generic online diagnostics (GOLD) verify that hardware and internal data paths are operating as designed. Boot-time diagnostics, continuous monitoring, and on-demand and scheduled tests are part of the Cisco GOLD feature set. GOLD allows rapid fault isolation and continuous system monitoring. For information about configuring GOLD, see the [Cisco MDS 9000 Family NX-OS System Management Configuration Guide](#).

Embedded Event Manager

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

Manageability

This section describes the manageability features in the Cisco NX-OS software.

Simple Network Management Protocol

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

Role-Based Access Control

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

Cisco NX-OS Software Configuration

This section describes the tools you can use to configure Cisco NX-OS software, and provides an overview of the software configuration process with links to the appropriate chapters.

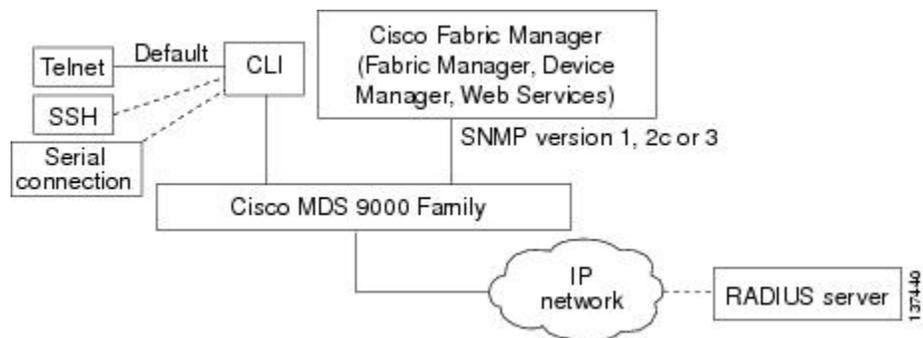
Tools for Software Configuration

You can use one of two configuration management tools to configure your SANs:

- The command-line interface (CLI) can manage Cisco MDS 9000 Family switches using Telnet, SSH, or a serial connection.
- The Cisco MDS 9000 Fabric Manager, a Java-based graphical user interface, can manage Cisco MDS 9000 Family switches using SNMP.

This figure shows the tools for configuring the Cisco NX-OS software.

Figure 1: Tools for Configuring Cisco NX-OS Software



CLI

With the CLI, you can type commands at the switch prompt, and the commands are executed when you press the **Enter** key. The CLI parser provides command help, command completion, and keyboard sequences that allow you to access previously executed commands from the buffer history.

Continue reading this document for more information on configuring the Cisco MDS switch using the CLI.

NTP

In a large enterprise network, having one time standard for all network devices is critical for management reporting and event logging functions when trying to correlate interacting events logged across multiple devices. Many enterprise customers with extremely mission-critical networks maintain their own stratum-1 NTP source.

Time synchronization occurs when several frames are exchanged between clients and servers. The switches in client mode know the address of one or more NTP servers. The servers act as the time source and receive client synchronization requests.

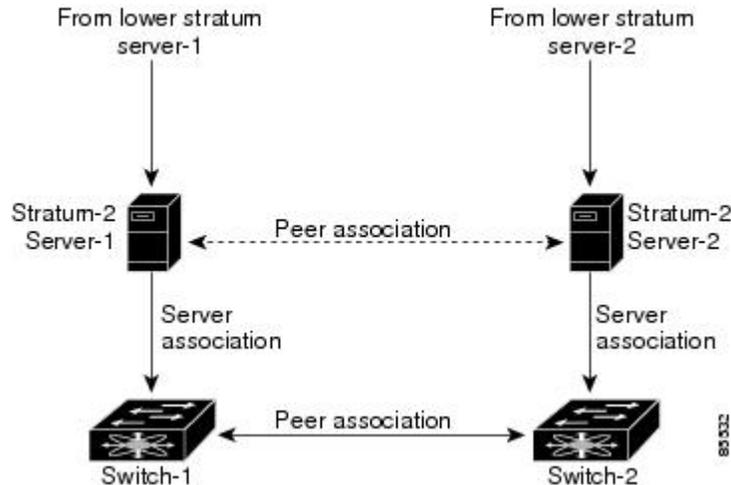
By configuring an IP address as a peer, the Cisco NX-OS device will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both of these instances point to different time servers, your NTP service is more reliable. Even if the active server link is lost, you can still maintain the correct time due to the presence of the peer.

If an active server fails, a configured peer helps in providing the NTP time. To ensure backup support if the active server fails, provide a direct NTP server association and configure a peer.

If you only configure a peer, the most accurate peer takes on the role of the NTP server and the other peer acts as a peer. Both devices end at the correct time if they have the correct time source or if they point to the correct NTP source.

Not even a server down time will affect well-configured switches in the network. This figure displays a network with two NTP stratum 2 servers and two switches.

Figure 2: NTP Peer and Server Association



In this configuration, the switches were configured as follows:

- Stratum-2 Server-1
 - IPv4 address-10.10.10.10
- Stratum-2 Server-2
 - IPv4 address-10.10.10.9

- Switch-1 IPv4 address-10.10.10.1
- Switch-1 NTP configuration
 - NTP server 10.10.10.10
 - NTP peer 10.10.10.2
- Switch-2 IPv4 address-10.10.10.2
- Switch-2 NTP configuration
 - NTP server 10.10.10.9
 - NTP peer 10.10.10.1

Licensing

The Cisco NX-OS software licensing feature allows you to access premium features on the device after you install the appropriate license for that feature. Any feature not included in a license package is bundled with the Cisco NX-OS software and is provided to you at no extra charge.

You must purchase and install a license for each device.

**Note**

You can enable a feature without installing its license. The Cisco NX-OS software gives you a grace period that allows you to try a feature before purchasing its license. You must install the Advanced Services license package to enable the Cisco TrustSec feature.

For detailed information about Cisco NX-OS software licensing, see the [Cisco MDS 9000 Family NX-OS Software Licensing Guide](#).

For information about troubleshooting licensing issues, see the [Cisco MDS 9000 Family NX-OS Troubleshooting Guide](#).

Quality of Service

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



Using the Cisco NX-OS Setup Utility

This chapter contains the following sections:

- [Information About the Cisco NX-OS Setup Utility, page 7](#)
- [Prerequisites for the Setup Utility, page 9](#)
- [Initial Setup Routine, page 9](#)
- [Where to Go Next, page 21](#)

Information About the Cisco NX-OS Setup Utility

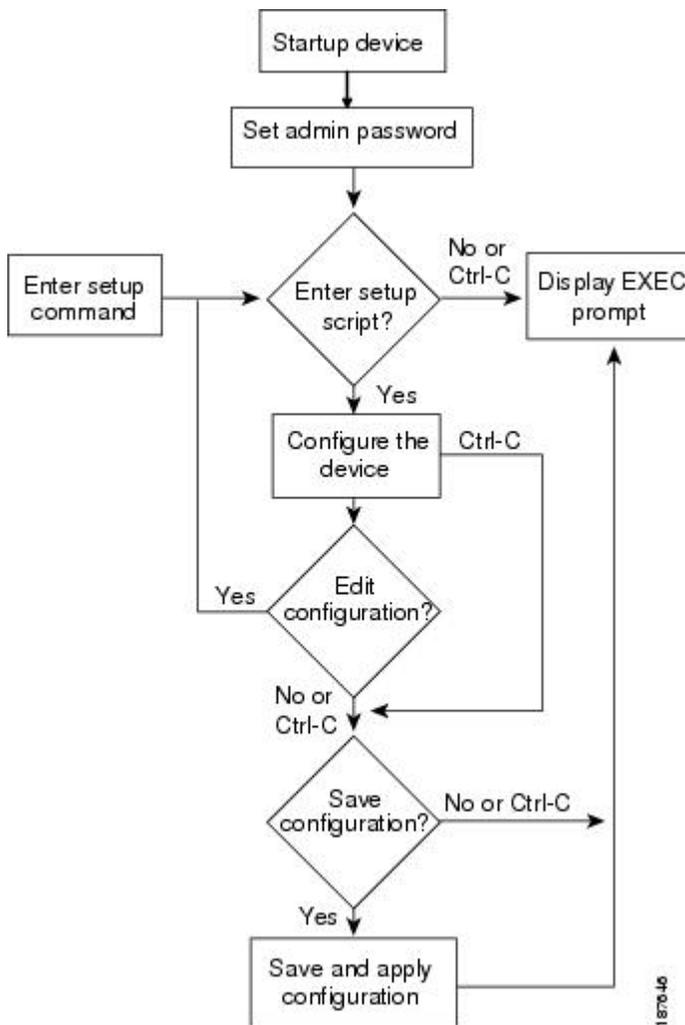
The Cisco NX-OS setup utility is an interactive command-line interface (CLI) mode that guides you through a basic (also called a startup) configuration of the system. The setup utility allows you to configure only enough connectivity for system management.

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

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

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

Figure 3: Setup Script Flow



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



Note

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



Note The setup script only supports IPv4.

Prerequisites for the Setup Utility

The setup utility has the following prerequisites:

- Have a password strategy for your network environment.
- Connect the console port on the supervisor module to the network. If you have dual supervisor modules, connect the console ports on both supervisor modules to the network.
- Connect the Ethernet management port on the supervisor module to the network. If you have dual supervisor modules, connect the Ethernet management ports on both supervisor modules to the network.
- Enable the licensing grace period, if applicable. For detailed information about licensing, see the [Cisco MDS 9000 Family NX-OS Software Licensing Guide](#).

Initial Setup Routine

The first time that you access a switch in the Cisco MDS 9000 Family, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch.

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

Configuring Out-of-Band Management

You can configure out-of-band management on the mgmt 0 interface.



Note You can configure both in-band and out-of-band configuration together by entering Yes in both Step 12c and Step 12d in the following procedure.

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Step 2 Enter yes (yes is the default) to enable secure password standard.

```
Do you want to enforce secure password standard (yes/no): yes
```

Note You can also enable secure password standard using the **password strength-check** command. A secure password should contain characters from at least three of the classes: lower case letters, upper case letters, digits, and special characters.

Step 3 Enter the new password for the administrator.

Enter the password for admin: *admin-password*

Confirm the password for admin: *admin-password*

Tip If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password as shown in the sample configuration. Passwords are case-sensitive.

Step 4 Enter yes to enter the setup mode.

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 5 Enter yes (no is the default) if you do not wish to create additional accounts.

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

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

Note User login IDs must contain non-numeric characters.

a) Enter the user login ID.

Enter the user login ID: *user_name*

b) Enter and confirm the user password.

Enter the password for *user_name*: *user-password*

Confirm the password for *user_name*: *user-password*

c) Assign the user role network-admin (network-operator is the default).

Enter the user role [network-operator]: **network-admin**

Step 6 Configure the read-only or read-write SNMP community string.

- a) Enter yes (no is the default) to avoid configuring the read-only SNMP community string.

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

- b) Enter the SNMP community string.

```
SNMP community string: snmp_community
```

Step 7 Enter a name for the switch.

Note The switch name is limited to 32 alphanumeric characters. The default is switch.

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

Step 8 Enter yes (yes is the default) at the configuration prompt to configure out-of-band management.

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

- a) Enter the mgmt0 IPv4 address.

```
Mgmt0 IPv4 address: ip_address
```

- b) Enter the mgmt0 IPv4 subnet mask.

```
Mgmt0 IPv4 netmask: subnet_mask
```

Step 9 Enter yes (yes is the default) to configure the default gateway.

```
Configure the default-gateway: (yes/no) [y]: yes
```

- a) Enter the default gateway IP address.

```
IP address of the default gateway: default_gateway
```

Step 10 Enter yes (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

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

- a) Enter no (no is the default) at the in-band management configuration prompt.

```
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: no
```

- b) Enter yes (yes is the default) to enable IPv4 routing capabilities.

```
Enable ip routing capabilities? (yes/no) [y]: yes
```

- c) Enter yes (yes is the default) to configure a static route.

Configure static route: (yes/no) [y]: **yes**

Enter the destination prefix.

Destination prefix: *dest_prefix*

Enter the destination prefix mask.

Destination prefix mask: *dest_mask*

Enter the next hop IP address.

Next hop ip address: *next_hop_address*

Note Be sure to configure the IP route, the default network IP address, and the default gateway IP address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

- d) Enter yes (yes is the default) to configure the default network.

Configure the default-network: (yes/no) [y]: **yes**

Enter the default network IPv4 address.

Note The default network IPv4 address is the destination prefix provided in Step 10c.

Default network IP address [dest_prefix]: *dest_prefix*

- e) Enter yes (yes is the default) to configure the DNS IPv4 address.

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

Enter the DNS IP address.

DNS IP address: *name_server*

- f) Enter yes (no is the default) to skip the default domain name configuration.

Configure the default domain name? (yes/no) [n]: **yes**

Enter the default domain name.

Default domain name: *domain_name*

- Step 11** Enter yes (yes is the default) to enable the SSH service.

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

Enter the SSH key type.

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

Enter the number of key bits within the specified range.

```
Enter the number of key bits? (768-2048) [1024]: 2048
```

Step 12 Enter yes (no is the default) to disable the Telnet service.

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

Step 13 Enter yes (yes is the default) to configure congestion or no_credit drop for FC interfaces.

```
Configure congestion or no_credit drop for fc interfaces? (yes/no) [q/quit] to quit [y]:yes
```

Step 14 Enter con(con is the default) to configure congestion or no_credit drop.

```
Enter the type of drop to configure congestion/no_credit drop? (con/no) [c]:con
```

Step 15 Enter a value from 100 to 1000 (d is the default) to calculate the number of milliseconds for congestion or no_credit drop.

```
Enter number of milliseconds for congestion/no_credit drop[100 - 1000] or [d/default] for default:100
```

Step 16 Enter a mode for congestion or no_credit drop.

```
Enter mode for congestion/no_credit drop[E/F]:
```

Step 17 Enter yes (no is the default) to configure the NTP server.

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

Enter the NTP server IPv4 address.

```
NTP server IP address: ntp_server_IP_address
```

Step 18 Enter shut (shut is the default) to configure the default switch port interface to the shut (disabled) state.

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

Note The management Ethernet interface is not shut down at this point. Only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

Step 19 Enter on (off is the default) to configure the switch port trunk mode.

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

Step 20 Enter yes (yes is the default) to configure the switchport mode F.

```
Configure default switchport mode F (yes/no) [n]: y
```

Step 21 Enter on (off is the default) to configure the PortChannel auto-create state.

```
Configure default port-channel auto-create state (on/off) [off]: on
```

Step 22 Enter permit (deny is the default) to deny a default zone policy configuration.

```
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 issuing a **write erase** command, you must explicitly change the default zone policy to permit for VSAN 1 after finishing the script using the following commands:

```
switch# configure terminal
switch(config)# zone default-zone permit vsan 1
```

Step 23 Enter yes (no is the default) to disable a full zone set distribution.

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

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

You see the new configuration. Review and edit the configuration that you have just entered.

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

```
switch# configure terminal
switch(config)# zoneset distribute full vsan 1
```

Step 24 Enter enhanced (basic is the default) to configure default-zone mode as enhanced.

```
Configure default zone mode (basic/enhanced) [basic]: enhanced
```

Overrides the switch-wide default zone mode as enhanced.

Note If you are executing the setup script after issuing a **write erase** command, you must explicitly change the default zoning mode to enhanced for VSAN 1 after finishing the script using the following commands:

```
switch# configure terminal
switch(config)# zone mode enhanced vsan 1
```

Step 25 Enter no (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

```
username admin password admin_pass role network-admin
username user_name password user_pass role network-admin
snmp-server community snmp_community ro
switchname switch
interface mgmt0
  ip address ip_address subnet_mask
  no shutdown
ip routing
ip route dest_prefix dest_mask dest_address
ip default-network dest_prefix
ip default-gateway default_gateway
ip name-server name_server
ip domain-name domain_name
```

```
telnet server disable
ssh key rsa 2048 force
ssh server enable
ntp server ipaddr ntp_server
system default switchport shutdown
system default switchport trunk mode on
system default switchport mode F
system default port-channel auto-create
zone default-zone permit vsan 1-4093
zoneset distribute full vsan 1-4093
system default zone mode enhanced
Would you like to edit the configuration? (yes/no) [n]: n
```

Step 26 Enter yes (yes is default) to use and save this configuration.

```
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 ensures that the kickstart and system images are also automatically configured.

Configuring In-Band Management

The in-band management logical interface is VSAN 1. This management interface uses the Fibre Channel infrastructure to transport IP traffic. An interface for VSAN 1 is created on every switch in the fabric. Each switch should have its VSAN 1 interface configured with either an IPv4 address or an IPv6 address in the same subnetwork. A default route that points to the switch providing access to the IP network should be configured on every switch in the Fibre Channel fabric.



Note You can configure both in-band and out-of-band configuration together by entering Yes in both Step 10c and Step 10d in the following procedure.

SUMMARY STEPS

1. Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.
2. Enter the new password for the administrator.
3. Enter yes to enter the setup mode.
4. Enter yes (yes is the default) to enable secure password standard
5. Enter no (no is the default) if you do not wish to create additional accounts.
6. Configure the read-only or read-write SNMP community string.
7. Enter a name for the switch.
8. Enter no (yes is the default) at the configuration prompt to configure out-of-band management.
9. Enter yes (yes is the default) to configure the default gateway.
10. Enter yes (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.
11. Enter no (no is the default) to disable the Telnet service.
12. Enter yes (yes is the default) to enable the SSH service.
13. Enter the SSH key type.
14. Enter the number of key bits within the specified range.
15. Enter no (no is the default) to configure the NTP server.
16. Enter shut (shut is the default) to configure the default switch port interface to the shut (disabled) state.
17. Enter auto (off is the default) to configure the switch port trunk mode.
18. Enter yes (yes is the default) to configure the switchport mode F.
19. Enter off (off is the default) to configure the PortChannel auto-create state.
20. Enter deny (deny is the default) to deny a default zone policy configuration.
21. Enter no (no is the default) to disable a full zone set distribution.
22. Enter enhanced (basic is the default) to configure default-zone mode as enhanced.
23. Enter no (no is the default) if you are satisfied with the configuration.
24. Enter yes (yes is default) to use and save this configuration.

DETAILED STEPS

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Step 2 Enter the new password for the administrator.

Enter the password for admin: **2004asdf*1kjh18**

Tip If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password as shown in the sample configuration. Passwords are case-sensitive.

Step 3 Enter yes to enter the setup mode.

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 yes (yes is the default) to enable secure password standard

Do you want to enforce secure password standard (yes/no): **yes**

Note You can also enable secure password standard using the **password strength-check** command. A secure password should contain characters from at least three of the classes: lower case letters, upper case letters, digits, and special characters.

Step 5 Enter no (no is the default) if you do not wish to create additional accounts.

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

Step 6 Configure the read-only or read-write SNMP community string.

a) Enter no (no is the default) to avoid configuring the read-only SNMP community string.

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

b) Enter yes (no is the default) to avoid configuring the read-write SNMP community string.

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

c) Enter the SNMP community string.

SNMP community string: *snmp_community*

Step 7 Enter a name for the switch.

Note The switch name is limited to 32 alphanumeric characters. The default is switch.

Enter the switch name: *switch_name*

Step 8 Enter no (yes is the default) at the configuration prompt to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **no**

Step 9 Enter yes (yes is the default) to configure the default gateway.

Configure the default-gateway: (yes/no) [y]: **yes**

- a) Enter the default gateway IP address.

IP address of the default gateway: *default_gateway*

- Step 10** Enter yes (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

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

- a) Enter yes (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **yes**

Enter the VSAN 1 IPv4 address.

VSAN1 IPv4 address: *ip_address*

Enter the IPv4 subnet mask.

VSAN1 IPv4 net mask: **subnet_mask**

- b) Enter no (yes is the default) to enable IPv4 routing capabilities.

Enable ip routing capabilities? (yes/no) [y]: **no**

- c) Enter no (yes is the default) to configure a static route.

Configure static route: (yes/no) [y]: **no**

- d) Enter no (yes is the default) to configure the default network

Configure the default-network: (yes/no) [y]: **no**

- e) Enter no (yes is the default) to configure the DNS IPv4 address.

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

- f) Enter no (no is the default) to skip the default domain name configuration.

Configure the default domain name? (yes/no) [n]: **no**

- Step 11** Enter no (no is the default) to disable the Telnet service.

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

- Step 12** Enter yes (yes is the default) to enable the SSH service.

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

Step 13 Enter the SSH key type.

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

Step 14 Enter the number of key bits within the specified range.

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

Step 15 Enter no (no is the default) to configure the NTP server.

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

Step 16 Enter shut (shut is the default) to configure the default switch port interface to the shut (disabled) state.

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

Note The management Ethernet interface is not shut down at this point. Only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

Step 17 Enter auto (off is the default) to configure the switch port trunk mode.

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

Step 18 Enter yes (yes is the default) to configure the switchport mode F.

```
Configure default switchport mode F (yes/no) [n]: y
```

Step 19 Enter off (off is the default) to configure the PortChannel auto-create state.

```
Configure default port-channel auto-create state (on/off) [off]: off
```

Step 20 Enter deny (deny is the default) to deny a default zone policy configuration.

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

Denies traffic flow to all members of the default zone.

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

```
switch# configure terminal  
switch(config)# zone default-zone permit vsan 1
```

Step 21 Enter no (no is the default) to disable a full zone set distribution.

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

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

You see the new configuration. Review and edit the configuration that you have just entered.

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

```
switch# configure terminal
switch(config)# zoneset distribute full vsan 1
```

Step 22 Enter enhanced (basic is the default) to configure default-zone mode as enhanced.

```
Configure default zone mode (basic/enhanced) [basic]: enhanced
```

Overrides the switch-wide default zone mode as enhanced.

Note If you are executing the setup script after issuing a **write erase** command, you must explicitly change the default zoning mode to enhanced for VSAN 1 after finishing the script using the following commands:

```
switch# configure terminal
switch(config)# zone mode enhanced vsan 1
```

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

```
switch# configure terminal
switch(config)# zoneset distribute full vsan 1
```

Step 23 Enter no (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

```
username admin password admin_pass role network-admin
snmp-server community snmp_community rw
switchname switch
interface vsan1
  ip address ip_address subnet_mask
  no shutdownip default-gateway default_gateway
no telnet server disable
ssh key rsa 2048 forcessh server enablesystem default switchport shutdown
system default switchport trunk mode
autosystem default switchport mode F
no zone default-zone permit vsan 1-4093
no zoneset distribute full vsan 1-4093
system default zone mode enhanced
```

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

Step 24 Enter yes (yes is default) to use and save this configuration.

```
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 ensures that the kickstart and system images are also automatically configured.

Where to Go Next

To become more familiar with the CLI, continue to .



Using PowerOn Auto Provisioning

This chapter describes how to deploy and use PowerOn Auto Provisioning (POAP) for the Cisco MDS 9148 and 9148S Multilayer Fabric Switch.

This chapter contains the following sections:

- [Network Requirements for POAP, page 23](#)
- [Guidelines and Limitations for POAP, page 29](#)
- [Setting Up the Network Environment to Use POAP, page 29](#)
- [Configuring a Switch Using POAP, page 30](#)
- [Verifying the Device Configuration, page 30](#)

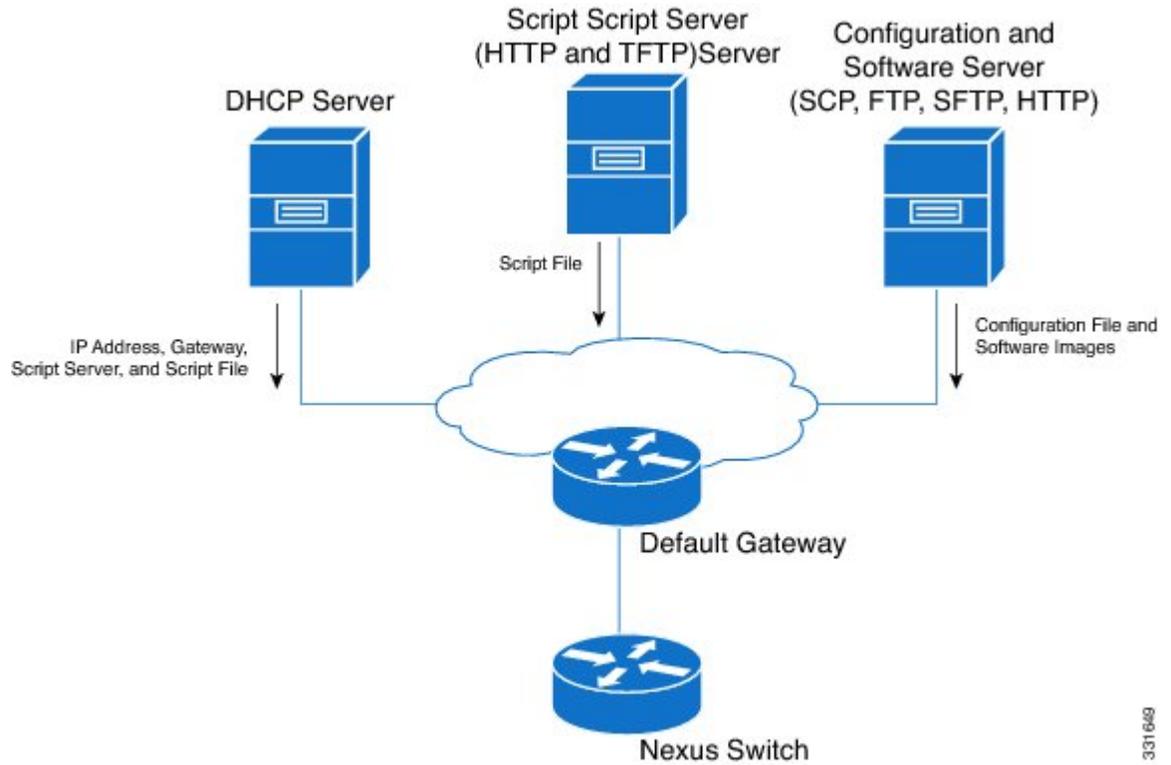
Network Requirements for POAP

If a USB (Universal Serial Device) device that contains the required installation files is not available, POAP requires the following network infrastructure:

- A DHCP server to bootstrap the interface IP address, gateway address, and DNS (Domain Name System) server.
- A TFTP server that contains the configuration script used to automate the software image installation and configuration process.

- One or more servers that contains the desired software images and configuration files.

Figure 4: POAP Network Infrastructure



331649

POAP Configuration Script

The reference script supplied by Cisco supports the following functionality:

- Retrieves the switch-specific identifier, for example, the serial number.
- Downloads the software image (system and kickstart images) if the files do not already exist on the switch. The software image is installed on the switch and is used at the next reboot.
- Schedules the downloaded configuration to be applied at the next switch reboot.
- Stores the configuration as the startup configuration.

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

API	Description
cli()	Returns the raw output of CLI commands, including the control/special characters.

API	Description
clid()	For CLI commands that support XML, this API puts the command output in a Python dictionary. This API can be useful to help search the output of show commands.

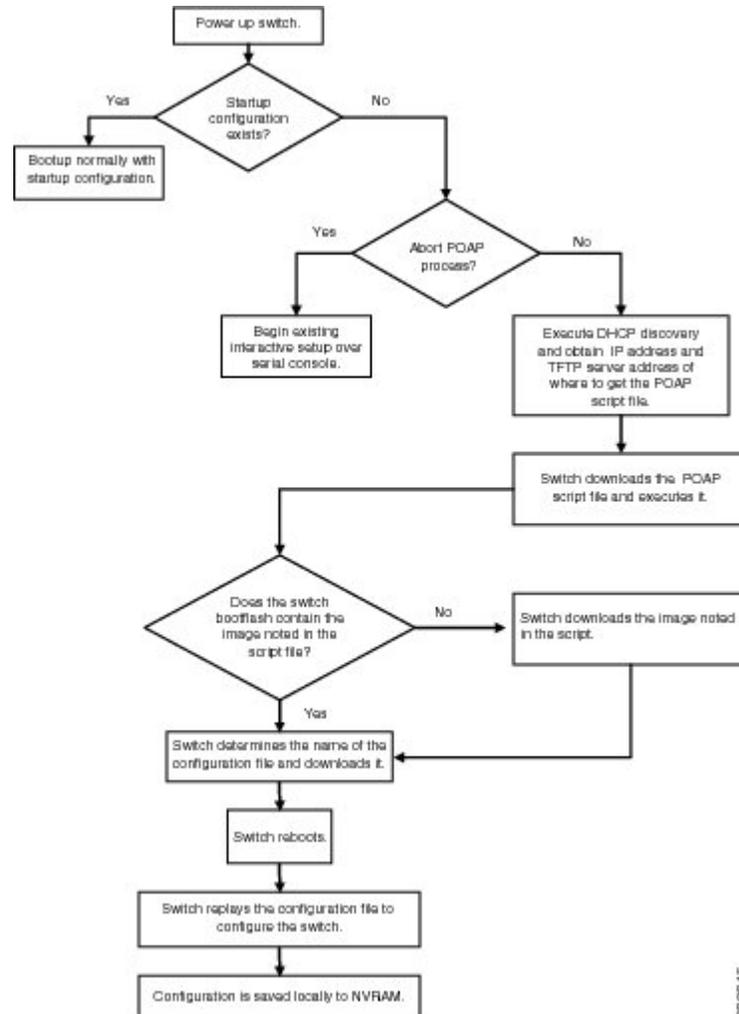
POAP Process

The POAP process has the following phases:

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

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

Figure 5: POAP Process



302215

Power-Up Phase

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

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



Note

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

If you exit POAP mode, you enter the normal interactive setup script. If you continue in POAP mode, all the front-panel interfaces are set up in the default configuration.

DHCP Discovery Phase

The switch sends out DHCP discover messages on the MGMT interface that solicits DHCP offers from the DHCP server or servers. (See the following figure.) The DHCP client on the Cisco MDS switch uses the switch serial number in the client-identifier option to identify itself to the DHCP server. The DHCP server can use this identifier to send information, such as the IP address and script filename, back to the DHCP client.

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

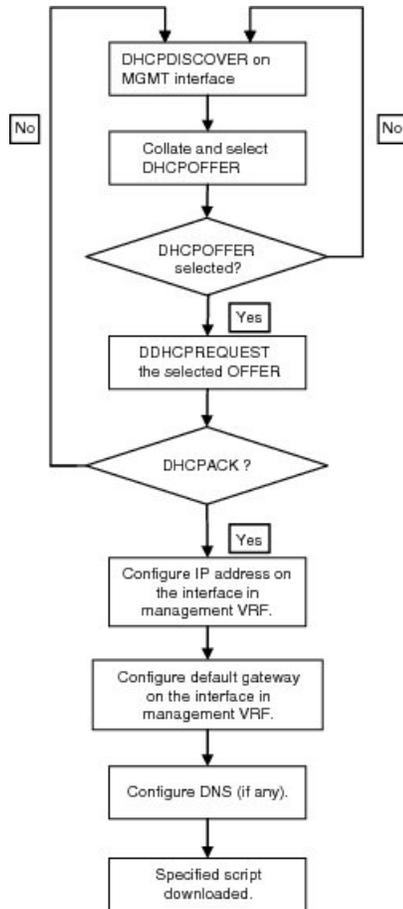
The DHCP discover message also solicits the following options from the DHCP server.

- TFTP server name or TFTP server address—The DHCP server relays the TFTP server name or TFTP server address to the DHCP client. The DHCP client uses this information to contact the TFTP server to obtain the script file.
- Bootfile name—The DHCP server relays the bootfile name to the DHCP client. The bootfile name includes the complete path to the bootfile on the TFTP server. The DHCP client uses this information to download the script file.

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

If no DHCP offers meet the requirements, the switch does not complete the DHCP negotiation (request and acknowledgment) and an IP address is not assigned.

Figure 6: DHCP Discovery Process



Script Execution Phase

After the device bootstraps itself using the information in the DHCP acknowledgment, the script file is downloaded from the TFTP server.

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

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



Note If the script execution fails, the DHCP discovery starts again.

Post-Installation Reload Phase

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

Guidelines and Limitations for POAP

POAP configuration guidelines and limitations are as follows:

- The Cisco MDS 9000 switch software image must support POAP for this feature to function.
- POAP does not support provisioning of the switch after it has been configured and is operational. Only auto-provisioning of a switch with no startup configuration is supported.
- 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.

You can configure the format of the script log file. Script file log formats are specified in the script. The template of the script log file has a default format; however, you can choose a different format for the script execution log file.

- The POAP feature does not require a license and is enabled by default. However for the POAP feature to function, appropriate licenses must be installed on the devices in the network before the deployment of the network.



Note To allow the POAP feature to function temporarily without the installation of the appropriate licenses, you can specify the **license grace-period** command in the configuration file.

This workaround allows you to install the appropriate licenses at a later time.

Setting Up the Network Environment to Use POAP

SUMMARY STEPS

1. (Optional) Put the POAP configuration script and any other desired software image and switch configuration files on a USB device that is accessible to the switch.
2. Deploy a DHCP server and configure it with the interface, gateway, and TFTP server IP addresses and a bootfile with the path and name of the configuration script file. This information is provided to the switch when it first boots.
3. Deploy a TFTP server to host the configuration script.
4. Deploy one or more servers to host the software images and configuration files.

DETAILED STEPS

-
- Step 1** (Optional) Put the POAP configuration script and any other desired software image and switch configuration files on a USB device that is accessible to the switch.
- Step 2** Deploy a DHCP server and configure it with the interface, gateway, and TFTP server IP addresses and a bootfile with the path and name of the configuration script file. This information is provided to the switch when it first boots. You do not need to deploy a DHCP server if all software image and switch configuration files are on the USB device.
- Step 3** Deploy a TFTP server to host the configuration script.
- Step 4** Deploy one or more servers to host the software images and configuration files.
-

Configuring a Switch Using POAP

Before You Begin

Make sure that the network environment is set up to use POAP. For more information, see 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
show running-config	Displays the running configuration.
show startup-config	Displays the startup configuration.

For detailed information about the fields in the output from these commands, see the Cisco MDS 9000 Family Command Reference.



Understanding the Command-Line Interface

This chapter contains the following sections:

- [Information About the CLI Prompt, page 34](#)
- [Command Modes, page 34](#)
- [Special Characters, page 37](#)
- [Keystroke Shortcuts, page 38](#)
- [Abbreviating Commands, page 40](#)
- [Completing a Partial Command Name, page 41](#)
- [Identifying Your Location in the Command Hierarchy, page 41](#)
- [Using the no Form of a Command , page 42](#)
- [Configuring CLI Variables, page 43](#)
- [Command Aliases, page 45](#)
- [Command Scripts, page 47](#)
- [Context-Sensitive Help , page 49](#)
- [Understanding Regular Expressions, page 51](#)
- [Searching and Filtering show Command Output, page 52](#)
- [Searching and Filtering from the --More-- Prompt, page 57](#)
- [Using the Command History, page 58](#)
- [Enabling or Disabling the CLI Confirmation Prompts, page 60](#)
- [Setting CLI Display Colors, page 61](#)
- [Sending Commands to Modules, page 61](#)
- [BIOS Loader Prompt, page 62](#)
- [Examples Using the CLI , page 63](#)

Information About the CLI Prompt

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

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

You can change the default device hostname.

From the CLI prompt, you can do the following:

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



Note

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

Command Modes

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

EXEC Command Mode

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

Global Configuration Command Mode

Global configuration mode provides access to the broadest range of commands. The term indicates characteristics or features that affect the device as a whole. You can enter commands in global configuration

mode to configure your device globally or to enter more specific configuration modes to configure specific elements such as interfaces or protocols.

SUMMARY STEPS

1. **configure terminal**

DETAILED STEPS

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

Interface Configuration Command Mode

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Subinterface Configuration Command Mode

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	interface <i>type number.subint</i> Example: switch(config)# interface ethernet 2/2.1 switch(config-subif)#	Specifies the VLAN interface to be configured. The CLI places you into a subinterface configuration mode for the specified VLAN interface. Note The CLI prompt changes to indicate that you are in global configuration mode.

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)#

```

Command Mode Summary

This table summarizes information about the main command modes.

Table 1: Command Mode Summary

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

Special Characters

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

Table 2: Special Characters

Character	Description
%	Percent

Character	Description
#	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 3: Keystroke Shortcuts

Keystokes	Description
Ctrl-A	Moves the cursor to the beginning of the line.
Ctrl-B	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.
Ctrl-C	Cancels the command and returns to the command prompt.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Moves the cursor to the end of the line.
Ctrl-F	Moves the cursor one character to the right.
Ctrl-G	Exits to the previous command mode without removing the command string.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-L	Redisplays the current command line.

Keystrokes	Description
Ctrl-N	Displays the next command in the command history.
Ctrl-O	Clears the terminal screen.
Ctrl-P	Displays the previous command in the command history.
Ctrl-R	Redisplays the current command line.
Ctrl-T	Transposes the character under the cursor with the character located to the right of the cursor. The cursor is then moved 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.
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.

Keystokes	Description
Tab	<p>Completes the word for you after you enter the first characters of the word and then press the Tab key. All options that match are presented.</p> <p>Use tabs to complete the following items:</p> <ul style="list-style-type: none"> • Command names • Scheme names in the file system • Server names in the file system • Filenames in the file system <p>Example:</p> <pre>switch(config)# xm<Tab> switch(config)# xml<Tab> switch(config)# xml server</pre> <p>Example:</p> <pre>switch(config)# c<Tab> callhome class-map clock cts cdp cli control-plane switch(config)# cl<Tab> class-map cli clock switch(config)# cla<Tab> switch(config)# class-map</pre> <p>Example:</p> <pre>switch# cd bootflash:<Tab> bootflash: bootflash://sup-1/ bootflash:/// bootflash://sup-2/ bootflash://module-5/ bootflash://sup-active/ bootflash://module-6/ bootflash://sup-local/</pre> <p>Example:</p> <pre>switch# cd bootflash://mo<Tab> 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 4: Examples of Command Abbreviations

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

Completing a Partial Command Name

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

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

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

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

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

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

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

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

Identifying Your Location in the Command Hierarchy

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

SUMMARY STEPS

1. where detail

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>where detail</p> <p>Example:</p> <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
Step 1	cli var name <i>variable-name variable-text</i> Example: switch# cli var name testinterface ethernet 2/1	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.
Step 2	show cli variables Example: switch# show cli variables	(Optional) Displays the CLI variable configuration.

Configuring Persistent CLI Variables

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	cli var name <i>variable-name variable-text</i> Example: switch(config)# cli var name testinterface ethernet 2/1	Configures the CLI persistent variable. The variable name is a case-sensitive, alphanumeric string and must begin with an alphabetic character. The maximum length is 31 characters.

	Command or Action	Purpose
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	show cli variables Example: switch# show cli variables	(Optional) Displays the CLI variable configuration.
Step 5	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Command Aliases

This section provides information about command aliases.

About Command Aliases

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

Command alias support has the following characteristics:

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

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

Defining Command Aliases

You can define command aliases for commonly used commands.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	cli alias name <i>alias-name alias-text</i> Example: switch(config)# cli alias name ethint interface ethernet	Configures the command alias. The alias name is an alphanumeric string that is not case sensitive and must begin with an alphabetic character. The maximum length is 30 characters.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	alias Example: switch# alias	(Optional) Displays the command alias configuration.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring Command Aliases for a User Session

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

SUMMARY STEPS

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

DETAILED STEPS

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

Command Scripts

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

Running a Command Script

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



Note

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

SUMMARY STEPS

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

DETAILED STEPS

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

Echoing Information to the Terminal

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

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

Table 5: Formatting Options for the echo Command

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	echo [backslash-interpret] [<i>text</i>] Example: <pre>switch# echo This is a test. This is a test.</pre>	The backslash-interpret keyword indicates that the text string contains formatting options. The <i>text</i> argument is alphanumeric, case sensitive, and can contain blanks. The maximum length is 200 characters. The default is a blank line.

Delaying Command Action

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

SUMMARY STEPS

1. `sleep seconds`

DETAILED STEPS

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

Context-Sensitive Help

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

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

This table shows example outputs of context sensitive help.

Table 6: Context-Sensitive Help Example

Example Outputs	Description
<pre>switch# clock ? set HH:MM:SS Current Time switch# clock</pre>	<p>Displays the command syntax for the clock command in EXEC mode.</p> <p>The switch output shows that the set keyword is required for using the clock command.</p>
<pre>switch# clock set ? WORD HH:MM:SS Current Time switch# clock set</pre>	<p>Displays the command syntax for setting the time.</p> <p>The help output shows that the current time is required for setting the clock and how to format the time.</p>
<pre>switch# clock set 13:32:00<CR> % Incomplete command switch#</pre>	<p>Adds the current time.</p> <p>The CLI indicates the command is incomplete.</p>
<pre>switch# <Ctrl-P> switch# clock set 13:32:00</pre>	<p>Displays the previous command that you entered.</p>
<pre>switch# clock set 13:32:00 ? <1-31> Day of the month switch# clock set 13:32:00</pre>	<p>Displays the additional arguments for the clock set command.</p>
<pre>switch# clock set 13:32:00 18 ? April Month of the year August Month of the year December Month of the year February Month of the year January Month of the year July Month of the year June Month of the year March Month of the year May Month of the year November Month of the year October Month of the year September Month of the year switch# clock set 13:32:00 18</pre>	<p>Displays the additional arguments for the clock set command.</p>
<pre>switch# clock set 13:32:00 18 April 08<CR> % Invalid input detected at '^' marker.</pre>	<p>Adds the date to the clock setting.</p> <p>The CLI indicates an error with the caret symbol (^) at 08.</p>
<pre>switch# clock set 13:32:00 18 April ? <2000-2030> Enter the year (no abbreviation) switch# clock set 13:32:00 18 April</pre>	<p>Displays the correct arguments for the year.</p>
<pre>switch# clock set 13:32:00 18 April 2008<CR> switch#</pre>	<p>Enters the correct syntax for the clock set command.</p>

Understanding Regular Expressions

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

Special Characters

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

This table lists the keyboard characters that have special meanings.

Table 7: Special Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
^	Matches the beginning of the string.
\$	Matches the end of the string.
_ (underscore)	Matches a comma (,), left brace ({}), right brace (}), left parenthesis ((), right parenthesis ()), the beginning of the string, the end of the string, or a space.

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 8: Special Characters Used for Anchoring

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

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



Note

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

Searching and Filtering show Command Output

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

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

```

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

```

Filtering and Searching Keywords

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

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

Table 9: Filtering and Searching Keywords

Keyword Syntax	Description
begin <i>string</i> Example: <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.
count Example: <code>show running-config count</code>	Displays the number of lines in the command output.
cut [-d <i>character</i>] {-b -c -f -s} Example: <code>show file testoutput cut -b 1-10</code>	Displays only part of the output lines. You can display a number of bytes (-b), characters (-vcut [-d <i>character</i>] {-b -c -f -s}), or fields (-f). You can also use the -d keyword to define a field delimiter other than the tag character default. The -s keyword suppresses the display of the lines that do not contain the delimiter.
end <i>string</i> Example: <code>show running-config end interface</code>	Displays all lines up to the last occurrence of the search string.
exclude <i>string</i> Example: <code>show interface brief exclude down</code>	Displays all lines that do not include the search string. The search string is case sensitive.
head [<i>lines lines</i>] Example: <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.

Keyword Syntax	Description
human Example: <code>show version human</code>	Displays the output in normal format if you have previously set the output format to XML using the terminal output xml command.
include <i>string</i> Example: <code>show interface brief include up</code>	Displays all lines that include the search string. The search string is case sensitive.
last [<i>lines</i>] Example: <code>show logging logfile last 50</code>	Displays the end of the output for the number of lines specified. The default number of lines is 10.
no-more Example: <code>show interface brief no-more</code>	Displays all the output without stopping at the end of the screen with the —More— prompt.
sscp <i>SSH-connection-name filename</i> Example: <code>show version sscp MyConnection</code> <code>show_version_output</code>	Redirects the output using streaming secure copy (sscp) to a named SSH connection. You can create the SSH named connection using the ssh name command.
wc [<i>bytes lines words</i>] Example: <code>show file testoutput wc bytes</code>	Displays counts of characters, lines, or words. The default is to display the number of lines, words, and characters.
xml Example: <code>show version xml</code>	Displays the output in XML format.

diff Utility

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

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

This table describes the keywords for the diff utility.

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

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

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

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

grep and egrep Utilities

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

The grep and egrep syntax is as follows:

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

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

Table 10: grep and egrep Parameters

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

less Utility

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

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 11: sort Utility Parameters

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

Parameter	Description
-t <i>delimiter</i>	Sorts using a specified delimiter. The default delimiter is the space character.
-u	Removes duplicate lines from the sort results. The sort output displays the duplicate lines.

Redirecting show Command Output Using sscp

You can use the Streamed Secure Copy Protocol (sscp) to redirect the **show** command output to a file on a remote server.

sscp *connection-name destination-file*



Note

You must create a named Secure Shell (SSH) connection before using sscp.

The following example shows how to copy **show** command output to a remote server using sscp:

```
switch# ssh name mybox testuser 172.23.152.34

                               WARNING!!!
                               READ THIS BEFORE ATTEMPTING TO LOGON

                               This System is for the use of authorized users only.  Individuals
                               using this computer without authority, or in excess of their
                               ...

testuser@172.23.152.34's password: Ctrl-C
switch# show running-config | sscp mybox /users/testuser/sscp_output
```

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 12: --More-- Prompt Commands

Commands	Description
[<i>lines</i>]<space>	Displays output lines for either the specified number of lines or the current screen size.
[<i>lines</i>]z	Displays output lines for either the specified number of lines or the current screen size. If you use the <i>lines</i> argument, that value becomes the new default screen size.

Commands	Description
[<i>lines</i>]<return>	Displays output lines for either the specified number of lines or the current default number of lines. The initial default is 1 line. If you use the optional <i>lines</i> argument, that value becomes the new default number of lines to display for this command.
[<i>lines</i>] d or [<i>lines</i>]Ctrl+shift+D	Scrolls through output lines for either the specified number of lines or the current default number of lines. The initial default is 11 lines. If you use the optional <i>lines</i> argument, that value becomes the new default number of lines to display for this command.
q or Q or Ctrl-C	Exits the <code>--More--</code> prompt.
[<i>lines</i>] s	Skips forward in the output for either the specified number of lines or the current default number of lines and displays a screen of lines. The default is 1 line.
[<i>lines</i>] f	Skips forward in the output for either the specified number of screens or the current default number of screens and displays a screen of lines. The default is 1 screen.
=	Displays the current line number.
[<i>count</i>]/ <i>expression</i>	Skips to the line that matches the regular expression and displays a screen of output lines. Use the optional <i>count</i> argument to search for lines with multiple occurrences of the expression. This command sets the current regular expression that you can use in other commands.
[<i>count</i>] n	Skips to the next line that matches the current regular expression and displays a screen of output lines. Use the optional <i>count</i> argument to skip past matches.
{! <i> </i> :! <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.

Configuring the CLI Edit Mode

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

SUMMARY STEPS

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

DETAILED STEPS

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

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. By default, the 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. Using the **terminal history no-exec-in-config** command, you can avoid recalling EXEC mode commands when you are in a configuration mode.

SUMMARY STEPS

1. [no] terminal history no-exec-in-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>[no] terminal history no-exec-in-config</p> <p>Example: switch# terminal history no-exec-in-config</p>	Configures the CLI history to remove the EXEC commands when you use the recall keystroke shortcuts in a configuration mode. The default recalls EXEC commands. You can revert to the default using the no form of the command.

Displaying the Command History

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

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

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

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 configuration commands in the command history:

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

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

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

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

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

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> Example: <code>switch# terminal dont-ask</code>	Disables the CLI confirmation prompt. The persist keyword makes the setting persistent across sessions for the current username. The default is enabled. Use the no form of the command to enable the CLI confirmation prompts.

Setting CLI Display Colors

You can change the CLI colors to display as follows:

- The prompt displays in green if the previous command succeeded.
- The prompt displays in red 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> Example: <code>switch# terminal color</code>	Sets the CLI display colors for the terminal session. The evening keyword is not supported. The persist keyword makes the setting persistent across sessions for the current username. The default setting is not persistent.

Sending Commands to Modules

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

The **slot** has the following syntax:

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

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

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

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

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

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

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

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

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

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

BIOS Loader Prompt

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

```
loader>
```

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

Examples Using the CLI

This section includes examples of using the CLI.

Defining Command Aliases

This example shows how to define command aliases:

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

This example shows how to use a command alias:

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

Using CLI Session Variables

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

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

```
switch# show interface $(testinterface)
Ethernet2/1 is down (Administratively down)
  Hardware is 10/100/1000 Ethernet, address is 0000.0000.0000 (bia 0019.076c.4dac)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
  Last clearing of "show interface" counters never
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun 0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
```

```
0 Rx pause 0 Tx pause 0 reset
```

Using the System-Defined Timestamp Variable

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

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

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

Running a Command Script

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

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

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

```
switch# run-script testfile
`configure terminal`
`interface ethernet 2/1`
`no shutdown`
`end`
`show interface ethernet 2/1 `
Ethernet2/1 is down (Link not connected)
Hardware is 10/100/1000 Ethernet, address is 0019.076c.4dac (bia 0019.076c.4dac)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is trunk
auto-duplex, auto-speed
Beacon is turned off
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
Switchport monitor is off
Last clearing of "show interface" counters 1d26.2uh
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
Rx
 0 input packets 0 unicast packets 0 multicast packets
 0 broadcast packets 0 jumbo packets 0 storm suppression packets
 0 bytes
Tx
 0 output packets 0 multicast packets
 0 broadcast packets 0 jumbo packets
 0 bytes
 0 input error 0 short frame 0 watchdog
 0 no buffer 0 runt 0 CRC 0 ecc
 0 overrun 0 underrun 0 ignored 0 bad etype drop
 0 bad proto drop 0 if down drop 0 input with dribble
 0 input discard
```

```
0 output error 0 collision 0 deferred
0 late collision 0 lost carrier 0 no carrier
0 babble
0 Rx pause 0 Tx pause 0 reset
```

Using the sscp Utility to Redirect show Command Output

This example shows how to redirect **show** command output using the sscp utility:

```
switch# ssh name MyConnection MyId 172.28.255.18
```

```
WARNING!!!
READ THIS BEFORE ATTEMPTING TO LOGON
```

```
This System is for the use of authorized users only. Individuals
using this computer without authority, or in excess of their
authority, are subject to having all of their activities on this
system monitored and recorded by system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored. Anyone using this system expressly
consents to such monitoring and is advised that if such
monitoring reveals possible criminal activity, system personnel
may provide the evidence of such monitoring to law enforcement
officials.
```

```
MyId@172.28.255.18's password:
```

```
switch# show version | sscp MyConnection show_version_output
switch#
```




CHAPTER 5

Configuring Terminal Settings and Sessions

This chapter contains the following sections:

- [Information About Terminal Settings and Sessions, page 67](#)
- [Configuring the Console Port, page 69](#)
- [Configuring the COM1 Port, page 71](#)
- [Configuring Virtual Terminals , page 73](#)
- [Configuring Modem Connections, page 75](#)
- [Clearing Terminal Sessions, page 80](#)
- [Displaying Terminal and Session Information, page 80](#)
- [Default Settings for Terminal Display and Session Parameters, page 81](#)

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 on the supervisor module. The following modems were tested on devices running the Cisco NX-OS software:

- MultiTech MT2834BA (http://www.multitech.com/en_us/support/families/multimodemii/)
- Hayes Accura V.92 (http://www.zoom.com/products/dial_up_external_serial.html#hayes)

**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
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	line console Example: <pre>switch# line console switch(config-console)#</pre>	Enters console configuration mode.
Step 3	databits <i>bits</i> Example: <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.
Step 4	exec-timeout <i>minutes</i> Example: <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.

	Command or Action	Purpose
Step 5	parity {even none odd} Example: switch(config-console)# parity even	Configures the parity. The default is none .
Step 6	speed {300 1200 2400 4800 9600 38400 57600 115200} Example: switch(config-console)# speed 115200	Configures the transmit and receive speed. The default is 115200 .
Step 7	stopbits {1 2} Example: switch(config-console)# stopbits 2	Configures the stop bits. The default is 1 .
Step 8	exit Example: switch(config-console)# exit switch(config)#	Exits console configuration mode.
Step 9	show line console Example: switch(config)# show line console	(Optional) Displays the console settings.
Step 10	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring the COM1 Port

You can set the following characteristics for the COM1 port:

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

Before You Begin

Log in to the console port or COM1 port.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	line com1 Example: switch# line com1 switch(config-com1)#	Enters COM1 configuration mode.
Step 3	databits <i>bits</i> Example: switch(config-com1)# databits 7	Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.
Step 4	flowcontrol hardware Example: switch(config-com1)# flowcontrol hardware	Enables flow control on the hardware. The default is enabled. Use the no flowcontrol hardware command to disable flow control on the hardware.
Step 5	parity {even none odd} Example: switch(config-com1)# parity even	Configures the parity. The default is none .
Step 6	speed {300 1200 2400 4800 9600 38400 57600 115200} Example: switch(config-com1)# speed 115200	Configures the transmit and receive speed. The default is 9600 .

	Command or Action	Purpose
Step 7	stopbits {1 2} Example: switch(config-com1)# stopbits 2	Configures the stop bits. The default is 1.
Step 8	exit Example: switch(config-com1)# exit switch(config)#	Exits COM1 configuration mode.
Step 9	show line com1 Example: switch(config)# show line com1	(Optional) Displays the COM1 port settings.
Step 10	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring Virtual Terminals

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

Configuring the Inactive Session Timeout

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	line vty Example: <pre>switch# line vty switch(config-line)#</pre>	Enters line configuration mode.
Step 3	exec-timeout <i>minutes</i> Example: <pre>switch(config-line)# exec-timeout 30</pre>	Configures the inactive session timeout. The range is from 0 to 525600 minutes (8760 hours). A value of 0 minutes disables the timeout. The default value is 30.
Step 4	exit Example: <pre>switch(config-line)# exit switch(config)#</pre>	Exits line configuration mode.
Step 5	show running-config all begin vty Example: <pre>switch(config)# show running-config all begin vty</pre>	(Optional) Displays the virtual terminal configuration.
Step 6	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Configuring the Session Limit

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	line vty Example: <pre>switch# line vty switch(config-line)#</pre>	Enters line configuration mode.
Step 3	session-limit <i>sessions</i> Example: <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.
Step 4	exit Example: <pre>switch(config-line)# exit switch(config)#</pre>	Exits line configuration mode.
Step 5	show running-config all begin vty Example: <pre>switch(config)# show running-config all begin vty</pre>	(Optional) Displays the virtual terminal configuration.
Step 6	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Configuring Modem Connections

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

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

Enabling a Modem Connection

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

Before You Begin

Log in to the console port.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose						
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.						
Step 2	Enter one of the following commands: <table border="1"> <thead> <tr> <th>Command</th> <th>Purpose</th> </tr> </thead> <tbody> <tr> <td>line com1</td> <td>Enters COM1 configuration mode.</td> </tr> <tr> <td>line console</td> <td>Enters console configuration mode.</td> </tr> </tbody> </table> Example: <pre>switch# line com1 switch(config-com1)#</pre>	Command	Purpose	line com1	Enters COM1 configuration mode.	line console	Enters console configuration mode.	Enters COM1 configuration mode or console configuration mode.
Command	Purpose							
line com1	Enters COM1 configuration mode.							
line console	Enters console configuration mode.							
Step 3	modem in Example: <pre>switch(config-com1)# modem in</pre>	Enables modem input on the COM1 or console port.						
Step 4	exit Example: <pre>switch(config-com1)# exit switch(config)#</pre>	Exits COM1 or console configuration mode.						
Step 5	show line Example: <pre>switch(config)# show line</pre>	(Optional) Displays the console and COM1 settings.						
Step 6	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.						

Downloading the Default Initialization String

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

Before You Begin

Log in to the console port.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose						
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.						
Step 2	Enter one of the following commands: <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>line com1</td> <td>Enters COM1 configuration mode.</td> </tr> <tr> <td>line console</td> <td>Enters console configuration mode.</td> </tr> </tbody> </table> Example: switch# line com1 switch(config-com1)#	Option	Description	line com1	Enters COM1 configuration mode.	line console	Enters console configuration mode.	
Option	Description							
line com1	Enters COM1 configuration mode.							
line console	Enters console configuration mode.							
Step 3	modem init-string default Example: switch(config-com1)# modem init-string default	Writes the default initialization string to the modem.						
Step 4	exit Example: switch(config-com1)# exit switch(config)#	Exits COM1 or console configuration mode.						

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

Configuring and Downloading a User-Specified Initialization String

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

Before You Begin

Log in to the console port.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose						
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.						
Step 2	Enter one of the following commands: <table border="1" data-bbox="261 1696 883 1866"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>line com1</td> <td>Enters COM1 configuration mode.</td> </tr> <tr> <td>line console</td> <td>Enters console configuration mode.</td> </tr> </tbody> </table>	Option	Description	line com1	Enters COM1 configuration mode.	line console	Enters console configuration mode.	
Option	Description							
line com1	Enters COM1 configuration mode.							
line console	Enters console configuration mode.							

	Command or Action	Purpose
	Example: <pre>switch# line com1 switch(config-com1)#</pre>	
Step 3	modem set-string user-input <i>string</i> Example: <pre>switch(config-com1)# modem set-string user-input ATE0Q1&D2&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. Note You must first set the user-input string before initializing the string.
Step 4	modem init-string user-input Example: <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	exit Example: <pre>switch(config-com1)# exit switch(config)#</pre>	Exits COM1 or console configuration mode.
Step 6	show line Example: <pre>switch(config)# show line</pre>	(Optional) Displays the COM1 and console settings.
Step 7	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

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

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

Before You Begin

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

Enable the modem connection on the port.

SUMMARY STEPS

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

DETAILED STEPS

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

Related Topics

[Enabling a Modem Connection, on page 75](#)

Clearing Terminal Sessions

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

SUMMARY STEPS

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

DETAILED STEPS

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

Displaying Terminal and Session Information

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

Command	Purpose
show terminal	Displays terminal settings.

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

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

Default Settings for Terminal Display and Session Parameters

This table lists the default settings for terminal displays and session parameters.

Table 13: Default Terminal Display and Session Parameter Settings

Parameters	Default
Terminal type	ansi
Terminal length	0 lines for console sessions 31 lines for virtual terminal sessions
Terminal width	80 columns
Terminal inactive session timeout	Disabled (0 minutes)
Console session data bits	8
Console inactive session timeout	Disabled (0 minutes)
Console session parity	none
Console session speed	11520 bps
Console session stop bits	1
COM1 session data bits	8
COM1 hardware flow control	Enabled
COM1 session parity	none
COM1 session speed	9600 bps

Parameters	Default
COM1 session stop bits	1
Virtual terminal inactive session timeout	Disabled (0 minutes)
Virtual terminal sessions limit	32
Modem default initialization string	ATE0Q1&D2&C1S0=1\015



CHAPTER 6

Basic Device Management

This chapter contains the following sections:

- [Information About Basic Device Management, page 83](#)
- [Changing the Device Hostname, page 85](#)
- [Configuring the Management Interface, page 86](#)
- [Configuring the Default Gateway, page 88](#)
- [Configuring the MOTD Banner, page 88](#)
- [Configuring the Time Zone, page 89](#)
- [Configuring Summer Time \(Daylight Saving Time\), page 90](#)
- [Manually Setting the Device Clock, page 92](#)
- [Managing Users, page 92](#)
- [Enabling or Disabling a Telnet Server Connection, page 93](#)
- [Verifying the Device Configuration, page 94](#)
- [Default Settings for Basic Device Parameters, page 95](#)

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.

Management Interface

The management interface allows multiple simultaneous Telnet or SNMP sessions. You can remotely configure the device 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. You can configure the mgmt 0 interface with either IPv4 address parameters or an IPv6 address.

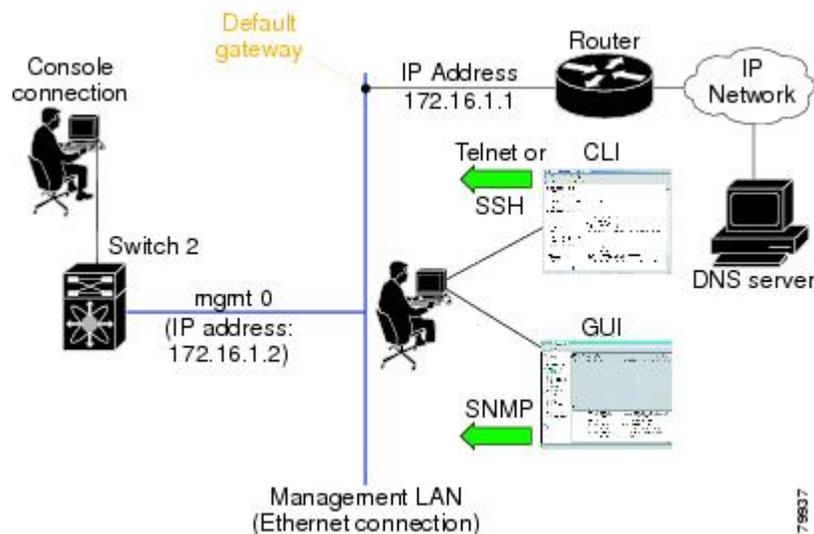
On devices with dual supervisor modules, a single IP address is used to manage the switch. The active supervisor module's mgmt0 interface uses this IP address. The mgmt0 interface on the standby supervisor module remains in an inactive state and cannot be accessed until a switchover happens. After a switchover, the mgmt0 interface on the standby supervisor module becomes active and assumes the same IP address as the previously active supervisor module.

The management port (mgmt0) is autosensing and operates in full duplex mode at a speed of 10/100/1000 Mbps (1000 Mbps is only available on the Supervisor-2 module). Autosensing supports both the speed and the duplex mode. On a Supervisor-1 module, the default speed is 100 Mbps and the default duplex mode is auto. On a Supervisor-2 module, the default speed is auto and the default duplex mode is auto.

Default Gateway

The supervisor module sends IP packets with unresolved destination IPv4 addresses to the default gateway.

Figure 7: Default Gateway



Message-of-the-Day Banner

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

Device Clock

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

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.

Telnet Server Connection

The Telnet server is disabled by default on all switches in the Cisco MDS 9000 Family. You can enable the Telnet server if you do not require a secure SSH connection. However, if you require a secure SSH connection, you need to disable the default Telnet connection and then enable the SSH connection.

**Note**

For information on connecting a terminal to the supervisor module console port, refer to the [Cisco MDS 9200 Series Hardware Installation Guide](#) or the [Cisco MDS 9500 Series Hardware Installation Guide](#).

**Note**

The Cisco NX-OS software allows a maximum of 16 sessions on any switch in the Cisco MDS 9500 Series or the Cisco MDS 9200 Series.

Changing the Device Hostname

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	{hostname switchname} name Example: Using the hostname command: <pre>switch(config)# hostname Engineering1 Engineering1(config)#</pre> Using the switchname command: <pre>Engineering1(config)# switchname Engineering2 Engineering2(config)#</pre>	Changes the device hostname. The <i>name</i> argument is alphanumeric, case sensitive, and has a maximum length of 32 characters. The default is switch. Note The switchname command performs the same function as the hostname command.
Step 3	exit Example: <pre>Engineering2(config)# exit Engineering2#</pre>	Exits global configuration mode.
Step 4	copy running-config startup-config Example: <pre>Engineering2# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Configuring the Management Interface

You can manually configure the management interface from the CLI. You can configure the mgmt 0 interface with either IPv4 address parameters or an IPv6 address.



Note You only need to configure the mgmt0 interface on the active supervisor module. When a supervisor module switchover occurs, the new active supervisor module uses the same configuration for the mgmt0 interface.

Before You Begin

Establish a connection on the console port.

SUMMARY STEPS

1. **configure terminal**
2. **interface mgmt 0**
3. **ip address** {*ipv4-address subnet-mask* | *ipv6-address*}
4. **exit**
5. (Optional) **show interface mgmt 0**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	interface mgmt 0 Example: <pre>switch(config)# interface mgmt 0 switch(config-if)#</pre>	Specifies the mgmt0 interface and enters the interface configuration mode.
Step 3	ip address { <i>ipv4-address subnet-mask</i> <i>ipv6-address</i> }	Configures the IPv4 or IPv6 address on the mgmt 0 interface.
	Example: <pre>switch(config-if)# ip address 1.1.1.0 255.255.255.0</pre>	
Step 4	exit Example: <pre>switch(config-if)# exit switch(config)#</pre>	Returns to global configuration mode.
Step 5	show interface mgmt 0 Example: <pre>switch(config)# show interface mgmt 0</pre>	(Optional) Displays the mgmt 0 interface information.
Step 6	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Configuring the Default Gateway

You can manually configure the management interface from the CLI. You can configure the mgmt 0 interface with either IPv4 address parameters or an IPv6 address.

Before You Begin

Establish a connection on the console port.

SUMMARY STEPS

1. **configure terminal**
2. **ip default gateway *ipv4-address***
3. (Optional) **show ip route**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	ip default gateway <i>ipv4-address</i> Example: switch(config)# ip default-gateway 172.16.1.1	Configures the IPv4 address for the default gateway.
Step 3	show ip route Example: switch(config)# show ip route	(Optional) Displays the default gateway configuration.
Step 4	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Configures the IPv4 or IPv6 address on the mgmt 0 interface.

Configuring the MOTD Banner

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

- Maximum of 80 characters per line

- Maximum of 40 lines

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring the Time Zone

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	clock timezone <i>zone-name</i> <i>offset-hours</i> <i>offset-minutes</i> Example: switch(config)# clock timezone EST -5 0	Configures the time zone. The <i>zone-name</i> argument is a 3-character string for the time zone acronym (for example, PST or EST). The <i>offset-hours</i> argument is the offset from the UTC and the range is from -23 to 23 hours. The range for the <i>offset-minutes</i> argument is from 0 to 59 minutes.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	show clock Example: switch# show clock	(Optional) Displays the time and time zone.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring Summer Time (Daylight Saving Time)

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	clock summer-time <i>zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes</i> Example: <pre>switch(config)# clock summer-time PDT 1 Sunday March 02:00 1 Sunday November 02:00 60</pre>	<p>Configures summer time or daylight saving time.</p> <p>The <i>zone-name</i> argument is a three character string for the time zone acronym (for example, PST and EST).</p> <p>The values for the <i>start-day</i> and <i>end-day</i> arguments are Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.</p> <p>The values for the <i>start-month</i> and <i>end-month</i> arguments are January, February, March, April, May, June, July, August, September, October, November, and December.</p> <p>The value for the <i>start-time</i> and <i>end-time</i> arguments are in the format <i>hh:mm</i>.</p> <p>The range for the <i>offset-minutes</i> argument is from 0 to 1440 minutes.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	show clock detail Example: <pre>switch(config)# show clock detail</pre>	(Optional) Displays the configured MOTD banner.
Step 5	copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Manually Setting the Device Clock

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

Before You Begin

Configure the time zone.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>clock set time day month year</code></p> <p>Example: <pre>switch# clock set 15:00:00 30 May 2008 Fri May 30 15:14:00 PDT 2008</pre></p>	<p>Configures the device clock.</p> <p>The format for the <i>time</i> argument is <i>hh:mm:ss</i>.</p> <p>The range for the <i>day</i> argument is from 1 to 31.</p> <p>The values for the <i>month</i> argument are January, February, March, April, May, June, July, August, September, October, November, and December.</p> <p>The range for the <i>year</i> argument is from 2000 to 2030.</p>
Step 2	<p><code>show clock</code></p> <p>Example: <pre>switch(config)# show clock</pre></p>	<p>(Optional)</p> <p>Displays the current clock value.</p>

Related Topics

[Configuring the Time Zone, on page 89](#)

Managing Users

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

Displaying Information about the User Sessions

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

SUMMARY STEPS

1. `show users`

DETAILED STEPS

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

Sending a Message to Users

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>show users</code> Example: <code>switch# show users</code>	(Optional) Displays the active user sessions.
Step 2	<code>send [session line] message-text</code> Example: <code>switch# send Reloading the device is 10 minutes!</code>	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.

Enabling or Disabling a Telnet Server Connection

You can enable or disable the Telnet server connection.

SUMMARY STEPS

1. **configure terminal**
2. **[no] feature telnet**
3. (Optional) **show telnet server**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] feature telnet Example: switch(config)# feature telnet	Enables the Telnet server connection. Use the no form of the command to disable the Telnet server connection. The default is disabled.
Step 3	show telnet server Example: switch(config)# show telnet server	(Optional) Displays the Telnet server configuration.
Step 4	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Verifying the Device Configuration

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

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

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

Default Settings for Basic Device Parameters

This table lists the default settings for basic device parameters.

Table 14: Default Basic Device Parameters

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



Using the Device File Systems, Directories, and Files

This chapter contains the following sections:

- [Information About the Device File Systems, Directories, and Files, page 97](#)
- [Formatting External Flash Devices, page 99](#)
- [Working with Directories, page 100](#)
- [Working with Files, page 103](#)
- [Working with Archive Files, page 109](#)
- [Examples of Using the File System, page 112](#)
- [Default Settings for File System Parameters, page 115](#)

Information About the Device File Systems, Directories, and Files

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

File Systems

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

Table 15: File System Syntax Components

File System Name	Module	Description
bootflash	sup-active sup-local	Internal CompactFlash memory located on the active supervisor module used for storing image files, configuration files, and other miscellaneous files. The initial default directory is bootflash.
	sup-standby sup-remote	Internal CompactFlash memory located on the standby supervisor module used for storing image files, configuration files, and other miscellaneous files.
slot0	—	External CompactFlash memory installed in a supervisor module used for storing system images, configuration files, and other miscellaneous files.
volatile	—	Volatile random-access memory (VRAM) located on a supervisor module used for temporary or pending changes.
nvrाम	—	Nonvolatile random-access memory (NVRAM) located on a supervisor module used for storing the startup-configuration file.
log	—	Memory on the active supervisor that stores logging file statistics.
system	—	Memory on a supervisor module used for storing the running-configuration file.
debug	—	Memory on a supervisor module used for debug logs.
usb1	—	External USB flash memory installed in a supervisor module used for storing image files, configuration files, and other miscellaneous files.

File System Name	Module	Description
usb2	—	External USB flash memory installed in a supervisor module used for storing image files, configuration files, and other miscellaneous files.

Directories

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

Files

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

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

Formatting External Flash Devices

You can format an external flash device to erase the contents and restore it to its factory-shipped state.



Note

For information on recovering corrupted bootflash using formatting, see the [Cisco MDS 9000 Family NX-OS Troubleshooting Guide](#).

Before You Begin

Insert the external flash device in the active supervisor module.

SUMMARY STEPS

1. (Optional) **dir** {slot0: | usb1: | usb2:}
2. **format** {slot0: | usb1: | usb2:}

DETAILED STEPS

	Command or Action	Purpose
Step 1	dir {slot0: usb1: usb2:} Example: switch# dir slot0:	(Optional) Displays the contents of an external flash device.
Step 2	format {slot0: usb1: usb2:} Example: switch# format slot0:	Formats an external flash device.

Working with Directories

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

Identifying the Current Directory

You can display the directory name of your current directory.

SUMMARY STEPS

1. pwd

DETAILED STEPS

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

Changing the Current Directory

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

SUMMARY STEPS

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

DETAILED STEPS

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

Creating a Directory

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

SUMMARY STEPS

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

DETAILED STEPS

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

Displaying Directory Contents

You can display the contents of a directory.

SUMMARY STEPS

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

DETAILED STEPS

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

Deleting a Directory

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Accessing Directories on the Standby Supervisor Module

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

Working with Files

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

Moving Files

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



Caution

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

Copying Files

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

**Note**

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	dir [<i>filesystem</i> : <i>//module</i>][<i>directory</i>] Example: switch# dir bootflash	(Optional) Displays the contents of the current directory. The file system and directory name are case sensitive.
Step 3	copy [<i>filesystem</i> : <i>//module</i>][<i>directory</i> /] <i>directory</i> /] <i>source-filename</i> { <i>filesystem</i> : <i>//module</i>][<i>directory</i> /]] <i>directory</i> /} <i>target-filename</i> Example: switch# move 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
Step 1	dir [<i>filesystem</i> : <i>//module</i>][<i>directory</i>] Example: switch# dir bootflash	(Optional) Displays the contents of the current directory. The file system and directory name are case sensitive.
Step 2	delete { <i>filesystem</i> : <i>//module</i>][<i>directory</i> /] <i>directory</i> /} <i>filename</i> Example: switch# move 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. Caution If you specify a directory, the delete command deletes the entire directory and all its contents.

Displaying File Contents

You can display the contents of a file.

SUMMARY STEPS

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

DETAILED STEPS

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

Displaying File Checksums

You can display checksums to check the file integrity.

SUMMARY STEPS

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

DETAILED STEPS

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

Compressing and Uncompressing Files

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

SUMMARY STEPS

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

DETAILED STEPS

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

Displaying the Last Lines in a File

You can display the last lines of a file.

SUMMARY STEPS

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

DETAILED STEPS

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

Redirecting show Command Output to a File

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

SUMMARY STEPS

1. (Optional) **terminal redirection-mode** {ascii | zipped}
2. *show-command* > [*filesystem:[//module/][directory]*] | [*directory /*][*filename*]

DETAILED STEPS

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

Finding Files

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	find <i>filename-prefix</i> Example: switch# find bgp_script	Finds all filenames in the default directory and in its subdirectories beginning with the filename prefix. The filename prefix is case sensitive.

Working with Archive Files

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

Creating an Archive Files

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

- bzip2
- gzip
- Uncompressed

The default is gzip.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	tar create { bootflash: volatile: } <i>archive-filename</i> [absolute] [bz2-compress] [gz-compress] [remove] [uncompressed] [verbose] <i>filename-list</i>	<p>Creates an archive file and adds files to it. The filename is alphanumeric, not case sensitive, and has a maximum length of 240 characters.</p> <p>The absolute keyword specifies that the leading backslash characters (\) should not be removed from the names of the files added to the archive file. By default, the leading backslash characters are removed.</p> <p>The bz2-compress, gz-compress, and uncompressed keywords determine the compression utility used when files are added, or later appended, to the archive and the decompression utility to use when extracting the files. If you do not specify an extension for the archive file, the defaults are as follows:</p> <ul style="list-style-type: none"> • For bz2-compress, the extension is .tar.bz2. • For gz-compress, the extension is .tar.gz.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • For uncompressed, the extension is .tar. <p>The remove keyword specifies that the Cisco NX-OS software should delete the files from the file system after adding them to the archive. By default, the files are not deleted.</p> <p>The verbose keyword specifies that the Cisco NX-OS software should list the files as they are added to the archive. By default, the files are listed as they are added.</p>

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

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

Appending Files to an Archive File

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Extracting Files from an Archive File

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Displaying the Filenames in an Archive File

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

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

The archive filename is not case sensitive.

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

Examples of Using the File System

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

Accessing Directories on Standby Supervisor Modules

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

```
switch# dir bootflash://sup-remote
 12198912   Aug 27 16:29:18 2003  m9500-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 the standby supervisor module:

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

Moving Files

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

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

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

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

Copying Files

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

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

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

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

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

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

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

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

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

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

Deleting a Directory

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

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

Displaying File Contents

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

```
switch# show file 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 16: Default File System Settings

Parameters	Default
Default filesystem	bootflash:



Working with Configuration Files

This chapter contains the following sections:

- [Information About Configuration Files, page 117](#)
- [Managing Configuration Files, page 118](#)
- [Verifying the Device Configuration, page 128](#)
- [Examples of Working with Configuration Files, page 128](#)

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 118

[Downloading the Startup Configuration From a Remote Server](#), on page 120

Managing Configuration Files

This section describes how to manage configuration files.

Saving the Running Configuration to the Startup Configuration

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

SUMMARY STEPS

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

DETAILED STEPS

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

Copying a Configuration File to a Remote Server

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	copy running-config <i>scheme://server/[url]</i> <i>/[filename]</i> Example: <pre>switch# copy running-config tftp://10.10.1.1/sw1-run-config.bak</pre>	Copies the running-configuration file to a remote server. For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the address or name of the remote server, and the <i>url</i> argument is the path to the source file on the remote server. The <i>server</i> , <i>url</i> , and <i>filename</i> arguments are case sensitive.
Step 2	copy startup-config <i>scheme://server/[url]</i> <i>/[filename]</i> Example: <pre>switch# copy startup-config tftp://10.10.1.1/sw1-start-config.bak</pre>	Copies the startup-configuration file to a remote server. For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the 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.

Downloading the Running Configuration From a Remote Server

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

Before You Begin

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Related Topics

[Copying Files, on page 112](#)

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 subnet if you do not have a router or a default gateway to route traffic between subnets.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	write erase Example: switch# write erase	Erases the startup configuration file.
Step 2	reload Example: switch# reload This command will reboot the system. (y/n)? [n] y ... Enter the password for "admin": <password> Confirm the password for "admin": <password> ... Would you like to enter the basic configuration dialog (yes/no): n switch#	Reloads the Cisco NX-OS device. Note Do not use the setup utility to configure the device.
Step 3	copy <i>scheme://server[/url /]filename</i> running-config Example: switch# copy tftp://10.10.1.1/my-config running-config	Downloads the running configuration file from a remote server. For the <i>scheme</i> argument, you can enter tftp: , ftp: , scp: , or sftp: . The <i>server</i> argument is the address or name of the remote server, and the <i>url</i> argument is the path to the source file on the remote server. The <i>server</i> , <i>url</i> , and <i>filename</i> arguments are case sensitive.
Step 4	copy running-config startup-config Example: switch# copy running-config startup-config	Saves the running configuration file to the startup configuration file.
Step 5	show startup-config Example: switch# show startup-config	(Optional) Displays the running configuration.

Related Topics[Copying Files, on page 112](#)

Copying Configuration Files to an External Flash Memory Device

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>dir {slot0: usb1: usb2:}[directory/]</code> Example: switch# dir slot0:	(Optional) Displays the files on the external flash memory device.
Step 2	<code>copy running-config {slot0: usb1: usb2:}[directory/]filename</code> Example: 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.
Step 3	<code>copy startup-config {slot0: usb1: usb2:}[directory/]filename</code> Example: 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.

Related Topics[Copying Files, on page 112](#)

Copying the Running Configuration from an External Flash Memory Device

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	dir {slot0: usb1: usb2:}[directory/] Example: switch# dir slot0:	(Optional) Displays the files on the external flash memory device.
Step 2	copy {slot0: usb1: usb2:}[directory/]filename running-config Example: switch# copy slot0:dsn-config.cfg running-config	Copies the running configuration from an external flash memory device. The <i>filename</i> argument is case sensitive.
Step 3	show running-config Example: switch# show running-config	(Optional) Displays the running configuration.
Step 4	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.
Step 5	show startup-config Example: switch# show startup-config	(Optional) Displays the startup configuration.

Related Topics

[Copying Files, on page 112](#)

Copying the Startup Configuration from an External Flash Memory Device

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	dir {slot0: usb1: usb2:}[<i>directory</i>] Example: switch# dir slot0:	(Optional) Displays the files on the external flash memory device.
Step 2	copy {slot0: usb1: usb2:}[<i>directory</i> /] <i>filename</i> startup-config Example: 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.
Step 3	show startup-config Example: switch# show startup-config	(Optional) Displays the startup configuration.

Related Topics

[Copying Files, on page 112](#)

Copying Configuration Files to an Internal File System

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

SUMMARY STEPS

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

DETAILED STEPS

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

Related Topics

[Copying Files, on page 112](#)

Rolling Back to a Previous Configuration

Problems, such as memory corruption, can occur that make it necessary for you to recover your configuration from a backed up version.



Note

Each time that you enter a **copy running-config startup-config** command, a binary file is created and the ASCII file is updated. A valid binary configuration file reduces the overall boot time significantly. A binary file cannot be uploaded, but its contents can be used to overwrite the existing startup configuration. The **write erase** command clears the binary file.

SUMMARY STEPS

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

DETAILED STEPS

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

Erasing a Configuration

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

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

- Startup
- Boot
- Debug



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

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

To remove the boot variable definitions and the IPv4 configuration on the mgmt0 interface, use the **write erase boot** command.

SUMMARY STEPS

1. **write erase [boot | debug]**

DETAILED STEPS

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

Verifying the Device Configuration

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

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

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

Examples of Working with Configuration Files

This section includes examples of working with configuration files.

Copying Configuration Files

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

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

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

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

Backing Up Configuration Files

This example shows how to create a snapshot of the startup configuration in a predefined location on the device (binary file):

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

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

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

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

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

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

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

Rolling Back to a Previous Configuration

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

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

**Note**

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

Beginning with Cisco NX-OS 6.2(2), you can use the **reload ascii** command to copy an ASCII version of the configuration to the start up configuration when reloading the device.

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



Configuring CDP

This chapter describes how to configure the Cisco Discovery Protocol (CDP) on Cisco MDS 9000 Family switches.

- [Information About CDP, page 131](#)
- [Configuring CDP, page 132](#)
- [Verifying the CDP Configuration, page 134](#)
- [Clearing CDP Counters and Tables, page 135](#)
- [CDP Example Configuration, page 135](#)
- [Default Settings for CDP, page 135](#)

Information About CDP

This section includes information about CDP.

CDP Overview

The Cisco Discovery Protocol (CDP) is an advertisement protocol used by Cisco devices to advertise itself to other Cisco devices in the same network. CDP runs on the data link layer and is independent of Layer 3 protocols. Cisco devices that receive the CDP packets cache the information to make it accessible through the CLI and SNMP.

The Cisco NX-OS software supports CDP on the management Ethernet (mgmt0) interface on the supervisor module and the Gigabit Ethernet interfaces on the IP Storage Services (IPS) and 14/2-port Multiprotocol Services (MPS-14/2) modules. The CDP daemon is restartable and switchable. The running and startup configurations are available across restarts and switchovers.

CDP version 1 (v1) and version 2 (v2) are supported in Cisco MDS 9000 Family switches. CDP packets with any other version number are silently discarded when received.

When the interface link is established, CDP is enabled by default and three CDP packets are sent at 1-second intervals. Following this action, the CDP frames are sent at the globally configured refresh interval.

High Availability for CDP

The Cisco NX-OS software supports stateless restarts for CDP. After a reboot or a supervisor module switchover, the Cisco NX-OS software applies the running configuration. For more information on high availability, see the [Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide](#).

Configuring CDP

This section describes how to configure CDP.

Enabling or Disabling CDP Globally

CDP is enabled by default. You can disable CDP and then reenble it.

CDP must be enabled on the device before you enable CDP on any interfaces. If CDP is disabled globally and you enable CDP on specified interfaces, CDP will not be active on those interfaces. The system does not return an error message when this occurs.

SUMMARY STEPS

1. **configure terminal**
2. **cdp enable**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters configuration mode.
Step 2	cdp enable Example: <pre>switch(config)# cdp enable</pre>	Enables the CDP feature on the entire device. This is enabled by default .
Step 3	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Saves this configuration change.

Enabling or Disabling CDP on an Interface

CDP is enabled by default on an interface. You can disable CDP on an interface.

If CDP is disabled globally and you enable CDP on specified interfaces, CDP will not be active on those interfaces. The system does not return an error message when this occurs.

Before You Begin

Ensure that CDP is enabled on the device.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **cdp enable**
4. (Optional) **show cdp interface** *interface-type slot/port*
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: switch(config)# interface gigabitethernet 1/2 switch(config-if)#	Enters interface configuration mode.
Step 3	cdp enable Example: switch(config-if)# cdp enable	Enables CDP on this interface. This is enabled by default.
Step 4	show cdp interface <i>interface-type slot/port</i> Example: switch(config-if)# show cdp interface gigabitethernet 1/2	(Optional) Displays CDP information for an interface.
Step 5	copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	(Optional) Saves this configuration change.

Configuring Optional CDP Parameters

You can use the following optional commands in global configuration mode to modify CDP:

Command	Purpose
cdp advertise {v1 v2} Example: <pre>switch(config)# cdp advertise v1</pre>	Sets the CDP version supported by the device. The default is v2.
cdp format device-id {mac-address serial-number system-name} Example: <pre>switch(config)# cdp format device-id mac-address</pre>	Sets the CDP device ID. The options are as follows: <ul style="list-style-type: none"> • mac-address—MAC address of the chassis. • serial-number—Chassis serial number or Organizationally Unique Identifier (OUI). • system-name—System name or fully qualified domain name (FQDN). The default is system-name .
cdp holdtime seconds Example: <pre>switch(config)# cdp holdtime 150</pre>	Sets the time that CDP holds onto neighbor information before discarding it. The range is from 10 to 255 seconds. The default is 180 seconds.
cdp timer seconds Example: <pre>switch(config)# cdp timer 50</pre>	Sets the refresh time when CDP sends advertisements to neighbors. The range is from 5 to 254 seconds. The default is 60 seconds.

Verifying the CDP Configuration

Use the following commands to verify the CDP configuration:

Command	Purpose
show cdp all	Displays all interfaces that have CDP enabled.
show cdp entry {all name entry-name}	Displays the CDP database entries.
show cdp global	Displays the CDP global parameters.
show cdp interface interface-type slot/port	Displays the CDP interface status.
show cdp neighbors {device-id interface interface-type slot/port} [detail]	Displays the CDP neighbor status.
show cdp traffic interface interface-type slot/port	Displays the CDP traffic statistics on an interface.

Clearing CDP Counters and Tables

Use the **clear cdp counters** command to clear CDP traffic counters for all interfaces. You can issue this command for a specified interface or for all interfaces (management and Gigabit Ethernet interfaces).

```
switch# clear cdp counters
```

Use the **clear cdp table** command to clear neighboring CDP entries for all interfaces. You can issue this command for a specified interface or for all interfaces (management and Gigabit Ethernet interfaces).

```
switch# clear cdp table interface gigabitethernet 4/1
```

CDP Example Configuration

This example enables the CDP feature and configures the refresh and hold timers:

```
configure terminal
 cdp enable
 cdp timer 50
 cdp holdtime 100
```

Default Settings for CDP

This table lists the CDP default settings.

Table 17: CDP Default Settings

Parameters	Default
CDP	Enabled globally and on all interfaces
CDP version	Version 2
CDP device ID	Serial number
CDP timer	60 seconds
CDP hold timer	180 seconds



Configuring NTP

This chapter describes how to configure the Network Time Protocol (NTP) on Cisco MDS 9000 Family switches.

- [Information About NTP, page 137](#)
- [Prerequisites for NTP , page 139](#)
- [Guidelines and Limitations for NTP, page 139](#)
- [Configuring NTP, page 139](#)
- [Verifying NTP Configuration, page 145](#)
- [NTP Example Configuration , page 145](#)
- [Default Settings for NTP, page 146](#)

Information About NTP

This section describes information about NTP.

NTP

In a large enterprise network, having one time standard for all network devices is critical for management reporting and event logging functions when trying to correlate interacting events logged across multiple devices. Many enterprise customers with extremely mission-critical networks maintain their own stratum-1 NTP source.

Time synchronization occurs when several frames are exchanged between clients and servers. The switches in client mode know the address of one or more NTP servers. The servers act as the time source and receive client synchronization requests.

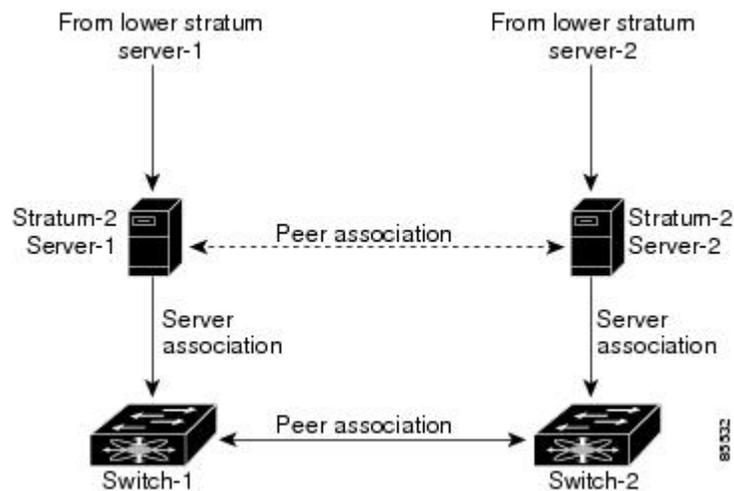
By configuring an IP address as a peer, the Cisco NX-OS device will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both of these instances point to different time servers, your NTP service is more reliable. Even if the active server link is lost, you can still maintain the correct time due to the presence of the peer.

If an active server fails, a configured peer helps in providing the NTP time. To ensure backup support if the active server fails, provide a direct NTP server association and configure a peer.

If you only configure a peer, the most accurate peer takes on the role of the NTP server and the other peer acts as a peer. Both devices end at the correct time if they have the correct time source or if they point to the correct NTP source.

Not even a server down time will affect well-configured switches in the network. This figure displays a network with two NTP stratum 2 servers and two switches.

Figure 8: NTP Peer and Server Association



In this configuration, the switches were configured as follows:

- Stratum-2 Server-1
 - IPv4 address-10.10.10.10
- Stratum-2 Server-2
 - IPv4 address-10.10.10.9
- Switch-1 IPv4 address-10.10.10.1
- Switch-1 NTP configuration
 - NTP server 10.10.10.10
 - NTP peer 10.10.10.2
- Switch-2 IPv4 address-10.10.10.2
- Switch-2 NTP configuration
 - NTP server 10.10.10.9
 - NTP peer 10.10.10.1

NTP Configuration Distribution Using CFS

You can enable NTP fabric distribution for all Cisco MDS switches in the fabric. When you perform NTP configurations, and distribution is enabled, the entire server and peer configuration is distributed to all the switches in the fabric.

You automatically acquire a fabric-wide lock when you issue the first configuration command after you enabled distribution in a switch. The NTP application uses the effective and pending database model to store or commit the commands based on your configuration.

High Availability for NTP

The Cisco NX-OS software supports stateless restarts for NTP. After a reboot or a supervisor switchover, the running configuration is applied. For more information on high availability, see the [Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide](#).

**Note**

You can configure NTP peers to provide redundancy in case an NTP server fails.

Prerequisites for NTP

NTP has the following prerequisite:

- If you configure NTP, you must have connectivity to at least one server that is running NTP.

Guidelines and Limitations for NTP

NTP has the following configuration guidelines and limitations:

- You should have a peer association with another device only when you are sure that your clock is reliable (which means that you are a client of a reliable NTP server).
- A peer configured alone takes on the role of a server and should be used as a backup. If you have two servers, you can configure several devices to point to one server and the remaining devices to point to the other server. You can then configure a peer association between these two servers to create a more reliable NTP configuration.
- If you only have one server, you should configure all the devices as clients to that server.
- You can configure up to 64 NTP entities (servers and peers).

Configuring NTP

This section describes how to configure NTP.

Enabling or Disabling the NTP Protocol

NTP is enabled on the device by default. You can disable NTP on the device and then reenabling it.

SUMMARY STEPS

1. **configure terminal**
2. **ntp enable**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	ntp enable Example: switch(config)# ntp enable	Enables or disables the NTP protocol on the entire device. The default state is enabled.
Step 3	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Saves this configuration change.

Configuring an NTP Server and Peer

You can configure NTP using IPv4 addresses, IPv6 addresses, or domain name server (DNS) names.

SUMMARY STEPS

1. **configure terminal**
2. **ntp server** *{ip-address | ipv6-address | dns-name}*
3. **ntp peer** *{ip-address | ipv6-address | dns-name}*
4. (Optional) **show ntp peers**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	ntp server {ip-address ipv6-address dns-name} Example: switch(config)# ntp server 192.0.2.10	Forms an association with a server.
Step 3	ntp peer {ip-address ipv6-address dns-name} Example: switch(config)# ntp peer 2001:0db8::4101	Forms an association with a peer. You can specify multiple peer associations.
Step 4	show ntp peers Example: switch(config)# show ntp peers	(Optional) Displays the configured server and peers. Note A domain name is resolved only when you have a DNS server configured.
Step 5	copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	(Optional) Saves this configuration change.

Displaying and Clearing NTP Statistics

NTP generates statistics that you can display and clear as needed.

SUMMARY STEPS

1. **display ntp statistics** {peer | io | local | memory}
2. **clear ntp statistics** {peer | io | local | memory}

DETAILED STEPS

	Command or Action	Purpose
Step 1	display ntp statistics {peer io local memory} Example: switch# show ntp statistics peers	Displays the NTP statistics. You can display the following NTP statistics: <ul style="list-style-type: none"> • peer—NTP statistics for per peer. • io—NTP statistics for I/O devices.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • local—NTP statistics for local devices. • memory—NTP statistics for memory.
Step 2	clear ntp statistics {peer io local memory} Example: switch# clear ntp statistics peers	Clears the NTP statistics.

Distributing the NTP Configuration Using CFS

You can distribute the NTP configuration changes to the fabric using CFS.

Enabling NTP Configuration Distribution

You can enable NTP configuration distribution using CFS.

Before You Begin

Ensure that CFS is enabled.

Ensure that NTP is enabled.

SUMMARY STEPS

1. **configure terminal**
2. **ntp distribute**
3. (Optional) **show ntp status**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	ntp distribute Example: switch(config)# ntp distribute	Enables NTP configuration distribution to all switches in the fabric. Acquires a fabric lock and stores all future configuration changes in the pending database. Use the no form of the command to disable NTP configuration distribution. The default is disabled.

	Command or Action	Purpose
Step 3	show ntp status Example: swtich(config)# show ntp status	(Optional) Displays the NTP configuration distribution status.
Step 4	copy running-config startup-config Example: swtich(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Committing NTP Configuration Changes

When you commit the NTP configuration changes, the Cisco NX-OS software applies the pending changes to the running configuration on the local Cisco MDS switch and to all the Cisco MDS switches in the fabric that can receive NTP configuration distributions. When you commit the NTP configuration changes without implementing the CFS session feature, the NTP configurations are distributed to all the switches in the fabric that have NTP distribution enabled.

Before You Begin

Enable NTP configuration distribution on other Cisco MDS switches in the fabric.

SUMMARY STEPS

1. **configure terminal**
2. **ntp commit**
3. (Optional) **show ntp session status**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	ntp commit Example: swtich(config)# ntp commit	Distributes the pending NTP configuration changes to running configuration files on the local Cisco MDS switch and to all Cisco MDS switches in the fabric that can receive NTP configuration distribution and releases the lock on the NTP configuration.

	Command or Action	Purpose
Step 3	show ntp session status Example: swtich(config)# show ntp session status	(Optional) Displays the NTP configuration distribution session status information.
Step 4	copy running-config startup-config Example: swtich(config)# copy running-config startup-config fabric	(Optional) Copies the running configuration to the startup configuration on the local switch and on all CFS-enabled switches in the fabric.

Discarding NTP Configuration Changes

After making the configuration changes, you can choose to discard the changes. This action releases the lock on the NTP configuration in the fabric.

SUMMARY STEPS

1. **configure terminal**
2. **ntp abort**
3. (Optional) **show ntp session status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	ntp abort Example: swtich(config)# ntp abort	Discards the NTP configuration changes in the pending database and releases the fabric lock.
Step 3	show ntp session status Example: swtich(config)# show ntp session status	(Optional) Displays the NTP configuration distribution session status information.

Releasing Fabric Session Lock on the NTP Configuration

If you have performed an NTP fabric task and have forgotten to release the lock by either committing or discarding the changes, an administrator can release the lock from any switch in the fabric. If the administrator performs this task, your changes to the pending database are discarded and the fabric lock is released.



Tip

The changes are only available in the volatile directory and are subject to being discarded if the switch is restarted.

To use administrative privileges and release a locked NTP session, use the **clear ntp session** command.

```
switch# clear ntp session
```

Verifying NTP Configuration

Use the following commands to display the NTP configuration:

Command	Purpose
show ntp peer-status	Displays the status for all NTP servers and peers.
show ntp peers	Displays all the NTP peers.
show ntp pending peers	Displays the temporary CFS database for NTP.
show ntp pending-diff	Displays the difference between the pending CFS database and the current NTP configuration.
show ntp session status	Displays the NTP session information.
show ntp statistics { io local memory peer { ipv4-address ipv6-address dns-name }	Displays the NTP statistics.
show ntp status	Displays the NTP distribution status.
show ntp timestamp status	Displays if the timestamp check is enabled.

NTP Example Configuration

This example configures an NTP server:

```
configure terminal
ntp server 192.0.2.10
```

Default Settings for NTP

This table lists the default settings for NTP parameters.

Table 18: Default NTP Settings

NTP	Disabled
-----	----------



Managing System Hardware

This chapter provides details on how to manage system hardware other than services and switching modules and how to monitor the health of the switch.

- [Displaying Switch Hardware Inventory, page 147](#)
- [Running CompactFlash Tests, page 149](#)
- [Running the CompactFlash CRC Checksum Test On Demand, page 153](#)
- [Displaying CompactFlash CRC Test and Firmware Update Statistics, page 156](#)
- [Displaying the Switch Serial Number, page 157](#)
- [Displaying Power Usage Information, page 157](#)
- [Power Supply Modes, page 158](#)
- [About Crossbar Management, page 162](#)
- [About Module Temperature Monitoring, page 165](#)
- [About Fan Modules, page 166](#)
- [About Clock Modules, page 168](#)
- [Displaying Environment Information, page 169](#)
- [Default Settings, page 170](#)

Displaying Switch Hardware Inventory

Use the **show inventory** command to view information on the field replaceable units (FRUs) in the switch, including product IDs, serial numbers, and version IDs. The following example shows the **show inventory** command output:

```
switch# show inventory
NAME: "Chassis", DESCR: "MDS 9506 chassis"
PID: DS-C9506 , VID: 0.104, SN: FOX0712S00T

NAME: "Slot 3", DESCR: "2x1GE IPS, 14x1/2Gbps FC Module"
PID: DS-X9302-14K9 , VID: 0.201, SN: JAB081405AF
```

```

NAME: "Slot 4",  DESCR: "2x1GE IPS, 14x1/2Gbps FC Module"
PID: DS-X9302-14K9      ,  VID: 0.201,  SN: JAB081605A5

NAME: "Slot 5",  DESCR: "Supervisor/Fabric-1"
PID: DS-X9530-SF1-K9   ,  VID: 4.0,  SN: JAB0747080H

NAME: "Slot 6",  DESCR: "Supervisor/Fabric-1"
PID: DS-X9530-SF1-K9   ,  VID: 4.0,  SN: JAB0746090H

NAME: "Slot 17",  DESCR: "MDS 9506 Power Supply"
PID: DS-CAC-1900W      ,  VID: 1.0,  SN: DCA07216052

NAME: "Slot 19",  DESCR: "MDS 9506 Fan Module"
PID: DS-6SLOT-FAN      ,  VID: 0.0,  SN: FOX0638S150

```

Use the **show hardware** command to display switch hardware inventory details. The following example shows the **show hardware** command output:

```

switch# show hardware
Cisco Storage Area Networking Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2003-2004 by Cisco Systems, Inc. All rights reserved.
The copyright for certain works contained herein are owned by
Cisco Systems, Inc. and/or other third parties and are used and
distributed under license.

Software
  BIOS:      version 1.0.8
  loader:    version 1.1(0.114)
  kickstart: version 1.3(4a)
  system:    version 1.3(4a)

  BIOS compile time:      08/07/03
  kickstart image file is: bootflash:///boot-17r
  kickstart compile time: 10/25/2010 12:00:00
  system image file is:   bootflash:///isan-17r
  system compile time:    10/25/2020 12:00:00

Hardware
  RAM 1024592 kB

  bootflash: 1000944 blocks (block size 512b)
  slot0:      0 blocks (block size 512b)

  172.22.90.21 uptime is 7 days 4 hours 48 minute(s) 2 second(s)

  Last reset at 272247 usecs after Thu Sep 11 21:47:05 1980
  Reason: Reset Requested by CLI command reload
  System version: 1.3(4a)

  This supervisor carries Pentium processor with 1024592 kB of memory
  Intel(R) Pentium(R) III CPU at family with 512 KB L2 Cache
  Rev: Family 6, Model 11 stepping 1

  512K bytes of non-volatile memory.
  1000944 blocks of internal bootflash (block size 512b)

  -----
  Chassis has 9 slots for Modules
  -----

  Module in slot 1 is empty

  Module in slot 2 is empty

  Module in slot 3 is empty

  Module in slot 4 is empty

  Module in slot 5 is ok
  Module type is "Supervisor/Fabric-1"
  No submodules are present

```

```
Model number is DS-X9530-SF1-K9
H/W version is 1.0
Part Number is 73-7523-06
Part Revision is A0
Manufacture Date is Year 6 Week 47
Serial number is JAB064705E1
CLEI code is CNP6NT0AAA

Module in slot 6 is empty

Module in slot 7 is empty

Module in slot 8 is empty

Module in slot 9 is empty

-----
Chassis has 2 Slots for Power Supplies
-----

PS in slot A is ok
Power supply type is "1153.32W 110v AC"
Model number is WS-CAC-2500W
H/W version is 1.0
Part Number is 34-1535-01
Part Revision is A0
Manufacture Date is Year 6 Week 16
Serial number is ART061600US
CLEI code is

PS in slot B is ok
Power supply type is "1153.32W 110v AC"
Model number is WS-CAC-2500W
H/W version is 1.0
Part Number is 34-1535-01
Part Revision is A0
Manufacture Date is Year 5 Week 41
Serial number is ART0541003V
CLEI code is

-----
Chassis has one slot for Fan Module
-----

Fan module is ok
Model number is WS-9SLOT-FAN
H/W version is 0.0
Part Number is 800-22342-01
Part Revision is
Manufacture Date is Year 0 Week 0
Serial number is
CLEI code is
```

Running CompactFlash Tests

you can run the CompactFlash CRC checksum test to identify if the CompactFlash firmware is corrupted and needs to be updated. By default, the CompactFlash CRC checksum test is enabled to automatically run in the background every seven days (you can change the automatic test interval by using the **system health module cf-crc-check frequency** command in configuration mode). You can run the test on demand by using the **system health cf-crc-check module** CLI command in EXEC mode. To turn the automatic testing off, use the **no system health module cf-crc-check** command in configuration mode.

The CompactFlash CRC checksum test can check if CompactFlash is corrupted on the following modules:

- DS-X9016

- DS-X9032
- DS-X9302-14K9
- DS-X9308-SMIP
- DS-X9304-SMIP
- DS-X9530-SF1-K9

Running the CompactFlash CRC Checksum Test On Demand

To run the CompactFlash CRC checksum test, use the **system health cf-crc-check module** command:
system health cf-crc-check module *number*
number indicates the slot in which the identified module resides.

```
switch# system health cf-crc-check module 4
```

Enabling and Disabling Automatic CompactFlash Firmware Update

By default, the Cisco NX-OS software update the CompactFlash firmware automatically every 30 days. You can disable the automatic update and then reenables the automatic update at a later time.

SUMMARY STEPS

1. **configure terminal**
2. **[no]system health module *slot-number* cf-re-flash**
3. (Optional) **show system health module *slot-number***
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no]system health module <i>slot-number</i> cf-re-flash Example: switch(config)# system health module 2 cf-re-flash	Enables the automatic CompactFlash firmware update. Use the no form of the command to disable automatic firmware updates. The default is enabled.

	Command or Action	Purpose
Step 3	show system health module <i>slot-number</i> Example: switch(config)# show system health module 2	(Optional) Displays the automatic CompactFlash firmware update status for a module.
Step 4	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Setting the CompactFlash CRC Checksum Test Interval

You can set the automatic CRC checksum test interval.

SUMMARY STEPS

1. **configure terminal**
2. **system health module *slot-number* cf-crc-check frequency *seconds***
3. (Optional) **show system health module *slot-number***
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	system health module <i>slot-number</i> cf-crc-check frequency <i>seconds</i> Example: switch(config)# system health module 2 cf-crc-check frequency 15	Sets the automatic CompactFlash CRC checksum test interval in seconds. The range is from 15 to 255.
Step 3	show system health module <i>slot-number</i> Example: switch(config)# show system health module 2	(Optional) Displays the automatic CompactFlash CRC checksum testing status for a module.

	Command or Action	Purpose
Step 4	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Enabling and Disabling Failure Action for a CompactFlash Checksum Test

You can prevent the Cisco NX-OS software from taking any action if a CompactFlash failure is determined while running the CRC checksum test and the failed CompactFlash is isolated from further testing. By default, this feature is enabled. The failure action is controlled at the module level.

SUMMARY STEPS

1. **configure terminal**
2. **[no]system health module *slot-number* cf-crc-check failiure-action**
3. (Optional) **show system health module *slot-number***
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no]system health module <i>slot-number</i> cf-crc-check failiure-action Example: <pre>switch(config)# system health module 2 cf-crc-check</pre>	Enables the automatic CompactFlash CRC checksum testing. Use the no form of the command to disable the failure action. The default is enabled.
Step 3	show system health module <i>slot-number</i> Example: <pre>switch(config)# show system health module 2</pre>	(Optional) Displays the automatic CompactFlash CRC checksum testing status for a module.
Step 4	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Running the CompactFlash CRC Checksum Test On Demand

To run the CompactFlash CRC checksum test, use the **system health cf-crc-check module** command:

```
system health cf-crc-check module number
```

number indicates the slot in which the identified module resides.

```
switch# system health cf-crc-check module 4
```

Updating the CompactFlash Firmware On Demand

You can update the CompactFlash firmware on demand using the following command:

```
system health cf-re-flash module slot-number
```

slot-number indicates the slot in which the identified module resides.

```
switch# system health cf-re-flash module 2
```

Enabling and Disabling the Automatic CompactFlash CRC Checksum Test

By default, the CompactFlash CRC checksum test is enabled to automatically run in the background. You can disable the automatic testing and then enable the testing at a later time.

SUMMARY STEPS

1. **configure terminal**
2. **system health module** *slot-number* **cf-crc-check**
3. (Optional) **show system health module** *slot-number*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	system health module <i>slot-number</i> cf-crc-check Example: switch(config)# system health module 2 cf-crc-check	Enables the automatic CompactFlash CRC checksum testing. Use the no form of the command to disable CompactFlash CRC checksum testing. The default is enabled.

	Command or Action	Purpose
Step 3	show system health module <i>slot-number</i> Example: switch(config)# show system health module 2	(Optional) Displays the automatic CompactFlash CRC checksum testing status for a module.
Step 4	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Setting the CompactFlash Firmware Update Interval

You can set the firmware update interval. The default interval is every 30 days.

SUMMARY STEPS

1. **configure terminal**
2. **system health module *slot-number* cf-re-flash frequency *days***
3. (Optional) **show system health module *slot-number***
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	system health module <i>slot-number</i> cf-re-flash frequency <i>days</i> Example: switch(config)# system health module 2 cf-re-flash frequency 45	Sets the automatic CompactFlash firmware update interval. The range is from 30 to 255. The default is every 30 days.
Step 3	show system health module <i>slot-number</i> Example: switch(config)# show system health module 2	(Optional) Displays the automatic CompactFlash firmware update interface configuration for a module.

	Command or Action	Purpose
Step 4	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Enabling and Disabling Failure Action for CompactFlash Firmware Updates

You can prevent the Cisco NX-OS software from taking any action if a CompactFlash failure occurs during the CompactFlash firmware update. By default, when a failure occurs, the Cisco NX-OS software isolates the failed CompactFlash from further testing. A failure action is controlled at the module level.

SUMMARY STEPS

1. **configure terminal**
2. **[no]system health module *slot-number* cf-re-flash failure-action**
3. (Optional) **show system health module *slot-number***
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no]system health module <i>slot-number</i> cf-re-flash failure-action Example: <pre>switch(config)# system health module 2 cf-re-flash</pre>	Enables the automatic CompactFlash firmware update failure action. Use the no form of the command to disable the failure action. The default is enabled.
Step 3	show system health module <i>slot-number</i> Example: <pre>switch(config)# show system health module 2</pre>	(Optional) Displays the automatic CompactFlash firmware update failure action status for a module.
Step 4	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Displaying CompactFlash Firmware Update Configuration

To display CompactFlash firmware update configuration for a specific module, use the following command:

```
show system health module slot-number
```

Displaying CompactFlash CRC Test and Firmware Update Statistics

To display the CompactFlash CRC checksum test and the flash update statistics, use the **show system health statistics** command.

```
switch# show system health statistics
```

```
Test statistics for module 2
```

Test Name	State	Frequency	Run	Pass	Fail	CFail	Errs
Bootflash	Running	10s	28316	28316	0	0	0
EOBC	Running	5s	56632	56632	0	0	0
Loopback	Running	5s	56618	56618	0	0	0
CF checksum	Running	2d	2	2	0	0	0
CF re-flash	Running	30d	1	1	0	0	0

```
Test statistics for module 5
```

Test Name	State	Frequency	Run	Pass	Fail	CFail	Errs
Bootflash	Running	10s	28314	28314	0	0	0
EOBC	Running	5s	56629	56629	0	0	0
Loopback	Running	5s	56614	56614	0	0	0
CF checksum	Running	1d	4	4	0	0	0
CF re-flash	Running	30d	1	1	0	0	0

```
Test statistics for module 7
```

Test Name	State	Frequency	Run	Pass	Fail	CFail	Errs
InBand	Running	5s	56643	56643	0	0	0
Bootflash	Running	10s	28323	28323	0	0	0
EOBC	Running	5s	56643	56643	0	0	0
Management Port	Running	5s	56643	56643	0	0	0

```
Test statistics for module 8
```

Test Name	State	Frequency	Run	Pass	Fail	CFail	Errs
InBand	Running	5s	56624	56624	0	0	0
Bootflash	Running	10s	28317	28317	0	0	0
EOBC	Running	5s	56624	56624	0	0	0

```
Test statistics for module 13
```

Test Name	State	Frequency	Run	Pass	Fail	CFail	Errs
Bootflash	Running	10s	28304	28304	0	0	0

```
EOBC          Running          5s    56608    56608        0        0        0
Loopback      Running          5s    56608    56608        0        0        0
-----
```

Displaying the Switch Serial Number

You can display the serial number of your Cisco MDS 9000 Family switch by looking at the serial number label on the back of the chassis (next to the power supply), or by using the **show sprom backplane 1** command.

```
switch# show sprom backplane 1
DISPLAY backplane sprom contents:
Common block:
  Block Signature : 0xabab
  Block Version  : 2
  Block Length   : 156
  Block Checksum : 0x106f
  EEPROM Size    : 512
  Block Count    : 3
  FRU Major Type : 0x6001
  FRU Minor Type : 0x0
  OEM String     : Cisco Systems, Inc.
  Product Number : DS-C9506
  Serial Number  : FOX0712S007
  Part Number    : 73-8697-01
  Part Revision  : 01
  Mfg Deviation  : 0
  H/W Version    : 0.1
  Mfg Bits       : 0
  Engineer Use   : 0
  snmpOID        : 9.12.3.1.4.26.0.0
  Power Consump  : 0
  RMA Code       : 0-0-0-0
Chassis specific block:
...
```



Note If you are installing a new license, use the **show license host-id** command to obtain the switch serial number. For more information, see the [Cisco MDS 9000 Family NX-OS Software Licensing Guide](#).

Displaying Power Usage Information

Use the **show environment power** command to display the actual power usage information for the entire switch. In response to this command, power supply capacity and consumption information is displayed for each module.



Note In a Cisco MDS 9500 Series switch, power usage is reserved for both supervisors regardless of whether one or both supervisor modules are present.

```
switch# show environment power
-----
PS  Model                Power      Power      Status
   (Watts)      (Amp @42V)
-----
1   DS-CAC-2500W         1153.32   27.46      ok
2   WS-CAC-2500W         1153.32   27.46      ok
```

Mod	Model	Power Requested (Watts)	Power Requested (Amp @42V)	Power Allocated (Watts)	Power Allocated (Amp @42V)	Status
1	DS-X9032	199.92	4.76	199.92	4.76	powered-up
4	DS-X9032	199.92	4.76	199.92	4.76	powered-up
5	DS-X9530-SF1-K9	126.00	3.00	126.00	3.00	powered-up
6	DS-X9530-SF1-K9	126.00	3.00	126.00	3.00	powered-up
9	DS-X9016	220.08	5.24	220.08	5.24	powered-up

Power Usage Summary:

```

-----
Power Supply redundancy mode:                redundant

Total Power Capacity                          1153.32 W

Power reserved for Supervisor(s) [-]         252.00 W
Power reserved for Fan Module(s) [-]         0.00 W
Power currently used by Modules[-]           619.92 W

-----
Total Power Available                          281.40 W
-----

```

Power Supply Modes

Switches in the MDS 9000 Family have two redundant power supply slots. The power supplies can be configured in either redundant or combined mode.

- Redundant mode—Uses the capacity of one power supply only. This is the default mode. In case of power supply failure, the entire switch has sufficient power available in the system.
- Combined mode—Uses the combined capacity of both power supplies. In case of power supply failure, the entire switch can be shut down (depends on the power used) causing traffic disruption. This mode is seldom used, except in cases where the switch has two low power supply capacities but a higher power usage.



Note

The chassis in the Cisco MDS 9000 Family uses 1200 W when powered at 110 V, and 2500 W when powered at 220 V.

Configuration Guidelines for Power Supplies

When configuring power supplies follow these guidelines:

- When power supplies with different capacities are installed in the switch, the total power available differs based on the configured mode, either redundant or combined:
 - Redundant mode—The total power is the lesser of the two power supply capacities. For example, suppose you have the following usage figures configured:

```

Power supply 1 = 2500 W
Additional power supply 2 = not used
Current usage = 2000 W

```

Current capacity = 2500 W

Then the following three scenarios will differ as specified:

Scenario 1: If 1800 W is added as power supply 2, then power supply 2 is shut down.

Reason: 1800 W is less than the usage of 2000 W.

Scenario 2: If 2200 W is added as power supply 2, then the current capacity decreases to 2200 W.

Reason: 2200 W is the lesser of the two power supplies.

Scenario 3: If 3000 W is added as power supply 2, then the current capacity value remains at 2500 W.

Reason: 2500 W is the lesser of the two power supplies.

This table describes the actions for the scenarios.

Table 19: Redundant Mode Power Supply Scenarios

Scenario	Power Supply 1 (Watts)	Current Usage (Watts)	Insertion of Power Supply 2 (Watts)	New Capacity (Watts)	Action Taken by Switch
1	2500	2000	1800	2500	Power supply 2 is shut down.
2	2500	2000	2200	2200	Capacity becomes 2200 W.
3	2500	2000	3300	2500	Capacity remains the same.

◦ Combined mode—The total power is twice the lesser of the two power supply capacities.

For example, suppose you have the following usage figures configured:

Power supply 1 = 2500 W
 Additional Power supply 2 = not used
 Current Usage = 2000 W
 Current capacity = 2500 W

Then the following three scenarios will differ as specified:

Scenario 1: If 1800 W is added as power supply 2, then the capacity increases to 3600 W.

Reason: 3600 W is twice the minimum (1800 W).

Scenario 2: If 2200 W is added as power supply 2, then the current capacity increases to 4400 W.

Reason: 4400 W is twice the minimum (2200 W).

Scenario 3: If 3000 W is added as power supply 2, then the current capacity increases to 5000 W.

Reason: 5000 W is twice the minimum (2500 W).

This table describes how these scenarios differ.

Table 20: Combined Mode Power Supply Scenarios

Scenario	Power Supply 1 (W)	Current Usage (W)	Insertion of Power Supply 2 (W)	New Capacity (W)	Action Taken by
1	2500	2000	1800	3600	Power is never shut down. The new capacity is changed.
2	2500	2000	2200	4400	
3	2500	2000	3300	5000	

- When you change the configuration from combined to redundant mode and the system detects a power supply that has a capacity lower than the current usage, the power supply is shut down. If both power supplies have a lower capacity than the current system usage, the configuration is not allowed.

Scenario 1: You have the following usage figures configured:

Power supply 1 = 2500 W
 Additional Power supply 2 = 1800 W
 Current Usage = 2000 W
 Current mode = combined mode (so current capacity is 3600 W)

You decide to change the switch to redundant mode. Then power supply 2 is shut down.

Reason: 1800 W is the lesser of the two power supplies and it is less than the system usage.

Scenario 2: You have the following usage figures configured:

Power supply 1 = 2500 W
 Additional Power supply 2 = 2200 W
 Current Usage = 2000 W
 Current mode = combined mode (so current capacity is 4400 W).

You decide to change the switch to redundant mode. Then the current capacity decreases to 2200 W.

Reason: 2200 W is the lesser of the two power supplies.

Scenario 3: You have the following usage figures configured:

Power supply 1 = 2500 W
 Additional Power supply 2 = 1800 W
 Current Usage = 3000 W
 Current mode = combined mode (so current capacity is 3600 W).

You decide to change the switch to redundant mode. Then the current capacity decreases to 2500 W and the configuration is rejected.

Reason: 2500 W is less than the system usage (3000 W).

This table describes these scenarios.

Table 21: Combined Mode Power Supply Scenarios

Scenario	Power Supply 1 (W)	Current Mode	Current Usage (W)	Power Supply 2 (W)	New Mode	New Capacity	Action Taken by Switch
1	2500	combined	2000	1800	N/A	3600	This is the existing configuration.
	2500	N/A	2000	1800	redundant	2500	Power supply 2 is shut down.
2	2500	combined	2000	2200	N/A	4400	This is the existing configuration.
	2500	N/A	2000	2200	redundant	2200	The new capacity is changed.
3	2500	combined	3000	1800	N/A	3600	This is the existing configuration.
	2500	N/A	3000	1800	redundant	N/A	Rejected, so the mode reverts to combined mode.

Configuring the Power Supply Mode

You can configure power supply modes.

SUMMARY STEPS

1. **configure terminal**
2. **power redundancy-mode {combined | insrc-redundant | ps-redundant | redundant}**
3. (Optional) **show environment power**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	power redundancy-mode {combined insrc-redundant ps-redundant redundant} Example: switch(config)# power redundancy-mode combined	Configures the power supply mode. The default is redundant .
Step 3	show environment power Example: switch(config)# show environment power	(Optional) Displays the power mode configuration.
Step 4	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

About Crossbar Management

Cisco MDS NX-OS software supports three types of hardware for the Cisco MDS 9500 Series Directors: Generation 1, Generation 2, and Generation 3.

Generation 3 includes the following:

- 48-port 8-Gbps Fibre Channel switching module
- 24-port 8-Gbps Fibre Channel switching module
- 4/44-port 8-Gbps Host-Optimized Fibre Channel module
- Cisco MDS 9513 Fabric-2 Crossbar Switching module


Note

The new software features in Cisco MDS NX-OS Release 4.1(1b) and later are not supported in the Generation 1 hardware.

**Note**

The Cisco MDS NX-OS software does not support the following hardware: Supervisor-1 module, the IPS-4 and IPS-8 storage modules, the Cisco MDS 9216 switch, the Cisco MDS 9216A switch, the Cisco MDS 9020 switch, the Cisco MDS 9120 switch, and the Cisco MDS 9140 switch.

Generation 2 hardware includes the following:

- Cisco MDS 9513 Director chassis
- Supervisor-2 module
- MSM-18/4 Multiservice Storage module
- Cisco MDS 9222i Module-1 module
- 48-port 4-Gbps Fibre Channel switching module
- 24-port 4-Gbps Fibre Channel switching module
- 12-port 4-Gbps Fibre Channel switching module
- 4-port 10-Gbps Fibre Channel switching module

The Cisco MDS NX-OS software on the Cisco MDS 9500 Series Directors supports the following types of crossbars:

- Integrated crossbar—Located on the Supervisor-1 and Supervisor-2 modules. The Cisco MDS 9506 and 9509 Directors only use integrated crossbars.
- External crossbar—Located on an external crossbar switching module. Cisco MDS 9513 Directors require external crossbar modules.

Generation 1 hardware includes the following:

- Cisco MDS 9506 and 9509 Director chassis
- Supervisor-1 module
- 32-port 2-Gbps Fibre Channel switching module
- 16-port 2-Gbps Fibre Channel switching module
- 8-port IP Storage Services (IPS-8) module
- 4-port IP Storage Services (IPS-4) module
- Storage Services Module (SSM)
- 14/2-port Multiprotocol Services (MPS-14/2) module

Operational Considerations when Removing Crossbars

You can mix and match Generation 1 and Generation 2 hardware on the Cisco MDS 9500 Series Directors running Cisco MDS NX-OS software without compromising the integrity and availability of your SANs based on Cisco MDS 9500 Series Directors.

To realize these benefits, you must gracefully shut down the crossbars and consider the backward compatibility of the Generation 1 modules.

Gracefully Shutting Down a Crossbar

You must perform a graceful shutdown of a crossbar (integrated or external) before removing it from the MDS 9500 Series Director.

- You must enter the EXEC mode **out-of-service xbar** command for a graceful shutdown of external crossbar modules in a Cisco MDS 9513 Director.

out-of-service xbar slot

slot indicates the external crossbar module slot number.



Note To reactivate the external crossbar module, you must remove and reinsert or replace the crossbar module.

- You must enter the EXEC mode **out-of-service module** command for a graceful shutdown of integrated crossbars on the supervisor module in a Cisco MDS 9506 or 9509 Director.

out-of-service module slot

slot indicates the chassis slot number on either the Supervisor-1 module or the Supervisor-2 module in which the integrated crossbar resides.



Note To reactivate the integrated crossbar, you must remove and reinsert or replace the Supervisor-1 module or Supervisor-2 module.



Caution Taking the crossbar out-of-service may cause a supervisor switchover.

Providing Backward Compatibility for Generation 1 Modules in Cisco MDS 9513 Directors

To provide backward compatibility for a Generation 1 module in a Cisco MDS 9513 chassis, the active and backup Supervisor-2 modules are associated to a specific crossbar module. The Supervisor-2 module in slot 7 is associated with crossbar module 1, and Supervisor-2 module in slot 8 is associated with crossbar module 2. You must plan for the following operational considerations before removing crossbar modules:

- Whenever a crossbar module associated with the active Supervisor-2 module goes offline or is brought online in a system that is already online, a stateful supervisor switchover occurs. This switchover does not disrupt traffic. Events that cause a crossbar module to go offline include the following:
 - Out-of-service requests
 - Physical removal
 - Errors
- Supervisor-2 module switchovers do not occur if the crossbar switching module associated with the backup Supervisor-2 module goes offline.

**Note**

Supervisor-2 module switchovers do not occur when removing crossbar switch modules on a Cisco MDS 9513 that has only Generation 2 modules installed.

About Module Temperature Monitoring

Built-in automatic sensors are provided in all switches in the Cisco MDS 9000 Family to monitor your switch at all times.

Each module (switching and supervisor) has four sensors: 1 (outlet sensor), 2 (intake sensor), 3 (onboard sensor), and 4 (onboard sensor). Each sensor has two thresholds (in degrees Celsius): minor and major.

**Note**

A threshold value of -127 indicates that no thresholds are configured or applicable.

- **Minor threshold**—When a minor threshold is exceeded, a minor alarm occurs and the following action is taken for all four sensors:
 - System messages are displayed.
 - Call Home alerts are sent (if configured).
 - SNMP notifications are sent (if configured).
- **Major threshold**—When a major threshold is exceeded, a major alarm occurs and the following action is taken:
 - For sensors 1, 3, and 4 (outlet and onboard sensors):

System messages are displayed.

Call Home alerts are sent (if configured).

SNMP notifications are sent (if configured).
 - For sensor 2 (intake sensor):

If the threshold is exceeded in a switching module, only that module is shut down.

If the threshold is exceeded in an active supervisor module with HA-standby or standby present, only that supervisor module is shut down and the standby supervisor module takes over.

If you do not have a standby supervisor module in your switch, you have an interval of 2 minutes to decrease the temperature. During this interval the software monitors the temperature every five (5) seconds and continuously sends system messages as configured.

**Tip**

To realize the benefits of these built-in automatic sensors on any switch in the Cisco MDS 9500 Series, we highly recommend that you install dual supervisor modules. If you are using a Cisco MDS 9000 Family switch without dual supervisor modules, we recommend that you immediately replace the fan module if even one fan is not working.

Displaying Module Temperatures

Use the **show environment temperature** command to display temperature sensors for each module.

This example shows the temperature information for Generation 1 hardware.

```
switch# show environment temperature
-----
Module   Sensor   MajorThresh  MinorThres  CurTemp  Status
         (Celsius) (Celsius)    (Celsius)
-----
2        Outlet   75           60          35       ok
2        Intake   65           50          33       ok

5        Outlet   75           60          44       ok
5        Intake   65           50          36       ok

6        Outlet   75           60          42       ok
6        Intake   65           50          35       ok

7        Outlet   75           60          33       ok
7        Intake   65           50          30       ok

9        Outlet   75           60          34       ok
9        Intake   65           50          39       ok
```

This example shows the temperature information for Generation 1 hardware.

```
switch# show environment temperature
-----
Module   Sensor   MajorThresh  MinorThres  CurTemp  Status
         (Celsius) (Celsius)    (Celsius)
-----
1        Outlet1  75           60          33       ok
1        Outlet2  65           50          30       ok
1        Intake1  65           50          30       ok
1        LcFwdUp  65           50          35       ok
1        LcFwdDn  65           50          39       ok
1        FC-MAC   65           50          34       ok

6        Outlet1  75           60          33       ok
6        Outlet2  65           50          30       ok
6        Intake1  65           50          30       ok
6        Crosbar  65           50          35       ok
6        Arbiter  65           50          39       ok
6        CPU     65           50          34       ok
```

About Fan Modules

Hot-swappable fan modules (fan trays) are provided in all switches in the Cisco MDS 9000 Family to manage airflow and cooling for the entire switch. Each fan module contains multiple fans to provide redundancy. The switch can continue functioning in the following situations:

- One or more fans fail within a fan module—Even with multiple fan failures, switches in the Cisco MDS 9000 Family can continue functioning. When a fan fails within a module, the functioning fans in the module increase their speed to compensate for the failed fan(s).
- The fan module is removed for replacement—The fan module is designed to be removed and replaced while the system is operating without presenting an electrical hazard or damage to the system. When

replacing a failed fan module in a running switch, be sure to replace the new fan module within five minutes.



Note

If one or more fans fail within a fan module, the Fan Status LED turns red. A fan failure could lead to temperature alarms if not corrected immediately.

The fan status is continuously monitored by the Cisco MDS NX-OS software. In case of a fan failure, the following action is taken:

- System messages are displayed.
- Call Home alerts are sent (if configured).
- SNMP notifications are sent (if configured).

Use the **show environment fan** command to display the fan module status.

This example shows the chassis fan information.

```
switch# show environment fan
-----
Fan           Model           Hw           Status
-----
Chassis      DS-9SLOT-FAN    1.2         ok
PS-1         --              --           ok
PS-2         --              --           absent
```

The possible Status field values for a fan module on the Cisco MDS 9500 Series switches are as follows:

- If the fan module is operating properly, the status is ok.
- If the fan is physically absent, the status is absent.
- If the fan is physically present but not working properly, the status is failure.

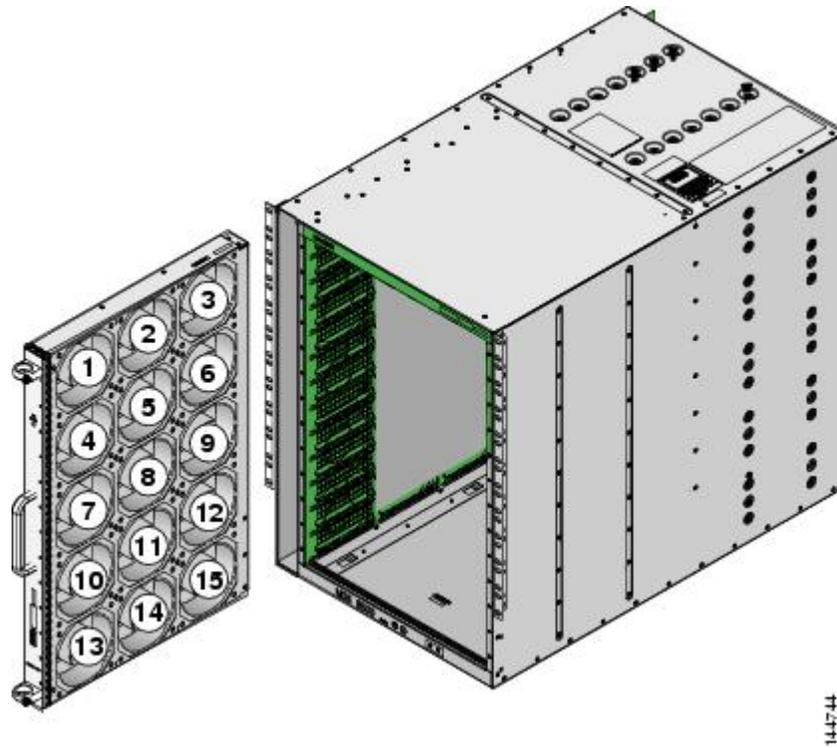
On the Cisco MDS 9513 Director, the front fan module has 15 fans. If the front fan module (DS-13SLT-FAN-F) State field contains "failure" in the **show environment fan** command output, it also displays the numbers of the failing fans.

This example shows a Cisco MDS 9513 front fan module failure.

```
switch# show environment fan
-----
Fan           Model           Hw           Status
-----
Chassis      DS-13SLT-FAN-F  0.3         failure 3 5 6 13
Chassis      DS-13SLT-FAN-R  0.3         ok
PS-1         --              --           ok
PS-2         --              --           ok
```

This figure shows the numbering of the fans in the front fan module on the Cisco MDS 9513 Director.

Figure 9: Cisco MDS 9513 Front Fan Module Numbering



The rear fan module (DS-13SLT-FAN-R) on the Cisco MDS 9513 Director has only two fans. If a fan in the rear fan module fails, the State field in the **show environment fan** command output only displays "failure" and not the failing fan number.

This example shows a fan module failure on a Cisco MDS 9513 Director.

```
switch# show environment fan
-----
Fan                Model                Hw                Status
-----
Chassis            DS-13SLT-FAN-F        0.3              ok
Chassis            DS-13SLT-FAN-R        0.3              failure
PS-1               --                   --               ok
PS-2               --                   --               ok
```

About Clock Modules

All switches in the Cisco MDS 9000 Family have two clock modules: Module A (primary) and Module B (redundant). The clock modules are designed, tested, and qualified for mission-critical availability with a mean time between failures (MTBF) of 3,660,316 hours. This translates to a potential failure every 365 years. Additionally, Cisco MDS 9000 Family switches are designed to automatically switch to the redundant clock module should the active clock module fail.



Tip

We recommend that you replace a failed clock module during a maintenance window.

Use the **show environment clock** command to display the status for both clock modules.

This example shows clock module information.

```
switch# show environment clock
-----
Clock          Model          Hw          Status
-----
A              DS-C9500-CL   0.0        ok/active
B              DS-C9500-CL   0.0        ok/standby
```

Displaying Environment Information

Use the **show environment** command to display all environment-related switch information.

```
switch# show environment
Clock:
-----
Clock          Model          Hw          Status
-----
A              Clock Module   1.0        ok/active
B              Clock Module   1.0        ok/standby

Fan:
-----
FAN            Model          Hw          Status
-----
Chassis        DS-2SLOT-FAN   0.0        ok
PS-1           --             --          ok
PS-2           --             --          absent

Temperature:
-----
Module  Sensor  MajorThresh  MinorThres  CurTemp  Status
      (Celsius)  (Celsius)    (Celsius)   (Celsius)
-----
1       1        75           60          32       ok
1       2        65           50          32       ok
1       3       -127         -127        43       ok
1       4       -127         -127        39       ok

Power Supply:
-----
PS  Model          Power      Power      Status
   (Watts)    (Amp @42V)
-----
1   PWR-950-AC     919.38    21.89     ok
2   --             --        --        absent
Mod Model          Power      Power      Power      Power      Status
   Requested Requested  Allocated Allocated
   (Watts)    (Amp @42V) (Watts)    (Amp @42V)
-----
1   DS-X9216-K9-SUP 220.08    5.24     220.08    5.24     powered-up

Power Usage Summary:
-----
Power Supply redundancy mode:          redundant
Total Power Capacity                   919.38  W
Power reserved for Supervisor(s) [-]  220.08  W
Power reserved for Fan Module(s) [-]   0.00   W
Power currently used by Modules [-]    0.00   W
-----
Total Power Available                   699.30  W
```

Default Settings

This table lists the default hardware settings

Table 22: Default Hardware Parameter Settings

Parameter	Default Setting
Power supply mode	Redundant mode.



Managing Modules

This chapter describes how to manage switching and services modules (also known as line cards) and provides information on monitoring module states.

- [About Modules, page 171](#)
- [Maintaining Supervisor Modules, page 174](#)
- [Verifying the Status of a Module, page 175](#)
- [Checking the State of a Module, page 176](#)
- [Connecting to a Module, page 177](#)
- [Reloading Modules, page 178](#)
- [Saving the Module Configuration, page 180](#)
- [Purging Module Configurations, page 181](#)
- [Powering Off Switching Modules, page 181](#)
- [Identifying Module LEDs, page 182](#)
- [EPLD Images, page 188](#)
- [SSI Boot Images, page 193](#)
- [Managing SSMs and Supervisor Modules, page 202](#)
- [Default Settings, page 206](#)

About Modules

This table describes the supervisor module options for switches in the Cisco MDS 9000 Family.

Table 23: Supervisor Module Options

Product	Number of Supervisor Modules	Supervisor Module Slot Number	Switching and Services Module Features
Cisco MDS 9513	Two modules	7 and 8	13-slot chassis allows any switching or services module in the other eleven slots.
Cisco MDS 9509	Two modules	5 and 6	9-slot chassis allows any switching or services module in the other seven slots.
Cisco MDS 9506	Two modules	5 and 6	6-slot chassis allows any switching or services module in the other four slots.
Cisco MDS 9216	One module	1	2-slot chassis allows one optional switching or services module in the other slot.
Cisco MDS 9216A	One module	1	2-slot chassis allows one optional switching or services module in the other slot.
Cisco MDS 9216i	One module	1	2-slot chassis allows one optional switching or services module in the other slot.

Supervisor Modules

Supervisor modules are automatically powered up and started with the switch. The Cisco MDS Family switches have the following supervisor module configurations:

- Cisco MDS 9513 Directors—Two supervisor modules, one in slot 7 (sup-1) and one in slot 8 (sup-2). When the switch powers up and both supervisor modules come up together, the active module is the one that comes up first. The standby module constantly monitors the active module. If the active module fails, the standby module takes over without any impact to user traffic.
- Cisco MDS 9506 and Cisco MDS 9509 Directors—Two supervisor modules, one in slot 5 (sup-1) and one in slot 6 (sup-2). When the switch powers up and both supervisor modules come up together, the active module is the one that comes up first. The standby module constantly monitors the active module. If the active module fails, the standby module takes over without any impact to user traffic.
- Cisco MDS 9216i switches—One supervisor module that includes an integrated switching module with 14 Fibre Channel ports and two Gigabit Ethernet ports.

- Cisco MDS 9200 Series switches—One supervisor module that includes an integrated 16-port switching module.

Module Terms	Fixed or Relative	Usage
module-7 and module-8	Fixed usage for the Cisco MDS 9513 Director	module-7 always refers to the supervisor module in slot 7 and module-8 always refers to the supervisor module in slot 8.
module-5 and module-6	Fixed usage for the Cisco MDS 9509 and Cisco MDS 9506 Directors	module-5 always refers to the supervisor module in slot 5 and module-6 always refers to the supervisor module in slot 6.
module-1	Fixed usage for the Cisco MDS 9200 Series switches	module-1 always refers to the supervisor module in slot 1.
sup-1 and sup-2	Fixed usage	On the Cisco MDS 9506 and MDS 9509 switches, sup-1 always refers to the supervisor module in slot 5 and sup-2 always refers to the supervisor module in slot 6. On the Cisco MDS 9513 Directors, sup-1 always refers to the supervisor module in slot 7 and sup-2 always refers to the supervisor module in slot 8.
sup-active and sup-standby	Relative usage	sup-active refers to the active supervisor module-relative to the slot that contains the active supervisor module. sup-standby refers to the standby supervisor module-relative to the slot that contains the standby supervisor module.

Module Terms	Fixed or Relative	Usage
sup-local and sup-remote	Relative usage	<p>If you are logged into the active supervisor, sup-local refers to the active supervisor module and sup-remote refers to the standby supervisor module.</p> <p>If you are logged into the standby supervisor, sup-local refers to the standby supervisor module (the one you are logged into.) There is no sup-remote available from the standby supervisor module (you cannot access a file system on the active sup).</p>

Switching Modules

Cisco MDS 9000 Family switches support any switching module in any non-supervisor slot. These modules obtain their image from the supervisor module.

Services Modules

Cisco MDS 9000 Family switches support any services module in any non-supervisor slot.

Refer to the [Cisco MDS 9000 Family SAN Volume Controller Configuration Guide](#) for more information on Cisco MDS 9000 Caching Services Modules (CSMs).

Maintaining Supervisor Modules

This section includes general information about replacing and using supervisor modules effectively.

Replacing Supervisor Modules

To avoid packet loss when removing a supervisor module from a Cisco MDS 9500 Series Director, take the supervisor modules out of service before removing the supervisor module.

Use the **out-of-service** command before removing the supervisor module.

out-of-service module *slot*

Where *slot* indicates the chassis slot number in which the supervisor module resides.



Note

You must remove and reinsert or replace the supervisor module to bring it into service.

Standby Supervisor Module Boot Variable Version

If the standby supervisor module boot variable images are not the same version as those running on the active supervisor module, the software forces the standby supervisor module to run the same version as the active supervisor module.

If you specifically set the boot variables of the standby supervisor module to a different version and reboot the standby supervisor module, the standby supervisor module will only load the specified boot variable if the same version is also running on the active supervisor module. At this point, the standby supervisor module is not running the images set in the boot variables.

Standby Supervisor Module Bootflash Memory

When updating software images on the standby supervisor module, verify that there is enough space available for the image using the `dir bootflash://sup-standby/` command. It is a good practice to remove older versions of Cisco MDS NX-OS images and kickstart images.

Standby Supervisor Module Boot Alert

If a standby supervisor module fails to boot, the active supervisor module detects that condition and generates a Call Home event and a system message and reboots the standby supervisor module approximately 3 to 6 minutes after the standby supervisor module moves to the loader> prompt.

The following system message is issued:

```
%DAEMON-2-SYSTEM_MSG:Standby supervisor failed to boot up.
```

This error message is also generated if one of the following situations apply:

- You remain at the loader> prompt for an extended period of time.
- You have not set the boot variables appropriately.

Verifying the Status of a Module

Before you begin configuring the switch, you need to ensure that the modules in the chassis are functioning as designed. To verify the status of a module at any time, issue the `show module` command. The interfaces in each module are ready to be configured when the ok status is displayed in the `show module` command output. A sample screenshot output of the `show module` command follows:

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  -
2    8      IP Storage Services Module DS-X9308-SMIP       ok
4    0      Caching Services Module   DS-X9530-SF1-K9     ok
5    0      Supervisor/Fabric-1       DS-X9530-SF1-K9     active *
6    0      Supervisor/Fabric-1       DS-X9530-SF1-K9     ha-standby
8    0      Caching Services Module   DS-X9560-SMAP       ok
9    32     1/2 Gbps FC Module        DS-X9032             ok

Mod  Sw          Hw          World-Wide-Name(s) (WWN)
---  -
-----
```

```

2   1.3(0.106a)  0.206  20:41:00:05:30:00:00:00 to 20:48:00:05:30:00:00:00
5   1.3(0.106a)  0.602  --
6   1.3(0.106a)  0.602  -- <----- New running version in module 6
8   1.3(0.106a)  0.702  --
9   1.3(0.106a)  0.3    22:01:00:05:30:00:00:00 to 22:20:00:05:30:00:00:00

```

```

Mod  MAC-Address(es)                               Serial-Num
----  -
2    00-05-30-00-9d-d2 to 00-05-30-00-9d-de  JAB064605a2
5    00-05-30-00-64-be to 00-05-30-00-64-c2
6    00-d0-97-38-b3-f9 to 00-d0-97-38-b3-fd  JAB06350B1R
8    00-05-30-01-37-7a to 00-05-30-01-37-fe  JAB072705ja
9    00-05-30-00-2d-e2 to 00-05-30-00-2d-e6  JAB06280ae9

```

* this terminal session

The Status column in the output should display an ok status for switching modules and an active or standby (or HA-standby) status for supervisor modules. If the status is either ok or active, you can continue with your configuration.



Note

A standby supervisor module reflects the HA-standby status if the HA switchover mechanism is enabled. If the warm switchover mechanism is enabled, the standby supervisor module reflects the standby status.

Checking the State of a Module

If your chassis has more than one switching module (also known as line card), you can check the progress by issuing the **show module** command several times and viewing the Status column each time. The switching module goes through a testing and an initializing stage before displaying an ok status.

This table describes the module states listed in the **show module** command output.

Table 24: Module States

Module Status Output	Description
powered up	The hardware has electrical power. When the hardware is powered up, the software begins booting.
testing	The switching module has established connection with the supervisor module and the switching module is performing bootup diagnostics.
initializing	The diagnostics have completed successfully and the configuration is being downloaded.
failure	The switch detects a switching module failure upon initialization and automatically attempts to power-cycle the module three times. After the third attempt it continues to display a failed state.
ok	The switch is ready to be configured.
power-denied	The switch detects insufficient power for a switching module to power up.
active	This module is the active supervisor module and the switch is ready to be configured.
HA-standby	The HA switchover mechanism is enabled on the standby supervisor module.
standby	The warm switchover mechanism is enabled on the standby supervisor module.

Connecting to a Module

At any time, you can connect to any module using the **attach module** command. Once you are at the module prompt, you can obtain further details about the module using module-specific commands.

You can also use the **attach module** command as follows:

- To display the standby supervisor module information. You cannot configure the standby supervisor module using this command.
- To display the switching module portion of the Cisco MDS 9200 Series supervisor module which resides in slot 1.

SUMMARY STEPS

1. **attach module** *slot*
2. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	attach module <i>slot</i> Example: <pre>switch# attach module 4 Attaching to module 4 ... To exit type 'exit', to abort type '\$.' module-4#</pre>	Provides direct access to the module in the specified slot.
Step 2	exit Example: <pre>module-4# exit rlogin: connection closed. switch#</pre>	Exits module access configuration mode.

Reloading Modules

You can reload the entire switch, reset specific modules in the switch, or reload the image on specific modules in the switch.

Reloading a Switch

To reload the switch, issue the **reload** command without any options. When you issue this command, you reboot the switch (see the [Cisco MDS 9000 NX-OS Release 4.1\(x\) and SAN-OS 3\(x\) Software Upgrade and Downgrade Guide](#)).

Power Cycling Modules

You can power cycle any module in a chassis. Power cycling reinitializes the module.

SUMMARY STEPS

1. Identify the module that needs to be reset.
2. Issue the **reload module** command to reset the identified module. This command power cycles the selected module.

DETAILED STEPS

Step 1 Identify the module that needs to be reset.

Step 2 Issue the **reload module** command to reset the identified module. This command power cycles the selected module.

reload module *number*

number indicates the slot in which the identified module resides.

```
switch# reload module 2
```

Caution Reloading a module disrupts traffic through the module.

Reloading Switching Modules

Switching modules automatically download their images from the supervisor module and do not need a forced download. This procedure is provided for reference if a new image is required.

SUMMARY STEPS

1. Identify the switching module that requires the new image.
2. Issue the **reload module** command to update the image on the switching module.

DETAILED STEPS

Step 1 Identify the switching module that requires the new image.

Step 2 Issue the **reload module** command to update the image on the switching module.

reload module *number* **force-dnld**

number indicates the slot in which the identified module resides. In this example, the identified module resides in slot 9:

```
switch# reload module 9 force-dnld
Jan  1 00:00:46 switch %LC-2-MSG:SLOT9 LOG_LC-2-IMG_DNLD_COMPLETE: COMPLETED
downloading of linecard image. Download successful...
```

Saving the Module Configuration

Issue the **copy running-config startup-config** command to save the new configuration into nonvolatile storage. Once this command is issued, the running and the startup copies of the configuration are identical.

This table displays various scenarios when module configurations are preserved or lost.

Table 25: Switching Module Configuration Status

Scenario	Consequence
You remove a switching module and issue the copy running-config startup-config command.	The configured module information is lost.
You remove a switching module and reinsert the same switching module before issuing the copy running-config startup-config command.	The configured module information is saved.
You remove a switching module, insert the same type switching module in the same slot, and issue a reload module number command.	The configured module information is saved.
You enter a reload module number command to reload a switching module.	The configured module information is preserved.
<p>You remove a switching module and insert a different type of switching module in the slot. For example, you replace a 16-port switching module with a 32-port switching module.</p> <p>Sample scenario:</p> <ol style="list-style-type: none"> 1 The switch currently has a 16-port switching module and the startup and running configuration files are the same. 2 You replace the 16-port switching module in the switch with a 32-port switching module. 3 Next, you remove the 32-port switching module and replace it with the same 16-port switching module referred to in Step 1. 4 You enter the reload command to reload the switch. 	<p>The configured module information is lost from the running configuration. The default configuration is applied.</p> <p>The configured module information remains in startup configuration until a copy running-config startup-config command is issued again.</p> <p>Sample response:</p> <ol style="list-style-type: none"> 1 The switch uses the 16-port switching module and the present configuration is saved in nonvolatile storage. 2 The factory default configuration is applied. 3 The factory default configuration is applied. 4 The configuration saved in nonvolatile storage referred to in Step 1 is applied.

Purging Module Configurations

Enter the **purge module *slot* running-config** command to delete the configuration in a specific module. Once you enter this command, the Cisco NX-OS software clears the running configuration for the specified slot. This command does not work on supervisor modules or on any slot that currently has a module. This command only works on an empty slot (where the specified module once resided).

The **purge module** command clears the configuration for any module that previously existed in a slot and has since been removed. While the module was in that slot, some parts of the configuration may have been stored in the running configuration and cannot be reused (for example, IP addresses), unless you clear it from the running configuration.

For example, suppose you create an IP storage configuration with an IPS module in slot 3 in Switch A. This module uses IP address 10.1.5.500. You decide to remove this IPS module and move it to Switch B, and you no longer need the IP address 10.1.5.500. If you try to configure this unused IP address, you will receive an error message that prevents you from proceeding with the configuration. In this case, you must enter the **purge module 3 running-config** command to clear the old configuration on Switch A before proceeding with using this IP address.

Powering Off Switching Modules

You can power off a switching module from the command-line interface (CLI). By default, all switching modules are in the power up state when the chassis loads or you insert the module into the chassis.

SUMMARY STEPS

1. **configure terminal**
2. **[no] poweroff module *slot***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] poweroff module <i>slot</i> Example: <pre>switch(config)# poweroff module 2</pre>	Powers off the specified module. Use the no form of the command to power on a module.

Identifying Module LEDs

This table describes the LEDs for the Cisco MDS 9200 Series integrated supervisor modules.

Table 26: LEDs for the Cisco MDS 9200 Series Supervisor Modules

LED	Status	Description
Status	Green	All diagnostics pass. The module is operational (normal initialization sequence).
	Orange	The module is booting or running diagnostics (normal initialization sequence). or The inlet air temperature of the system has exceeded the maximum system operating temperature limit (a minor environmental warning). To ensure maximum product life, you should immediately correct the environmental temperature and restore the system to normal operation.
	Red	The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. or The inlet air temperature of the system has exceeded the safe operating temperature limits of the card (a major environmental warning). The card has been shut down to prevent permanent damage. The system will be shut down after two minutes if this condition is not cleared.
Speed	On	2-Gbps mode and beacon mode disabled.
	Off	1-Gbps mode and beacon mode disabled.
	Flashing	Beacon mode enabled.

LED	Status	Description
Link	Solid green	Link is up.
	Solid yellow	Link is disabled by software.
	Flashing yellow	A fault condition exists.
	Off	No link.

This table describes the LEDs for the Cisco MDS 9200 Series interface module.

Table 27: LEDs on the Cisco MDS 9200 Series Interface Module

LED	Status	Description
Status	Green	All diagnostics pass. The module is operational (normal initialization sequence).
	Orange	The module is booting or running diagnostics (normal initialization sequence). or The inlet air temperature of the system has exceeded the maximum system operating temperature limit (a minor environmental warning). To ensure maximum product life, you should immediately correct the environmental temperature and restore the system to normal operation.
	Red	The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. or The inlet air temperature of the system has exceeded the safe operating temperature limits of the card (a major environmental warning). The card has been shut down to prevent permanent damage.

LED	Status	Description
System	Green	All chassis environmental monitors are reporting OK.
	Orange	The power supply failed or the power supply fan failed. or Incompatible power supplies are installed. or The redundant clock failed.
	Red	The temperature of the supervisor module exceeded the major threshold.
MGMT 10/100 Ethernet Link LED	Green	Link is up.
	Off	No link.
MGMT 10/100 Ethernet Activity LED	Green	Traffic is flowing through port.
	Off	No link or no traffic.

This table describes the LEDs for the 16-port and 32-port switching modules, and the 4-port, 12-port, 24-port, and 48-port Generation 2 switching modules.

Table 28: LEDs for the Cisco MDS 9000 Family Fibre Channel Switching Modules

LED	Status	Description
Status	Green	All diagnostics pass. The module is operational (normal initialization sequence).
	Red	The module is booting or running diagnostics (normal initialization sequence). or The inlet air temperature of the system has exceeded the maximum system operating temperature limit (a minor environmental warning). To ensure maximum product life, you should immediately correct the environmental temperature and restore the system to normal operation.
	Orange	The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. or The inlet air temperature of the system has exceeded the safe operating temperature limits of the card (a major environmental warning). The card has been shut down to prevent permanent damage.
Speed	On	2-Gbps mode.
	Off	1-Gbps mode.

LED	Status	Description
Link	Solid green	Link is up.
	Steady flashing green	Link is up (beacon used to identify port).
	Intermittent flashing green	Link is up (traffic on port).
	Solid yellow	Link is disabled by software.
	Flashing yellow	A fault condition exists.
	Off	No link.

The LEDs on the supervisor module indicate the status of the supervisor module, power supplies, and the fan module.

This table provides more information about these LEDs.

Table 29: LEDs for the Cisco MDS 9500 Series Supervisor Modules

LED	Status	Description
Status	Green	All diagnostics pass. The module is operational (normal initialization sequence).
	Orange	The module is booting or running diagnostics (normal initialization sequence). or An over temperature condition has occurred (a minor threshold has been exceeded during environmental monitoring).
	Red	The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. or An over temperature condition occurred (a major threshold was exceeded during environmental monitoring).

LED	Status	Description
System Note The System and Pwr Mgmt LEDs on a redundant supervisor module are synchronized to the active supervisor module.	Green	All chassis environmental monitors are reporting OK.
	Orange	The power supply has failed or the power supply fan has failed. or Incompatible power supplies are installed. or The redundant clock has failed.
	Red	The temperature of the supervisor module major threshold has been exceeded.
Active	Green	The supervisor module is operational and active.
	Orange	The supervisor module is in standby mode.
Pwr Mgmt ¹	Green	Sufficient power is available for all modules.
	Orange	Sufficient power is not available for all modules.
MGMT 10/100 Ethernet Link LED	Green	Link is up.
	Off	No link.
MGMT 10/100 Ethernet Activity LED	Green	Traffic is flowing through port.
	Off	No link or no traffic.
Compact Flash	Green	The external CompactFlash card is being accessed.
	Off	No activity.

EPLD Images

Switches and directors in the Cisco MDS 9000 Family contain several electrical programmable logical devices (EPLDs) that provide hardware functionalities in all modules. EPLD image upgrades are periodically provided to include enhanced hardware functionality or to resolve known issues.



Tip

Refer to the Cisco MDS NX-OS Release Notes to verify if the EPLD has changed for the Cisco NX-OS image version being used.

Upgrading EPLD Images

You can upgrade the EPLD images on the modules.



Note

The same procedure used to upgrade the EPLD images on a module can be used to downgrade the EPLD images.

SUMMARY STEPS

1. Log into the switch through the console port, an SSH session, or a Telnet session.
2. Enter the **show version** command to verify the Cisco MDS NX-OS software release running on the MDS switch.
3. If necessary, upgrade the Cisco MDS NX-OS software running on your switch (see the [Cisco MDS 9000 NX-OS Release 4.1\(x\) and SAN-OS 3\(x\) Software Upgrade and Downgrade Guide](#)).
4. Issue the **dir bootflash:** or **dir slot0:** command to verify that the EPLD software image file corresponding to your Cisco MDS NX-OS release is present on the active supervisor module. For example, if your switch is running Cisco MDS SAN-OS Release 2.1(2), you must have m9000-epld-2.1.2.img in bootflash: or slot0: on the active supervisor module.
5. If you need to obtain the appropriate EPLD software image file, follow these steps:
6. Use the **install module number epld url** command on the active supervisor module to upgrade EPLD images for a module.

DETAILED STEPS

Step 1 Log into the switch through the console port, an SSH session, or a Telnet session.

Step 2 Enter the **show version** command to verify the Cisco MDS NX-OS software release running on the MDS switch.

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
```

```
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html
```

```
Software
  BIOS:      version 1.0.8
  loader:    version unavailable [last: 1.0(0.267c)]
  kickstart: version 2.1(2) [build 2.1(2.47)] [gdb]
  system:    version 2.1(2) [build 2.1(2.47)] [gdb]
```

```
...
```

Step 3 If necessary, upgrade the Cisco MDS NX-OS software running on your switch (see the [Cisco MDS 9000 NX-OS Release 4.1\(x\) and SAN-OS 3\(x\) Software Upgrade and Downgrade Guide](#)).

Step 4 Issue the **dir bootflash:** or **dir slot0:** command to verify that the EPLD software image file corresponding to your Cisco MDS NX-OS release is present on the active supervisor module. For example, if your switch is running Cisco MDS SAN-OS Release 2.1(2), you must have m9000-epld-2.1.2.img in bootflash: or slot0: on the active supervisor module.

```
switch# dir bootflash:
 12288 Jan 01 00:01:07 1980 lost+found/
2337571 May 31 13:43:02 2005 m9000-epld-2.1.2.img
...
```

You can find the EPLD images at the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/mds-epld>

Step 5 If you need to obtain the appropriate EPLD software image file, follow these steps:

- 1 Download the EPLD software image file from Cisco.com to your FTP server.
- 2 Verify that you have enough free space available on the active and standby supervisor memory devices that you plan to use, either bootflash: or slot0:. The download site on Cisco.com shows the size of the EPLD image file in bytes.

The following example shows how to display the available memory for the bootflash: devices on the active and standby supervisors:

```
switch# dir bootflash:
 12288 Jan 01 00:01:06 1980 lost+found/
14765056 Mar 21 15:35:06 2005 m9500-sflek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sflek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sflek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sflek9-mz.2.1.1a.bin
```

```
Usage for bootflash://sup-local
141066240 bytes used
 43493376 bytes free
184559616 bytes total
```

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  ---    -
```

```

2    32    Storage Services Module          DS-X9032-SSM          ok
5     0    Supervisor/Fabric-1                DS-X9530-SF1-K9      active *
6     0    Supervisor/Fabric-1                DS-X9530-SF1-K9      ha-standby
...

```

The **show module** command output shows that the standby supervisor is in slot 6. Use the **attach** command to access the supervisor module.

```

switch# attach module 6
...
switch(standby)# dir bootflash:
 12288 Jan 01 00:01:06 1980 lost+found/
14765056 Mar 21 15:35:06 2005 m9500-sflek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sflek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sflek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sflek9-mz.2.1.1a.bin

Usage for bootflash://sup-local
141066240 bytes used
 43493376 bytes free
184559616 bytes total

switch(standby)# exit
switch#

```

The following example shows how to display the available memory for the slot0: devices on the active and standby supervisors:

```

switch# dir slot0:
 12288 Jan 01 00:01:06 1980 lost+found/
14765056 Mar 21 15:35:06 2005 m9500-sflek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sflek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sflek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sflek9-mz.2.1.1a.bin

Usage for slot:
141066240 bytes used
43493376 bytes free
184559616 bytes total

```

```

switch# show module
Mod  Ports  Module-Type          Model          Status
---  ---  -
2    32    Storage Services Module  DS-X9032-SSM  ok
5     0    Supervisor/Fabric-1    DS-X9530-SF1-K9  active *
6     0    Supervisor/Fabric-1    DS-X9530-SF1-K9  ha-standby
...

```

The **show module** command output shows that the standby supervisor is in slot 6. Use the **attach** command to access the supervisor module.

```

switch# attach module 6

```

```

...
switch(standby)# dir slot0:
  12288 Jan 01 00:01:06 1980 lost+found/
 14765056 Mar 21 15:35:06 2005 m9500-sflek9-kickstart-mz.2.1.1.bin
 15944704 Apr 06 16:46:04 2005 m9500-sflek9-kickstart-mz.2.1.1a.bin
 48063243 Mar 21 15:34:46 2005 m9500-sflek9-mz.2.1.1.bin
 48036239 Apr 06 16:45:41 2005 m9500-sflek9-mz.2.1.1a.bin

Usage for slot0:
141066240 bytes used
 43493376 bytes free
184559616 bytes total

switch(standby)# exit
switch#

```

- 3 If there is not enough space, delete unneeded files.

```
switch# delete bootflash:m9500-sflek9-kickstart-mz.2.1.1.bin
```

The **show module** command output shows that the standby supervisor is in slot 6. Use the **attach** command to access the supervisor module.

```
switch# attach module 6
switch(standby)# delete bootflash:m9500-sflek9-kickstart-mz.2.1.1.bin
switch(standby)# exit
switch#

```

- 4 Copy the EPLD image file from the FTP server to the bootflash: or slot0: device in the active supervisor module. The following example shows how to copy to bootflash:

```
switch# copy ftp://10.1.7.2/m9000-epld-2.1.2.img bootflash:m9000-epld-2.1.2.img
```

Note The system will automatically synchronize the EPLD image to the standby supervisor if automatic copying is enabled.

```
switch# configure terminal
switch(config)# boot auto-copy
```

- Step 6** Use the **install module *number* *epld url*** command on the active supervisor module to upgrade EPLD images for a module.

```
switch# install module 2 epld bootflash:m9000-epld-2.1.2.img
```

EPLD	Curr Ver	New Ver
XBUS IO	0x07	0x07
UD Flow Control	0x05	0x05
PCI ASIC I/F	0x05	0x05
PCI Bridge	0x05	0x07

WARNING: Upgrade process could take upto 15 minutes.

```

Module 2 will be powered down now!!
Do you want to continue (y/n) ? y
\ <-----progress twirl
Module 2 EPLD upgrade is successful

```

If you forcefully upgrade a module that is not online, all EPLDs are forcefully upgraded. If the module is not present in the switch, an error is returned. If the module is present, the command process continues. To upgrade a module that is not online but is present in the chassis, use the same command. The switch software prompts you to continue after reporting the module state. When you confirm your intention to continue, the upgrade continues.

```

switch# install module 2 epld bootflash:m9000-epld-2.1.2.img
\ <-----progress twirl
Module 2 EPLD upgrade is successful

```

Note When you upgrade the EPLD module on Cisco MDS 9100 Series switches, you receive the following message:

```

Data traffic on the switch will stop now!!
Do you want to continue (y/n) ?

```

Displaying EPLD Image Versions

Use the **show version module *number* epld** command to view all current EPLD versions on a specified module.

```

switch# show version module 2 epld
EPLD Device          Version
-----
Power Manager        0x07
XBUS IO               0x07
UD Flow Control      0x05
PCI ASIC I/F         0x05
PCI Bridge            0x07

```

Use the **show version module epld *url*** command to view the available EPLD versions.

```

switch# show version epld bootflash:m9000-epld-2.1.1a.img
MDS series EPLD image, built on Wed May  4 09:52:37 2005

Module Type          EPLD Device          Version
-----
MDS 9500 Supervisor 1  XBUS 1 IO            0x09
                    XBUS 2 IO            0x0c
                    UD Flow Control      0x05
                    PCI ASIC I/F         0x04

1/2 Gbps FC Module (16 Port)  XBUS IO              0x07
                    UD Flow Control      0x05
                    PCI ASIC I/F         0x05

1/2 Gbps FC Module (32 Port)  XBUS IO              0x07
                    UD Flow Control      0x05
                    PCI ASIC I/F         0x05

Advanced Services Module  XBUS IO              0x07

```

	UD Flow Control	0x05
	PCI ASIC I/F	0x05
	PCI Bridge	0x07
IP Storage Services Module (8 Port)	Power Manager	0x07
	XBUS IO	0x03
	UD Flow Control	0x05
	PCI ASIC I/F	0x05
	Service Module I/F	0x0a
	IPS DB I/F	0x1a
IP Storage Services Module (4 Port)	Power Manager	0x07
	XBUS IO	0x03
	UD Flow Control	0x05
	PCI ASIC I/F	0x05
	Service Module I/F	0x1a
Caching Services Module	Power Manager	0x08
	XBUS IO	0x03
	UD Flow Control	0x05
	PCI ASIC I/F	0x05
	Service Module I/F	0x72
	Memory Decoder 0	0x02
	Memory Decoder 1	0x02
MDS 9100 Series Fabric Switch	XBUS IO	0x03
	PCI ASIC I/F	0x40000003
2x1GE IPS, 14x1/2Gbps FC Module	Power Manager	0x07
	XBUS IO	0x05
	UD Flow Control	0x05
	PCI ASIC I/F	0x07
	IPS DB I/F	0x1a

SSI Boot Images

As of Cisco SAN-OS Release 2.0(2b), you can specify the SSI boot image for a Storage Services Module (SSM) to configure Fibre Channel switching and Intelligent Storage Services (see [Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide](#) and the [Cisco MDS 9000 Family SAN-Tap Deployment Guide](#)). Once you set the SSI image boot variable, you do not need to reset it for upgrades or downgrades to any Cisco MDS NX-OS or SAN-OS release that supports the SSI image.



Note

If your switch is running Cisco MDS SAN-OS Release 2.1(2) or later, a newly installed SSM initially operates in Fibre Channel switching mode by default.



Note

If you downgrade to a Cisco MDS SAN-OS release that does not support the SSM, you must power down the module. The boot variables for the SSM are lost.

Installing the SSI Boot Image

You can install the SSI boot image on the following modules:

- Storage Services Module (SSM)

- MSM-18+4 Multiservice Module
- MDS 9222i Module-1 Module

The SSM supports normal Fibre Channel switching and Intelligent Storage Services. To use Fibre Channel switching and Intelligent Storage Services, you must install an SSI boot image on the SSM.



Note A newly installed SSM initially operates in Fibre Channel switching mode by default.

SUMMARY STEPS

1. Log into the switch through the console port, an SSH session, or a Telnet session.
2. Enter the **dir modflash://slot-1/** command to verify that the SSI boot image file corresponding to your Cisco MDS NX-OS release is present on the active supervisor module.
3. If the file is not present in bootflash: or the modflash:, follow these steps:
4. Enter the **install ssi** command to install the SSI boot image on the SSM.
5. Enter the **show module** command to verify the status of the SSM.

DETAILED STEPS

Step 1 Log into the switch through the console port, an SSH session, or a Telnet session.

Step 2 Enter the **dir modflash://slot-1/** command to verify that the SSI boot image file corresponding to your Cisco MDS NX-OS release is present on the active supervisor module.
For example, if your switch is running Cisco NX-OS Release 4.1(1b), you must have m9000-ek9-ssi-mz.4.1.1b.bin in modflash: on the SSM. To determine the correct SSI boot image to use, refer to the [Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images](#).

You can find the SSI images at the following URL:

<http://www.cisco.com/pcgi-bin/tablebuild.pl/mds9000-ssi-3des>

Step 3 If the file is not present in bootflash: or the modflash:, follow these steps:

- 1 Enter the **dir modflash://slot-1/** command to ensure that there is enough free space for the SSI image file. If necessary, enter the **delete modflash://slot-1/filename** command to remove files.
- 2 Download the appropriate SSI boot image file to your FTP server and copy it from an FTP server to modflash: on the SSM:

```
switch# copy ftp://10.1.7.2/m9000-ek9-ssi-mz.4.1.1b.bin
modflash://4-1/m9000-ek9-ssi-mz.4.1.1b.bin
```

Step 4 Enter the **install ssi** command to install the SSI boot image on the SSM.

Note As of Cisco SAN-OS Release 3.0(2), if the SSI boot image is located on bootflash: the **install ssi** command copies the SSI boot image to the modflash: on the SSM.

```
switch# install ssi modflash://4-1/m9000-ek9-ssi-mz.4.1.1b.bin
```

Step 5 Enter the **show module** command to verify the status of the SSM.

```
switch# show module
Mod Ports Module-Type                               Model                Status
-----
4    32    Storage Services Module                          DS-X9032-SSM        ok
...
Mod      Application Image Description                    Application Image Version
-----
4        SSI linecard image                             4.1 (1b)
...
```

Upgrading or Downgrading the SSI Boot Image

You can upgrade the SSI boot image.

SUMMARY STEPS

1. Verify that the correct SSI boot image is present on your switch
2. Update the SSI boot image using one of the following methods:

DETAILED STEPS

Step 1 Verify that the correct SSI boot image is present on your switch

Step 2 Update the SSI boot image using one of the following methods:

- If your switch is running Cisco MDS SAN-OS Release 2.0(1a) through Release 2.1(1a), configure the SSI boot variable to upgrade or downgrade the SSI boot image on the module.
- Use the **install ssi** command to upgrade or downgrade the SSI boot image on the module.

SSI Boot Image Upgrade Considerations for the SSM

When you upgrade, or downgrade, the SSI boot image on an SSM, you might disrupt traffic through the module.

This table describes how updating the SSI boot image affects SSM traffic.

Table 30: SSI Boot Image Upgrading Effects on SSM Traffic

Cisco MDS SAN-OS Release	Traffic Type	Disrupts Traffic?
2.0(2b) through 2.1(1a)	All	Yes

Cisco MDS SAN-OS Release	Traffic Type	Disrupts Traffic?
2.1(2) and later	Layer 2 Fiber Channel switching only	No Note Requires EPLD version 2.1(2).
	Both Layer 2 Fiber Channel switching and Layer 3 Intelligent Storage Services (such as FCWA, NASB, SANTap, ISAPI virtualization)	Yes
	Layer 3 Intelligent Storage Services (such as FCWA, NASB, SANTap, ISAPI virtualization) only	Yes



Note Updating the SSI boot image disrupts Layer 3 Intelligent Storage Services traffic. If you have configured Layer 3 Intelligent Storage Services on your SSM, we recommend that you shut down these services before upgrading the SSI boot image. You can use dual fabric configuration to minimize the impact of shutting down Layer 3 services.

Verifying the SSI Boot Image

You can verify the Cisco MDS NX-OS release and SSI boot image on your switch.

SUMMARY STEPS

1. Log into the switch through the console port, an SSH session, or a Telnet session.
2. Enter the **show version** command to ensure that your switch is running Cisco MDS SAN-OS Release 2.1(1a) or later system and kickstart images.
3. If necessary, upgrade the Cisco MDS SAN-OS or NX-OS software running on your switch (see the [Cisco MDS 9000 NX-OS Release 4.1\(x\) and SAN-OS 3\(x\) Software Upgrade and Downgrade Guide](#)).
4. Issue the **dir bootflash:** or **dir slot0:** command to verify that the SSI software image file corresponding to your Cisco MDS SAN-OS release is present on the active supervisor module. For example, if your switch is running Cisco MDS NX-OS Release 4.1(1b), you must have m9000-ek9-ssi-mz.4.1.1b.bin in bootflash: or slot0: on the active supervisor module. See to the [Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images](#).
5. If you need to obtain the appropriate SSI software image file, perform the following steps:

DETAILED STEPS

Step 1 Log into the switch through the console port, an SSH session, or a Telnet session.

Step 2 Enter the **show version** command to ensure that your switch is running Cisco MDS SAN-OS Release 2.1(1a) or later system and kickstart images.

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

Software
  BIOS:      version 1.0.8
  loader:    version unavailable [last: 1.0(0.267c)]
  kickstart: version 2.1(2) [build 2.1(2.47)] [gdb]
  system:    version 2.1(2) [build 2.1(2.47)] [gdb]

...
```

Step 3 If necessary, upgrade the Cisco MDS SAN-OS or NX-OS software running on your switch (see the [Cisco MDS 9000 NX-OS Release 4.1\(x\) and SAN-OS 3\(x\) Software Upgrade and Downgrade Guide](#)).

Step 4 Issue the **dir bootflash:** or **dir slot0:** command to verify that the SSI software image file corresponding to your Cisco MDS SAN-OS release is present on the active supervisor module. For example, if your switch is running Cisco MDS NX-OS Release 4.1(1b), you must have m9000-ek9-ssi-mz.4.1.1b.bin in bootflash: or slot0: on the active supervisor module. See to the [Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images](#).

Note As of Cisco MDS SAN-OS Release 2.1(2), we recommend that you use modflash: on the SSM. You can check for the presence of the SSI software image using the **dir modflash://slot-1/** command.

```
switch# dir bootflash:
 12288 Jan 01 00:01:07 1980 lost+found/
3821032 May 10 13:43:02 2005 m9000-ek9-ssi-mz.2.1.2.bin
...
```

You can find the SSI images at the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/mds9000-ssi-3des>

Step 5 If you need to obtain the appropriate SSI software image file, perform the following steps:

- 1 Download the SSI software image file from Cisco.com to your FTP server.
- 2 Verify that you have enough free space available on the active and standby supervisor memory devices which you plan to use, either bootflash: or slot0:. The download site on Cisco.com shows the size of the boot image file in bytes.

Note As of Cisco MDS SAN-OS Release 2.1(2), we recommend that you use modflash: on the SSM. You can check the available space using the **dir modflash://slot-1/** command.

The following example shows how to display the available memory for the bootflash: devices on the active and standby supervisors:

```
switch# dir bootflash:
 12288 Jan 01 00:01:06 1980 lost+found/
14765056 Mar 21 15:35:06 2005 m9500-sflek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sflek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sflek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sflek9-mz.2.1.1a.bin
```

```
Usage for bootflash://sup-local
141066240 bytes used
 43493376 bytes free
184559616 bytes total
```

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  -
4    32     Storage Services Module    DS-X9032-SSM        ok
5    0      Supervisor/Fabric-1        DS-X9530-SF1-K9     active *
6    0      Supervisor/Fabric-1        DS-X9530-SF1-K9     ha-standby
...
```

The **show module** command output shows that the standby supervisor is in slot 6. Use the **attach** command to access the supervisor module.

```
switch# attach module 6
...
switch(standby)# dir bootflash:
 12288 Jan 01 00:01:06 1980 lost+found/
14765056 Mar 21 15:35:06 2005 m9500-sflek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sflek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sflek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sflek9-mz.2.1.1a.bin
```

```
Usage for bootflash://sup-local
141066240 bytes used
 43493376 bytes free
184559616 bytes total
```

```
switch(standby)# exit
switch#
```

The following example shows how to display the available memory for the slot0: devices on the active and standby supervisors.

```
switch# dir slot0:
 12288 Jan 01 00:01:06 1980 lost+found/
14765056 Mar 21 15:35:06 2005 m9500-sflek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sflek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sflek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sflek9-mz.2.1.1a.bin
```

```
Usage for slot:
141066240 bytes used
 43493376 bytes free
184559616 bytes total
```

```
switch# show module
Mod  Ports  Module-Type                               Model                               Status
---  -
4    32     Storage Services Module                  DS-X9032-SSM                       ok
5    0      Supervisor/Fabric-1                      DS-X9530-SF1-K9                    active *
6    0      Supervisor/Fabric-1                      DS-X9530-SF1-K9                    ha-standby
...
```

The **show module** command output shows that the standby supervisor is in slot 6. Use the **attach** command to access the supervisor module.

```
switch# attach module 6
...
switch(standby)# dir slot0:
 12288 Jan 01 00:01:06 1980 lost+found/
14765056 Mar 21 15:35:06 2005 m9500-sflek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sflek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sflek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sflek9-mz.2.1.1a.bin
```

```
Usage for slot0:
141066240 bytes used
 43493376 bytes free
184559616 bytes total
```

```
switch(standby)# exit
switch#
```

- 3 If there is not enough space, delete unneeded files.

```
switch# delete bootflash:m9500-sflek9-kickstart-mz.2.1.1.bin
```

The **show module** command output shows that the standby supervisor is in slot 6. Use the **attach** command to access the supervisor module.

```
switch# attach module 6
switch(standby)# delete bootflash:m9500-sflek9-kickstart-mz.2.1.1.bin
switch(standby)# exit
switch#
```

- 4 Copy the EPLD image file from the FTP server to the bootflash: or slot0: device in the active supervisor module. The following example shows how to copy to bootflash:

```
switch# copy ftp://10.1.7.2/m9000-epld-4.1.1b.img bootflash:m9000-epld-4.1.1b.img
```

Note The system will automatically synchronize the ELPD image to the standby supervisor if automatic copying is enabled.

```
switch# configure terminal
switch(config)# boot auto-copy
```

Using the install ssi Command

You can use the **install ssi** command to update the boot image on an SSM. If the SSM is performing Fibre Channel switching and no Intelligent Storage Services are provisioned on the module, this operation does not disrupt traffic through the module. If the SSM is configured for Intelligent Storage Services, a warning is displayed at the command prompt indicating that the operation will disrupt traffic and asking if you wish to continue.



Note The SSM must be running EPLD version 2.1(2) to use the **install ssi** command. You must install the SSM on a Cisco MDS 9500 Series switch to update the EPLD.

SUMMARY STEPS

1. Log into the switch through the console port, an SSH session, or a Telnet session.
2. Verify that the SSM is physically installed in the switch. If the module is not physically installed, insert it into the desired slot. Issue a **show module** command to verify the status of the module.
3. Verify the Cisco MDS NX-OS release running on the switch and the location and name of the SSI boot image on the switch.
4. Install the SSI image on the SSM.
5. Issue the **show boot** command to display the current contents of the image boot variable for the SSM.
6. Save the new boot variable configuration so the new boot image is used when the switch reboots.
7. Issue the **show module** command to verify the status of the SSM.

DETAILED STEPS

Step 1 Log into the switch through the console port, an SSH session, or a Telnet session.

Step 2 Verify that the SSM is physically installed in the switch. If the module is not physically installed, insert it into the desired slot. Issue a **show module** command to verify the status of the module.

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  -
4    32     Storage Services Module    DS-X9032-SSM        ok
5    0      Supervisor/Fabric-1        DS-X9530-SF1-K9     active *
6    0      Supervisor/Fabric-1        DS-X9530-SF1-K9     ha-standby
```

...

Note the slot number for later reference.

Step 3 Verify the Cisco MDS NX-OS release running on the switch and the location and name of the SSI boot image on the switch.

Step 4 Install the SSI image on the SSM.

Note If the SSI boot image is located on bootflash: the **install ssi** command copies the SSI boot image to modflash: on the SSM.

```
switch# install ssi modflash://4-1/m9000-ek9-ssi-mz.4.1.1b.bin module 4
```

Note If the SSM is configured for Layer 3 Fibre Channel switching or Intelligent Storage Services, a warning will be displayed at the command prompt indicating that the operation will disrupt traffic and you will be asked if you wish to continue.

Note We recommend that you reference the SSI boot image on modflash: on the SSM. Use the **install ssi modflash://slot-1/filename module alor** command to install the SSI image.

Step 5 Issue the **show boot** command to display the current contents of the image boot variable for the SSM.

```
switch# show boot
sup-1
kickstart variable = bootflash:/boot-2-0-1-9
system variable =
bootflash:/isan-2-0-1-9;bootflash:/isan-2-0-0-181b;bootflash:/isan-2-0-0-181b
sup-2
kickstart variable = bootflash:/boot-2-0-1-9
system variable =
bootflash:/isan-2-0-1-9;bootflash:/isan-2-0-0-181b;bootflash:/isan-2-0-0-181b
Module 4
ssi variable = modflash://4-1/m9000-ek9-ssi-mz.4.1.1b.bin
```

Step 6 Save the new boot variable configuration so the new boot image is used when the switch reboots.

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

Note If you do not save this configuration, it is lost on a switch reboot. In addition, the SSM comes up in Fibre Channel switching mode. You must perform this procedure again to recover the SSI image boot variable configuration.

Step 7 Issue the **show module** command to verify the status of the SSM.

```
switch# show module
```

Mod	Ports	Module-Type	Model	Status
4	32	Storage Services Module	DS-X9032-SSM	ok
5	0	Supervisor/Fabric-1	DS-X9530-SF1-K9	active *
6	0	Supervisor/Fabric-1	DS-X9530-SF1-K9	ha-standby

Mod	Sw	Hw	World-Wide-Name (s)	(WWN)
---	-----	-----	-----	-----

```

4    2.1(2)      0.30    20:c1:00:05:30:00:06:de to 20:e0:00:05:30:00:06:de
5    2.1(2)      4.0     --
6    2.1(2)      4.0     --

```

```

Mod      Application Image Description      Application Image Version
-----
4        SSI linecard image      4.1 (1b)

```

```

Mod  MAC-Address(es)      Serial-Num
---  -
4    00-05-30-00-9e-b2 to 00-05-30-00-9e-b6  JAB06480590
5    00-0e-38-c6-2c-6c to 00-0e-38-c6-2c-70  JAB082504MQ
6    00-0f-34-94-4d-34 to 00-0f-34-94-4d-38  JAB083407D3

```

* this terminal session

Managing SSMs and Supervisor Modules

This section describes the guidelines for replacing SSMs and supervisor modules and for upgrading and downgrading Cisco MDS NX-OS and SAN-OS releases.

Configuring SSM and MSM Global Upgrade Delay

When there are multiple SSMs or MSMs in the same chassis, you can set the amount of time to delay between upgrading the SSMs or MSMs in a rolling SSI upgrade.

SUMMARY STEPS

1. **configure terminal**
2. **[no] ssm upgrade delay seconds**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	<p>[no] ssm upgrade delay <i>seconds</i></p> <p>Example: switch(config)# ssm upgrade delay 30</p>	<p>Delays the SSI upgrade between SSMs or MSMs by the specified number of seconds. The range is from 1 to 600 seconds. The default is 0 seconds.</p> <p>Use the no form of the command to clear the delay timer.</p>
Step 3	<p>copy running-config startup-config</p> <p>Example: switch(config)# copy running-config startup-config</p>	<p>(Optional) Copies the running configuration to the startup configuration.</p>

Guidelines for Replacing SSMs and Supervisor Modules

If you replace an SSM or supervisor module, consider the following guidelines:

- If you replace an SSM with another SSM and the SSM boot image is on bootflash:, you can leave the boot image installed on the active supervisor module.
- If you replace an SSM with another SSM and the SSI boot image is on the modflash:, the SSM might not initialize.
- If you replace an SSM with any other type of module, you can leave the SSM boot image installed on the active supervisor module or remove it. The active supervisor module detects the module type and boots the module appropriately.
- If you replace a supervisor module in a switch with active and standby supervisor modules, no action is required because the boot image is automatically synchronized to the new supervisor module.
- If you replace a supervisor module in a switch with no standby supervisor module, you need to reimplement the configuration on the new supervisor module.

Recovering an SSM After Replacing Corrupted CompactFlash Memory

As of Cisco MDS NX-OS Release 4.1(1a) and SAN-OS Release 2.1(2), you can use the CompactFlash memory (modflash:) on the SSM to store the SSI image. If the modflash: on the SSM is replaced, the SSM might not initialize.

SUMMARY STEPS

1. Log into the switch through the console port, an SSH session, or a Telnet session.
2. Display the values assigned to the SSI image boot variable for each module and note the values for later reference.
3. Clear the values assigned to the SSI image boot variable.
4. Reload the SSM to initialize in Fibre Channel switching mode.
5. After the SSM initializes, upgrade the SSI boot image.
6. Reassign the SSI boot variables cleared in Step 3.

DETAILED STEPS

Step 1 Log into the switch through the console port, an SSH session, or a Telnet session.

Step 2 Display the values assigned to the SSI image boot variable for each module and note the values for later reference.

```
switch# show boot module
Module 2
ssi variable = modflash://2-1/m9000-ek9-ssi-mz.2.1.2.bin
Module 4
ssi variable = modflash://4-1/m9000-ek9-ssi-mz.2.1.2.bin
```

Step 3 Clear the values assigned to the SSI image boot variable.

```
switch# configure terminal
switch(config)# no boot ssi
```

Step 4 Reload the SSM to initialize in Fibre Channel switching mode.

```
switch# reload module 4
reloading module 4 ...
```

Step 5 After the SSM initializes, upgrade the SSI boot image.

Step 6 Reassign the SSI boot variables cleared in Step 3.

```
switch# configure terminal
switch(config)# boot ssi modflash://2-1/m9000-ek9-ssi-mz.2.1.2.bin module 2
```

Guidelines for Upgrading and Downgrading Cisco MDS NX-OS Releases

Consider the following guidelines when upgrading and downgrading the Cisco MDS NX-OS software on a switch containing an SSM:

- Once you set the SSI image boot variable, you do not need to reset it for upgrades or downgrades to any Cisco MDS NX-OS release that supports boot images. You can use the **install all** command or Fabric Manager GUI to upgrade SSMs once it has been installed.
- If you downgrade to a Cisco MDS NX-OS release that does not support the SSM, you must power down the module. The boot variables for the module are lost.
- The SSM cannot be configured for both the SSI and any other third-party software on the module such as VSFN.

The following example shows successful **install all** command output including an SSI image upgrade.



Note

The SSI boot variable setting is included in the **install all** output. Also, if the SSI boot image is located on bootflash: the **install all** command copies the SSI boot image to the modflash: on the SSMs.

```
Switch# install all system bootflash:isan-2-1-1a kickstart bootflash:boot-2-1-1a
ssi bootflash:ssi-2.1.1a
```

```
Copying image from bootflash:ssi-2.1.1a to modflash://2-1/ssi-2.1.1a.
[#####] 100% -- SUCCESS
```

```
Verifying image bootflash:/ssi-2.1.1a
[#####] 100% -- SUCCESS
```

```
Verifying image bootflash:/boot-2-1-1a
[#####] 100% -- SUCCESS
```

```
Verifying image bootflash:/isan-2-1-1a
[#####] 100% -- SUCCESS
```

```
Extracting "slc" version from image bootflash:/isan-2-1-1a.
[#####] 100% -- SUCCESS
```

```
Extracting "ips4" version from image bootflash:/isan-2-1-1a.
[#####] 100% -- SUCCESS
```

```
Extracting "system" version from image bootflash:/isan-2-1-1a.
[#####] 100% -- SUCCESS
```

```
Extracting "kickstart" version from image bootflash:/boot-2-1-1a.
[#####] 100% -- SUCCESS
```

```
Extracting "loader" version from image bootflash:/boot-2-1-1a.
[#####] 100% -- SUCCESS
```

Compatibility check is done:

```
Module bootable Impact Install-type Reason
-----
2 yes non-disruptive rolling
3 yes disruptive rolling Hitless upgrade is not supported
4 yes disruptive rolling Hitless upgrade is not supported
5 yes non-disruptive reset
```

Images will be upgraded according to following table:

Module	Image	Running-Version	New-Version	Upg-Required
2	slc	2.0(3)	2.1(1a)	yes
2	bios	v1.1.0(10/24/03)	v1.1.0(10/24/03)	no
3	slc	2.0(3)	2.1(1a)	yes
3	SSI	2.0(3)	2.1(1a)	yes
3	bios	v1.0.8(08/07/03)	v1.1.0(10/24/03)	yes
4	ips4	2.0(3)	2.1(1a)	yes
4	bios	v1.1.0(10/24/03)	v1.1.0(10/24/03)	no

```

5      system      2.0(3)          2.1(1a)         yes
5      kickstart   2.0(3)          2.1(1a)         yes
5      bios        v1.1.0(10/24/03) v1.1.0(10/24/03) no
5      loader      1.2(2)          1.2(2)          no

```

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

Install is in progress, please wait.

Module 6:Force downloading.
-- SUCCESS

Syncing image bootflash:/SSI-2.1.1a to standby.
[#####] 100% -- SUCCESS

Syncing image bootflash:/boot-2-1-1a to standby.
[#####] 100% -- SUCCESS

Syncing image bootflash:/isan-2-1-1a to standby.
[#####] 100% -- SUCCESS

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

Module 3:Upgrading Bios/loader/bootrom.
[#####] 100% -- SUCCESS

Module 6:Waiting for module online.
-- SUCCESS

"Switching over onto standby".

Default Settings

This table lists the default settings for the supervisor module.

Table 31: Default Supervisor Module Settings

Parameter	Default
Administrative connection	Serial connection.
Global switch information	<ul style="list-style-type: none"> • No value for system name. • No value for system contact. • No value for location.
System clock	No value for system clock time.
In-band (VSAN 1) interface	IP address, subnet mask, and broadcast address assigned to the VSAN are set to 0.0.0.0.

This table lists the default settings for the SSM.

Table 32: Default Supervisor Module Settings

Parameter	Default
Initial state when installed	<ul style="list-style-type: none">• Power-down state on switches with Cisco MDS SAN-OS Release 2.1(1a) and earlier installed.• Fibre Channel switching mode on switches with Cisco MDS SAN-OS Release 2.1(2) and NX-OS Release 4.1(1b), or later installed and SSMs with EPLD version 2.0(2) and later installed.



INDEX

- More-- prompt [57](#)
 - filtering output [57](#)
 - searching output [57](#)

A

- aliases, See [command aliases](#)
- archive files [109, 110, 111](#)
 - appending files [110](#)
 - creating [109](#)
 - displaying the contents to the screen [111](#)
 - extracting files [111](#)
 - listing archived filenames [111](#)

B

- banners, See [MOTD banners](#)
- BIOS [62](#)
 - loader> prompt [62](#)
- boot variables [127](#)
 - erasing configuration [127](#)

C

- Call Home [2](#)
 - description [2](#)
- CDP [131, 134, 135](#)
 - clearing cache [134](#)
 - clearing counters [135](#)
 - clearing statistics [134](#)
 - clearing tables [135](#)
 - configuring timers, example [135](#)
 - default settings [135](#)
 - description [131](#)
 - optional parameters [134](#)
 - verifying configuration [134](#)
- characters [37](#)
 - special [37](#)

- Cisco Embedded Event Manager., See [EEM](#)
- Cisco MDS 9200 Series interfaces modules [182](#)
 - LED description [182](#)
- Cisco MDS 9200 Series supervisor modules [182](#)
 - LED description [182](#)
- Cisco MDS 9200 Series switching modules [182](#)
 - LED description [182](#)
- CLI [34, 41, 58, 59, 60, 61, 63](#)
 - command history [58](#)
 - command modes [34](#)
 - command name completion [41](#)
 - command prompt [34](#)
 - configuring the edit mode [59](#)
 - disabling confirmation prompts [60](#)
 - enabling confirmation prompts [60](#)
 - examples [63](#)
 - setting display colors [61](#)
- CLI history [59](#)
 - controlling command recall [59](#)
- CLI prompt [34](#)
 - description [34](#)
- CLI variables [43, 44, 63, 64](#)
 - characteristics [43](#)
 - description [43](#)
 - examples [63](#)
 - persistent [44](#)
 - referencing [43](#)
 - session-only [43](#)
 - system-defined variables [64](#)
- clock modules [168](#)
 - description [168](#)
 - displaying information [168](#)
- clocks [85, 92, 95](#)
 - default settings [95](#)
 - description [85](#)
 - setting manually [92](#)
- COM1 port [68](#)
 - settings [68](#)
- COM1 ports [71, 75, 81](#)
 - configuring settings [71](#)
 - default settings [81](#)
 - enabling modem connections [75](#)

- command aliases [45, 46, 47, 63](#)
 - characteristics [45](#)
 - defining [46](#)
 - description [45](#)
 - examples [63](#)
 - user session only [47](#)
 - command history [58, 60](#)
 - description [58](#)
 - displaying [60](#)
 - command modes [34, 35, 36, 37](#)
 - description [34](#)
 - EXEC [34](#)
 - global configuration [34](#)
 - interface [35](#)
 - restoring [36](#)
 - saving [36](#)
 - subinterface [36](#)
 - summary (table) [37](#)
 - command scripts [47, 48, 49, 64](#)
 - delaying command actions [49](#)
 - description [47](#)
 - echoing text to terminals [48](#)
 - examples [64](#)
 - commands [40, 42, 59](#)
 - abbreviations [40](#)
 - no form [42](#)
 - recalling [59](#)
 - commands scripts [47](#)
 - running [47](#)
 - CompactFlash [149, 150, 151, 152, 153, 154, 155, 156](#)
 - Disabling automatic firmware update [150](#)
 - disabling automatic testing [153](#)
 - disabling checksum failure actions [152](#)
 - disabling firmware update failure actions [155](#)
 - displaying CRC test statistics [156](#)
 - displaying firmware update configuration [156](#)
 - displaying firmware update statistics [156](#)
 - Enabling automatic firmware update [150](#)
 - enabling automatic testing [153](#)
 - enabling checksum failure actions [152](#)
 - enabling firmware update failure actions [155](#)
 - running tests [149](#)
 - setting CRC checksum test intervals [151](#)
 - setting firmware update intervals [154](#)
 - updating firmware on demand [153](#)
 - compatibility [1](#)
 - software [1](#)
 - configuration [30, 94, 128](#)
 - displaying [30, 94, 128](#)
 - configuration files [117, 118, 122, 124, 125, 127, 128, 129](#)
 - copying from remote servers [118](#)
 - copying to external memory [122](#)
 - copying to internal file systems [124](#)
 - description [117](#)
 - configuration files (*continued*)
 - erasing [127](#)
 - example backup [129](#)
 - example copy [128](#)
 - example roll back [129](#)
 - rolling back to previous configurations [125](#)
 - types [117](#)
 - configuration prompts [60](#)
 - disabling [60](#)
 - enabling [60](#)
 - configuring devices [24, 25, 26, 27, 28, 29, 30](#)
 - POAP process [25, 26, 27, 28, 29](#)
 - DHCP phase [27](#)
 - post-installation reload phase [29](#)
 - power up phase [26](#)
 - script execution phase [28](#)
 - using POAP [24, 30](#)
 - console ports [68, 69, 75, 81](#)
 - configuring settings [69](#)
 - default settings [81](#)
 - enabling modem connections [75](#)
 - settings [68](#)
 - context-sensitive help [49](#)
 - syntax checking [49](#)
 - crossbar management [162, 163, 164](#)
 - backward compatibility for Generation 1 modules [164](#)
 - description [162](#)
 - graceful shutdown [164](#)
 - removing [163](#)
- ## D
- daylight savings time, See [summer time](#)
 - default gateway [84](#)
 - description [84](#)
 - default settings [81, 95, 115, 135, 146, 170](#)
 - CDP [135](#)
 - clocks [95](#)
 - COM1 ports [81](#)
 - console ports [81](#)
 - file systems [115](#)
 - modems [81](#)
 - MOTD banners [95](#)
 - NTP [146](#)
 - system hardware [170](#)
 - Telnet servers [95](#)
 - terminals [81](#)
 - virtual terminals [81](#)
 - diagnostics., See [online diagnostics](#)
 - diff utility [54](#)
 - description [54](#)

- directories [99, 100, 101, 102](#)
 - changing current directories [100](#)
 - creating [101](#)
 - description [99](#)
 - displaying contents [102](#)
 - displaying current directory [100](#)
 - working with [100](#)
 - downgrading [204](#)
 - guidelines [204](#)
- ## E
- EDLD images [188](#)
 - downgrading [188](#)
 - EEM [2](#)
 - description [2](#)
 - egrep utility [55](#)
 - filtering show command output [55](#)
 - searching show command output [55](#)
 - EPLD images [188, 192](#)
 - description [188](#)
 - displaying versions [192](#)
 - upgrading [188](#)
 - examples [112, 113, 114, 115, 128, 129](#)
 - accessing directories on standby supervisor modules [112](#)
 - backing up configuration files [129](#)
 - compressing files [114](#)
 - copying configuration files [128](#)
 - copying files [112](#)
 - displaying file checksums [114](#)
 - displaying file contents [113](#)
 - finding files [115](#)
 - moving files [112](#)
 - redirecting show command output [114](#)
 - rolling back to a previous configuration [129](#)
 - uncompressing files [114](#)
 - EXEC command mode [34](#)
 - description [34](#)
- ## F
- fan modules [166](#)
 - description [166](#)
 - file systems [97, 100, 103, 115](#)
 - accessing standby supervisor modules [103](#)
 - changing current directories [100](#)
 - default settings [115](#)
 - description [97](#)
 - specifying [97](#)
 - files [99, 103, 104, 105, 106, 107, 108, 109, 112, 113, 114, 115](#)
 - compressing [106](#)
- files (*continued*)
 - compressing, examples [114](#)
 - copying [104](#)
 - copying, examples [112](#)
 - deleting [105](#)
 - description [99](#)
 - displaying checksums [106](#)
 - displaying contents [105](#)
 - displaying files checksums, examples [114](#)
 - displaying files contents, examples [113](#)
 - displaying last lines [107](#)
 - finding [108](#)
 - finding, example [115](#)
 - moving [103](#)
 - moving, examples [112](#)
 - redirecting command output [107](#)
 - renaming [103](#)
 - tar files [109](#)
 - uncompressing [106](#)
 - uncompressing, examples [114](#)
 - files systems [100](#)
 - displaying current directory [100](#)
 - filtering [52, 53, 54, 55, 56, 57](#)
 - More-- prompt [57](#)
 - diff utility [54](#)
 - egrep utility [55](#)
 - grep utility [55](#)
 - keywords [53](#)
 - less utility [56](#)
 - sed utility [56](#)
 - show command output [52](#)
 - Flash devices [99](#)
 - formatting [99](#)
- ## G
- global configuration command mode [34](#)
 - description [34](#)
 - global configuration mode [37](#)
 - summary [37](#)
 - grep utility [55](#)
 - searching show command output [55](#)
 - grep utility filtering show command output [55](#)
 - guidelines and limitations [29](#)
 - POAP [29](#)
- ## H
- hardware [147](#)
 - displaying inventory [147](#)

- high availability [132, 139](#)
 - CDP [132](#)
 - NTP [132, 139](#)
 - hostname [83, 85](#)
 - configuring [85](#)
 - description [83](#)
- I**
- install all command [200](#)
 - SSI boot images [200](#)
 - Interface configuration command mode [35](#)
 - description [35](#)
 - interface configuration mode [37](#)
 - summary [37](#)
- K**
- keystrokes [38](#)
 - shortcuts [38](#)
- L**
- LEDs [182](#)
 - descriptions [182](#)
 - less utility [56](#)
 - filtering show command output [56](#)
 - searching show command output [56](#)
 - licensing [5](#)
 - support [5](#)
 - loader> prompt [62](#)
 - description [62](#)
- M**
- manageability [2](#)
 - description [2](#)
 - management [15](#)
 - configuring in-band management [15](#)
 - management interface [86](#)
 - configuring [86](#)
 - message-of-the-day banners, See [MOTD banners](#)
 - modems [69, 75, 77, 78, 79, 81](#)
 - configuring connections [75](#)
 - configuring user-specific initialization strings [78](#)
 - default settings [81](#)
 - downloading initialization string [77](#)
 - enabling connections [75](#)
 - initializing connection [79](#)
 - modems (*continued*)
 - settings [69](#)
 - modes, See [command modes](#)
 - module temperature monitoring [165](#)
 - description [165](#)
 - modules [61, 126, 165, 171, 172, 174, 175, 176, 177, 178, 180, 181](#)
 - checking states [176](#)
 - connecting to with CLI [177](#)
 - description [171](#)
 - monitoring temperatures [165](#)
 - power cycling [178](#)
 - purging configurations [181](#)
 - reloading [178](#)
 - removing configuration after removal [126](#)
 - saving configurations [180](#)
 - sending commands from the supervisor module session [61](#)
 - services modules [174](#)
 - supervisor modules [172](#)
 - switching modules [174](#)
 - verifying status [175](#)
 - MOTD banner [88](#)
 - configuring [88](#)
 - MOTD banners [84, 95](#)
 - default settings [95](#)
 - description [84](#)
 - MSMs [202](#)
 - configuring global delay timers [202](#)
- N**
- NTP [4, 132, 137, 139, 140, 141, 145, 146](#)
 - configuring server [140](#)
 - clearing a session [145](#)
 - clearing statistics [141, 145](#)
 - configuration distribution [139](#)
 - configuring a server, example [145](#)
 - configuring peer [140](#)
 - default settings [146](#)
 - description [4, 137](#)
 - displaying statistics [141](#)
 - guidelines [139](#)
 - high availability [132, 139](#)
 - limitations [139](#)
 - prerequisites [139](#)
 - verifying configuration [145](#)
 - NTP configuration distribution [142](#)
 - enabling [142](#)
 - NTP configuration distribution [143, 144, 145](#)
 - committing changes [143](#)
 - discarding changes [144](#)
 - releasing the fabric session lock [145](#)

O

- online diagnostics [2](#)
 - description [2](#)

P

- POAP [24, 25, 27, 29, 30](#)
 - configuration script [24](#)
 - DHCP discovery phase [27](#)
 - guidelines and limitations [29](#)
 - post-installation reload phase [29](#)
 - process [25](#)
 - setting up the network environment [29](#)
 - using to configure a switch [30](#)
- power [157](#)
 - displaying usage information [157](#)
- power cycling [178](#)
 - modules [178](#)
- Power On Auto Provisioning [26](#)
 - power up phase [26](#)
 - provisioning devices [26](#)
 - POAP process [26](#)
 - power up phase [26](#)
- power supple mode [158](#)
 - description [158](#)
- power supply modes [158, 161](#)
 - configuration guidelines [158](#)
 - configuring [161](#)
- PowerOn Auto Provisioning [28](#)
 - See also [POAP](#)
 - script execution phase [28](#)
 - See also [POAP](#)
- privileged EXEC mode [37](#)
 - summary [37](#)
- prompts, See [confirmation prompts](#)
- provisioning devices [24, 25, 27, 28, 29](#)
 - POAP process [25, 27, 28, 29](#)
 - DHCP phase [27](#)
 - post-installation reload phase [29](#)
 - script execution phase [28](#)
 - using POAP [24](#)

Q

- QoS [5](#)
 - description [5](#)
- Quality of Service., See [QoS](#)

R

- RBAC [3](#)
 - description [3](#)
- regular expressions [51, 52](#)
 - anchoring [52](#)
 - filtering CLI output [51](#)
 - multiple-character patterns [51](#)
 - special characters [51](#)
- role-based access control., See [RBAC](#)
- running configuration [30, 94, 128](#)
 - displaying [30, 94, 128](#)
- running configurations [118, 119, 122, 124, 125, 126, 128, 129](#)
 - copying from external memory devices [122](#)
 - copying to internal file systems [124](#)
 - downloading from remote servers [119](#)
 - example backup [129](#)
 - example copy [128](#)
 - example roll back [129](#)
 - removing configuration for missing modules [126](#)
 - rolling back to previous configurations [125](#)
 - saving to startup configurations [118](#)

S

- scripts, See [command scripts](#)
- searching [52, 53, 54, 55, 56, 57](#)
 - More-- prompt [57](#)
 - diff utility [54](#)
 - egrep utility [55](#)
 - grep utility [55](#)
 - keywords [53](#)
 - less utility [56](#)
 - sed utility [56](#)
 - show command output [52](#)
- sed utility [56](#)
 - filtering show command output [56](#)
 - searching show command output [56](#)
- serial number [157](#)
 - displaying [157](#)
- serviceability [1](#)
 - description [1](#)
- services modules [174](#)
 - description [174](#)
- setup utility [7, 9](#)
 - description [7](#)
 - prerequisites [9](#)
- shortcuts [38](#)
 - keystrokes [38](#)
- show command output [114](#)
 - redirecting, example [114](#)
- show commands [52](#)
 - filtering output [52](#)

- show commands (*continued*)
 - searching output [52](#)
 - Simple Network Management Protocol., See [SNMP](#)
 - SNMP [2](#)
 - description [2](#)
 - software compatibility [1](#)
 - description [1](#)
 - sort utility [56](#)
 - description [56](#)
 - SPAN [2](#)
 - description [2](#)
 - special characters [37](#)
 - description [37](#)
 - sscp [53, 57, 65](#)
 - example [65](#)
 - redirecting show command output [53, 57](#)
 - SSI boot images [193, 195, 196, 200](#)
 - description [193](#)
 - downgrading [195](#)
 - installing [193](#)
 - upgrading [195](#)
 - Using install all command [200](#)
 - verifying [196](#)
 - SSMs [202, 203, 206](#)
 - configuring global delay timers [202](#)
 - default settings [206](#)
 - downgrading software, guidelines [202](#)
 - recovering after replacing corrupted Compact Flash [203](#)
 - replacing, guidelines [203](#)
 - replacing, guidelines [202](#)
 - upgrading software, guidelines [202](#)
 - standby supervisor modules [103, 112](#)
 - accessing directories, examples [112](#)
 - accessing file systems [103](#)
 - startup configuration [30, 94, 127, 128](#)
 - displaying [30, 94, 128](#)
 - erasing [127](#)
 - startup configurations [118, 120, 123, 124, 125, 128, 129](#)
 - copying from external memory devices [123](#)
 - copying from running configurations [118](#)
 - copying to internal file systems [124](#)
 - downloading from remote servers [120](#)
 - example backup [129](#)
 - example copy [128](#)
 - example roll back [129](#)
 - rolling back to previous configurations [125](#)
 - streaming secure copy, See [sscp](#)
 - subinterface configuration command mode [36](#)
 - description [36](#)
 - subinterface configuration mode [37](#)
 - summary [37](#)
 - summer time [85, 90](#)
 - configuring [90](#)
 - description [85](#)
 - supervisor modules [172, 202, 203, 206](#)
 - default settings [206](#)
 - description [172](#)
 - downgrading, guidelines [202](#)
 - replacing, guidelines [202, 203](#)
 - upgrading, guidelines [202](#)
 - Switched Port Analyzer., See [SPAN](#)
 - switches [178](#)
 - reloading [178](#)
 - switching module [179](#)
 - reloading [179](#)
 - switching modules [174, 181](#)
 - description [174](#)
 - powering off [181](#)
 - switchname [85](#)
 - See also [hostname](#)
 - configuring [85](#)
 - See also [hostname](#)
 - syntax checking, See [context-sensitive help](#)
 - system hardware [170](#)
 - default settings [170](#)
- ## T
- Telnet servers [85, 93, 95](#)
 - connections [85](#)
 - default settings [95](#)
 - disabling connection [93](#)
 - enabling connection [93](#)
 - terminal sessions [67, 80](#)
 - clearing [80](#)
 - displaying information [80](#)
 - settings [67](#)
 - terminals [81](#)
 - default settings [81](#)
 - time zones [85, 89](#)
 - configuring [89](#)
 - description [85](#)
- ## U
- upgrading [204](#)
 - guidelines [204](#)
 - user sessions [85, 93](#)
 - description [85](#)
 - sending messages [93](#)
 - users [92](#)
 - managing [92](#)
 - users sessions [92](#)
 - displaying information [92](#)

V

variables, See [CLI variables](#)
virtual terminals [69, 73, 74, 81](#)
 configuring [73](#)

virtual terminals (*continued*)
 configuring session limits [74](#)
 default settings [81](#)
 settings [69](#)

