Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide, Release 5.x

First Published: August 17, 2012

Last Modified: August 17, 2012

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-27692-01

© 2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xiii

Audience xiii

Document Conventions xiii

Related Documentation xiv

Obtaining Documentation and Submitting a Service Request xvii

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 19

CHAPTER 3 Understanding the Command-Line Interface 21
Information About the CLI Prompt 22
Command Modes 22
EXEC Command Mode 22
Global Configuration Command Mode 22
Interface Configuration Command Mode 23
Subinterface Configuration Command Mode 23
Saving and Restoring a Command Mode 24
Command Mode Summary 24
Special Characters 25
Keystroke Shortcuts 26
Abbreviating Commands 28
Completing a Partial Command Name 29
Identifying Your Location in the Command Hierarchy 29
Using the no Form of a Command 30
Configuring CLI Variables 31
About CLI Variables 31
Configuring CLI Session-Only Variables 31
Configuring Persistent CLI Variables 32
Command Aliases 33
About Command Aliases 33
Defining Command Aliases 33
Configuring Command Aliases for a User Session 34
Command Scripts 34
Running a Command Script 35
Echoing Information to the Terminal 35
Delaying Command Action 36
Context-Sensitive Help 36
Understanding Regular Expressions 38
Special Characters 38

Multiple-Character Patterns 38
Anchoring 39
Searching and Filtering show Command Output 39
Filtering and Searching Keywords 40
diff Utility 41
grep and egrep Utilities 43
less Utility 43
sed Utility 44
sort Utility 44
Redirecting show Command Output Using sscp 45
Searching and Filtering from the --More-- Prompt 45
Using the Command History 46
Recalling a Command 46
Configuring the CLI Edit Mode 47
Controlling CLI History Recall 47
Displaying the Command History 48
Enabling or Disabling the CLI Confirmation Prompts 48
Setting CLI Display Colors 49
Sending Commands to Modules 49
BIOS Loader Prompt 50
Examples Using the CLI 50
Defining Command Aliases 50
Using CLI Session Variables 51
Using the System-Defined Timestamp Variable 51
Running a Command Script 52
Using the sscp Utility to Redirect show Command Output 52

CHAPTER 4 **Configuring Terminal Settings and Sessions 55**
Information About Terminal Settings and Sessions 55
Terminal Session Settings 55
Console Port 56
COM1 Port 56
Virtual Terminals 57
Modem Support 57
Configuring the Console Port 57

Configuring the COM1 Port 59
Configuring Virtual Terminals 60
Configuring the Inactive Session Timeout 61
Configuring the Session Limit 61
Configuring Modem Connections 62
Enabling a Modem Connection 62
Downloading the Default Initialization String 63
Configuring and Downloading a User-Specified Initialization String 65
Initializing a Modem for a Powered-Up Cisco NX-OS Device 66
Clearing Terminal Sessions 66
Displaying Terminal and Session Information 67
Default Settings for Terminal Display and Session Parameters 67

CHAPTER 5 Basic Device Management 69
Information About Basic Device Management 69
Device Hostname 69
Management Interface 70
Default Gateway 70
Message-of-the-Day Banner 70
Device Clock 71
Time Zone and Summer Time (Daylight Saving Time) 71
User Sessions 71
Telnet Server Connection 71
Changing the Device Hostname 71
Configuring the Management Interface 72
Configuirng the Default Gateway 73
Configuring the MOTD Banner 74
Configuring the Time Zone 75
Configuring Summer Time (Daylight Saving Time) 76
Manually Setting the Device Clock 77
Managing Users 77
Displaying Information about the User Sessions 78
Sending a Message to Users 78
Enabling or Disabling a Telnet Server Connection 78
Verifying the Device Configuration 79

Default Settings for Basic Device Parameters 79

CHAPTER 6 **Using the Device File Systems, Directories, and Files 81**

Information About the Device File Systems, Directories, and Files 81

File Systems 81

Directories 83

Files 83

Formatting External Flash Devices 83

Working with Directories 84

Identifying the Current Directory 84

Changing the Current Directory 84

Creating a Directory 85

Displaying Directory Contents 85

Deleting a Directory 85

Accessing Directories on the Standby Supervisor Module 86

Working with Files 86

Moving Files 86

Copying Files 87

Deleting Files 88

Displaying File Contents 88

Displaying File Checksums 88

Compressing and Uncompressing Files 89

Displaying the Last Lines in a File 89

Redirecting show Command Output to a File 90

Finding Files 90

Working with Archive Files 91

Creating an Archive Files 91

Appending Files to an Archive File 92

Extracting Files from an Archive File 92

Displaying the Filenames in an Archive File 93

Examples of Using the File System 93

Accessing Directories on Standby Supervisor Modules 93

Moving Files 94

Copying Files 94

Deleting a Directory 94

Displaying File Contents 95
Displaying File Checksums 95
Compressing and Uncompressing Files 96
Redirecting show Command Output 96
Finding Files 96
Default Settings for File System Parameters 97

CHAPTER 7 Working with Configuration Files 99
Information About Configuration Files 99
Types of Configuration Files 99
Managing Configuration Files 100
Saving the Running Configuration to the Startup Configuration 100
Copying a Configuration File to a Remote Server 100
Downloading the Running Configuration From a Remote Server 101
Downloading the Startup Configuration From a Remote Server 102
Copying Configuration Files to an External Flash Memory Device 103
Copying the Running Configuration From an External Flash Memory Device 104
Copying the Startup Configuration From an External Flash Memory Device 105
Copying Configuration Files to an Internal File System 106
Rolling Back to a Previous Configuration 106
Removing the Configuration for a Missing Module 107
Erasing a Configuration 108
Verifying the Device Configuration 109
Examples of Working with Configuration Files 109
Copying Configuration Files 109
Backing Up Configuration Files 109
Rolling Back to a Previous Configuration 110

CHAPTER 8 Configuring CDP 111
Information About CDP 111
CDP Overview 111
High Availability for CDP 112
Configuring CDP 112
Enabling or Disabling CDP Globally 112
Enabling or Disabling CDP on an Interface 112

Configuring Optional CDP Parameters 113
Verifying the CDP Configuration 114
Clearing CDP Counters and Tables 115
CDP Example Configuration 115
Default Settings for CDP 115

CHAPTER 9 Configuring NTP 117
Information About NTP 117
NTP 117
NTP Configuration Distribution Using CFS 119
High Availability for NTP 119
Prerequisites for NTP 119
Guidelines and Limitations for NTP 119
Configuring NTP 119
Enabling or Disabling the NTP Protocol 120
Configuring an NTP Server and Peer 120
Displaying and Clearing NTP Statistics 121
Distributing the NTP Configuration Using CFS 121
Enabling NTP Configuration Distribution 121
Committing NTP Configuration Changes 122
Discarding NTP Configuration Changes 123
Releasing Fabric Session Lock on the NTP Configuration 124
Verifying NTP Configuration 124
NTP Example Configuration 125
Default Settings for NTP 125

CHAPTER 10 Managing System Hardware 127
Displaying Switch Hardware Inventory 127
Running CompactFlash Tests 129
Running the CompactFlash CRC Checksum Test On Demand 130
Enabling and Disabling Automatic CompactFlash Firmware Update 130
Setting the CompactFlash CRC Checksum Test Interval 131
Enabling and Disabling Failure Action for a CompactFlash Checksum Test 131
Running the CompactFlash CRC Checksum Test On Demand 132
Updating the CompactFlash Firmware On Demand 132

Enabling and Disabling the Automatic CompactFlash CRC Checksum Test 132
Setting the CompactFlash Firmware Update Interval 133
Enabling and Disabling Failure Action for CompactFlash Firmware Updates 134
Displaying CompactFlash Firmware Update Configuration 135
Displaying CompactFlash CRC Test and Firmware Update Statistics 135
Displaying the Switch Serial Number 136
Displaying Power Usage Information 136
Power Supply Modes 137
Configuration Guidelines for Power Supplies 137
Configuring the Power Supply Mode 140
About Crossbar Management 141
Operational Considerations when Removing Crossbars 142
Gracefully Shutting Down a Crossbar 143
Provideing Backward Compatibility for Generation 1 Modules in Cisco MDS 9513 Directors 143
About Module Temperature Monitoring 144
Displaying Module Temperatures 145
About Fan Modules 145
About Clock Modules 147
Displaying Environment Information 148
Default Settings 149

CHAPTER 11 **Managing Modules 151**
About Modules 151
Supervisor Modules 152
Switching Modules 154
Services Modules 154
Maintaining Supervisor Modules 154
Replacing Supervisor Modules 154
Standby Supervisor Module Boot Variable Version 155
Standby Supervisor Module Bootflash Memory 155
Standby Supervisor Module Boot Alert 155
Verifying the Status of a Module 155
Checking the State of a Module 156
Connecting to a Module 157

Reloading Modules 158
Reloading a Switch 158
Power Cycling Modules 158
Reloading Switching Modules 159
Saving the Module Configuration 159
Purging Module Configurations 160
Powering Off Switching Modules 160
Identifying Module LEDs 161
EPLD Images 168
Upgrading EPLD Images 168
Displaying EPLD Image Versions 172
SSI Boot Images 173
Installing the SSI Boot Image 173
Upgrading or Downgrading the SSI Boot Image 174
SSI Boot Image Upgrade Considerations for the SSM 175
Verifying the SSI Boot Image 176
Using the install ssi Command 179
Managing SSMs and Supervisor Modules 181
Configuring SSM and MSM Global Upgrade Delay 181
Guidelines for Replacing SSMs and Supervisor Modules 181
Recovering an SSM After Replacing Corrupted CompactFlash Memory 182
Guidelines for Upgrading and Downgrading Cisco MDS NX-OS Releases 183
Default Settings 184

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 xvii

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.
Italic	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.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

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

This document uses the following conventions:

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

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

Related Documentation

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/doclocater.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 9500 Series 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*

Cisco Fabric Manager

- *Cisco Fabric Manager Fundamentals Configuration Guide*
- *Cisco Fabric Manager System Management Configuration Guide*
- *Cisco Fabric Manager Interfaces Configuration Guide*
- *Cisco Fabric Manager Fabric Configuration Guide*
- *Cisco Fabric Manager Quality of Service Configuration Guide*
- *Cisco Fabric Manager Security Configuration Guide*
- *Cisco Fabric Manager IP Services Configuration Guide*
- *Cisco Fabric Manager Intelligent Storage Services Configuration Guide*
- *Cisco Fabric Manager High Availability and Redundancy Configuration Guide*
- *Cisco Fabric Manager Inter-VSAN Routing Configuration Guide*
- *Cisco Fabric Manager Online Help*
- *Cisco Fabric Manager Web Services Online Help*

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, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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.

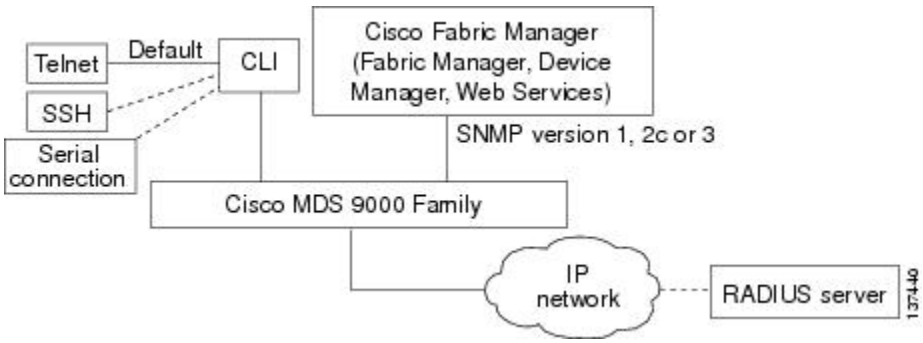
Tools for Software Configuration

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.

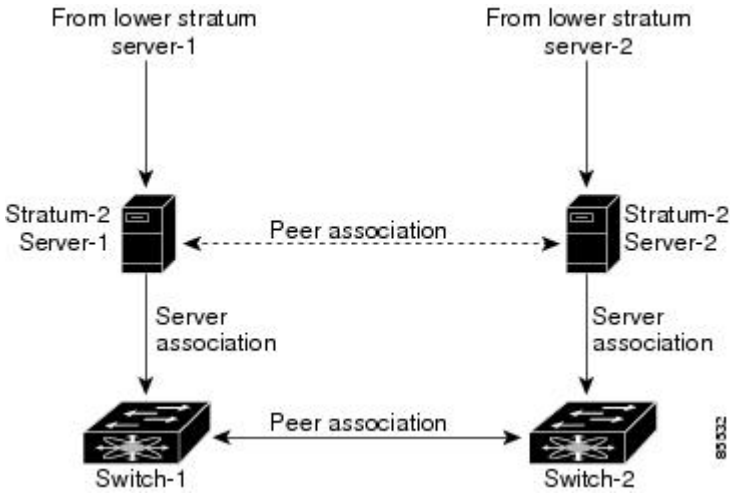
By configuring an IP address as a peer, the Cisco NX-OS device will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both of these instances point to different time servers, your NTP service is more reliable. Even if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

CHAPTER 2

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 19

Information About the Cisco NX-OS Setup Utility

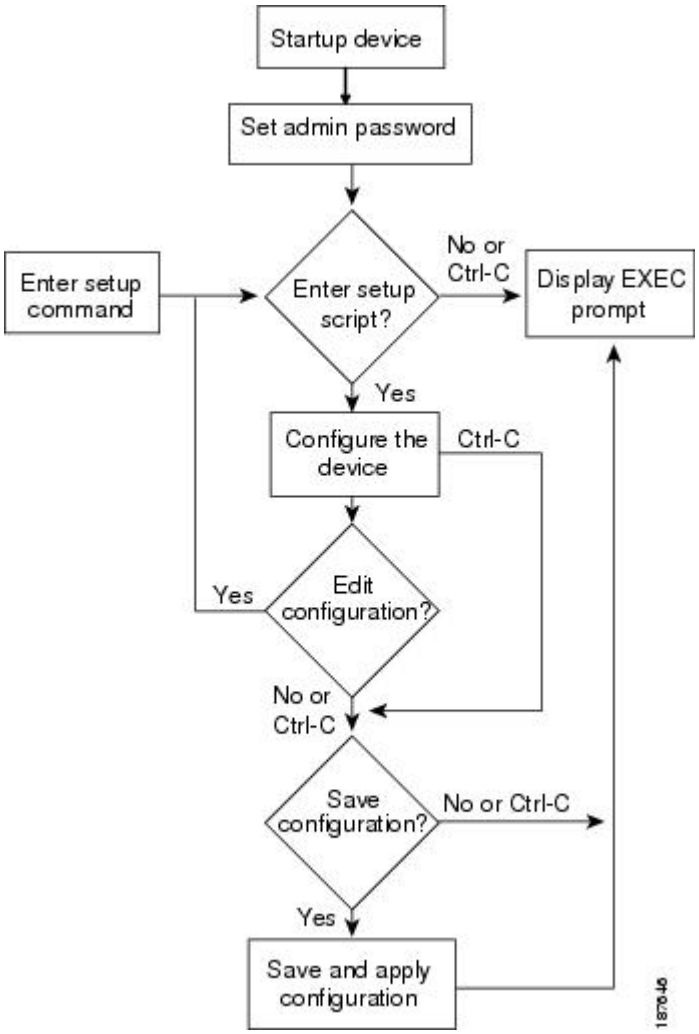
The Cisco NX-OS setup utility is an interactive command-line interface (CLI) mode that guides you through a basic (also called a startup) configuration of the system. The setup utility allows you to configure only enough connectivity for system management.

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.

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.

Procedure

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*lkjh18
```

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 .

CHAPTER 3

Understanding the Command-Line Interface

This chapter contains the following sections:

- Information About the CLI Prompt, page 22
- Command Modes, page 22
- Special Characters, page 25
- Keystroke Shortcuts, page 26
- Abbreviating Commands, page 28
- Completing a Partial Command Name, page 29
- Identifying Your Location in the Command Hierarchy, page 29
- Using the no Form of a Command , page 30
- Configuring CLI Variables, page 31
- Command Aliases, page 33
- Command Scripts, page 34
- Context-Sensitive Help , page 36
- Understanding Regular Expressions, page 38
- Searching and Filtering show Command Output, page 39
- Searching and Filtering from the --More-- Prompt, page 45
- Using the Command History, page 46
- Enabling or Disabling the CLI Confirmation Prompts, page 48
- Setting CLI Display Colors, page 49
- Sending Commands to Modules, page 49
- BIOS Loader Prompt, page 50
- Examples Using the CLI , page 50

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.

Procedure

	Command or Action	Purpose

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

Interface Configuration Command Mode

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

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

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

Procedure

	Command or Action	Purpose

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

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

Subinterface Configuration Command Mode

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

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

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

Procedure

	Command or Action	Purpose

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

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

Saving and Restoring a Command Mode

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

The following example shows how to save and restore a command mode:

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

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
#	Pound, hash, or number
...	Ellipsis
|	Vertical bar
< >	Less than or greater than
[ ]	Brackets

Character	Description
{ }	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.
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.

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

Keystokes	Description

Tab	Completes the word for you after entering the first characters of the word, and then pressing the Tab key. All options that match are presented.
	Use tabs to complete the following items:
	• Command names
	• Scheme names in the file system
	• Server names in the file system
	• Filenames in the file system
	Example:
	`switch(config)# xm<Tab>`
	`switch(config)# xml<Tab>`
	`switch(config)# xml server`

	Example:
	`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`

	Example:
	`switch# cd bootflash:<Tab>`
	`bootflash:  bootflash://sup-1/`
	`bootflash:///  bootflash://sup-2/`
	`bootflash://module-5/`
	`bootflash://sup-active/`
	`bootflash://module-6/  bootflash://sup-local/`

	Example:
	`switch# cd bootflash://mo<Tab>`
	`bootflash://module-5/`
	`bootflash://module-6/cv`
	`switch# cd bootflash://module-`

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, 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 allows you to modify the command if the full command was not what you intended by the abbreviation. If you enter a set of characters that could indicate more than one command, a list of matching commands displays.

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

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

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

Identifying Your Location in the Command Hierarchy

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

Procedure

	Command or Action	Purpose

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

Using the no Form of a Command

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

This example shows how to disable a feature:

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

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

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

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

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

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

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

switch(config)# no radius-server host 10.10.2.2
switch(config)# show radius-server
retransmission count:0
```

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

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

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

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

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

Configuring CLI Variables

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

About CLI Variables

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

You can refer to CLI variables in the following ways:

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

CLI variables have the following characteristics:

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

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

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

Configuring CLI Session-Only Variables

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

Procedure

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

Configuring Persistent CLI Variables

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

Procedure

	Command or Action	Purpose

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

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

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

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

Command Aliases

This section provides information about command aliases.

About Command Aliases

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

Command alias support has the following characteristics:

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

Defining Command Aliases

You can define command aliases for commonly used commands.

Procedure

	Command or Action	Purpose

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

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

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

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

Procedure

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

Command Scripts

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

Running a Command Script

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

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

Procedure

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

Echoing Information to the Terminal

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

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

Table 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.

Formatting Option	Description
nnn	Displays the corresponding ASCII octal character.

Procedure

	Command or Action	Purpose

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

Delaying Command Action

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

Procedure

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

Context-Sensitive Help

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

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

This table shows example outputs of context sensitive help.

Table 6: Context-Sensitive Help Example

Example Outputs	Description

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

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

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

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

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

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

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

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

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

Understanding Regular Expressions

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

Special Characters

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

This table lists the keyboard characters that have special meanings.

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

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

diff Utility

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

Caution Do not use the diff utility for **show** commands that have very long output, such as the **show tech-support** command.

The diff utility syntax is as follows:

diff [**--left-column**] [**-B**] [**-I**] [**-W** *columns*] [**-b**] [**-c** *lines*] [**-I**] [**-q**] [**-s**] [**-y**] [**again**] [**echo**]

This table describes the keywords for the diff utility.

Table 10: diff Utility Keywords

Keyword	Description
--left-column	Prints only the left column of the two common lines in side-by-side format.
-B	Ignores the changes that only insert or delete blank lines.
-I	Ignores the changes that only insert or delete lines that match the regular expression.
-W *columns*	Specifies the output column width for the side-by-side format. The range is from 0 to 4294967295.
-b	Ignores the changes in the amount of white space. The default is to display the white space differences.
-c *lines*	Sets the number of lines of context displayed. The default number of lines is 3. The range is from 0 to 4294967295.
-I	Ignores uppercase and lowercase differences. The default is to report the uppercase and lowercase differences.
-q	Indicates whether the files differ but does not display the details of the differences. The default is to display the differences.
-s	Indicates whether the two outputs are the same. The default is no indication when the outputs are the same.
-y	Uses the side-by-side format for the output differences. The default is to display the old output lines first, followed by the current output lines.
again	Does not create new output file: use old ones, just change display options or add more filters.
echo	Echoes the current command output. This keyword is only effective when there is no previous command output.

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

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

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

grep and egrep Utilities

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

The grep and egrep syntax is as follows:

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

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

Table 11: grep and egrep Parameters

Parameter	Description
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.
expression	Specifies a regular expression for searching the output.

less Utility

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

sed Utility

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

sed *command*

The *command* argument contains sed utility commands.

sort Utility

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

The sort utility syntax is as follows:

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

Table 12: 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 *field-number*[**.***char-position*][*ordering*]	Sorts according to a key value. There is no default key value.
-n	Sorts according to a numeric string value.
-r	Reverses order of the sort results. The default sort output is in ascending order.
-t *delimiter*	Sorts using a specified delimiter. The default delimiter is the space character.
-u	Removes duplicate lines from the sort results. The sort output displays the duplicate lines.

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 13: --More-- Prompt Commands

Commands	Description
[*lines*]<space>	Displays output lines for either the specified number of lines or the current screen size.
[*lines*]**z**	Displays output lines for either the specified number of lines or the current screen size. If you use the *lines* argument, that value becomes the new default screen size.
[*lines*]<return>	Displays output lines for either the specified number of lines or the current default number of lines. The initial default is 1 line. If you use the optional *lines* argument, that value becomes the new default number of lines to display for this command.

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

Using the Command History

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

Recalling a Command

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

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

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

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

Configuring the CLI Edit Mode

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

Procedure

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

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.

Procedure

	Command or Action	Purpose
Step 1	[**no**] **terminal history no-exec-in-config** **Example:** `switch# terminal history no-exec-in-config`	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.

Procedure

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

Setting CLI Display Colors

You can change the CLI colors to display as follows:

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

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

Procedure

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

Sending Commands to Modules

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

The **slot** has the following syntax:

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

By default, the keyword and arguments in the *command-string* argument are space-separated. 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 only supported on the supervisor module session.

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

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

The following 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 th `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 4

Configuring Terminal Settings and Sessions

This chapter contains the following sections:

- Information About Terminal Settings and Sessions, page 55
- Configuring the Console Port, page 57
- Configuring the COM1 Port, page 59
- Configuring Virtual Terminals , page 60
- Configuring Modem Connections, page 62
- Clearing Terminal Sessions, page 66
- Displaying Terminal and Session Information, page 67
- Default Settings for Terminal Display and Session Parameters, page 67

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.

Procedure

	Command or Action	Purpose

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

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

Step 3	**databits** *bits* **Example:** `switch(config-console)# databits 7`	Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.
Step 4	**exec-timeout** *minutes* **Example:** `switch(config-console)# exec-timeout 30`	Configures the timeout for an inactive session. The range is from 0 to 525600 minutes (8760 hours). A value of 0 minutes disables the session timeout. The default is 30 minutes.
Step 5	**parity** {**even** | **none** | **odd**} **Example:** `switch(config-console)# parity even`	Configures the parity. The default is **none**.
Step 6	**speed** {**300** | **1200** | **2400** | **4800** | **9600** | **38400** | **57600** | **115200**} **Example:** `switch(config-console)# speed 115200`	Configures the transmit and receive speed. The default is **115200**.
Step 7	**stopbits** {**1** | **2**} **Example:** `switch(config-console)# stopbits 2`	Configures the stop bits. The default is **1**.

	Command or Action	Purpose

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.

Procedure

	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.

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

Procedure

	Command or Action	Purpose

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

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

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

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

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

Configuring the Session Limit

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

Procedure

	Command or Action	Purpose

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

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

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

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

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

Configuring Modem Connections

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

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

Enabling a Modem Connection

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

Before You Begin

Log in to the console port.

Procedure

	Command or Action	Purpose

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

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

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

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

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

Downloading the Default Initialization String

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

Before You Begin

Log in to the console port.

Procedure

	Command or Action	Purpose

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

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

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

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

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.

Procedure

	Command or Action	Purpose

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

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

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

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

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

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

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

Before You Begin

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

Enable the modem connection on the port.

Procedure

	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 62

Clearing Terminal Sessions

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

Procedure

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

Displaying Terminal and Session Information

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

Command	Purpose
show terminal	Displays terminal settings.
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 14: 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

Parameters	Default
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
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 5

Basic Device Management

This chapter contains the following sections:

- Information About Basic Device Management, page 69
- Changing the Device Hostname, page 71
- Configuring the Management Interface, page 72
- Configuirng the Default Gateway, page 73
- Configuring the MOTD Banner, page 74
- Configuring the Time Zone, page 75
- Configuring Summer Time (Daylight Saving Time), page 76
- Manually Setting the Device Clock, page 77
- Managing Users, page 77
- Enabling or Disabling a Telnet Server Connection, page 78
- Verifying the Device Configuration, page 79
- Default Settings for Basic Device Parameters, page 79

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.

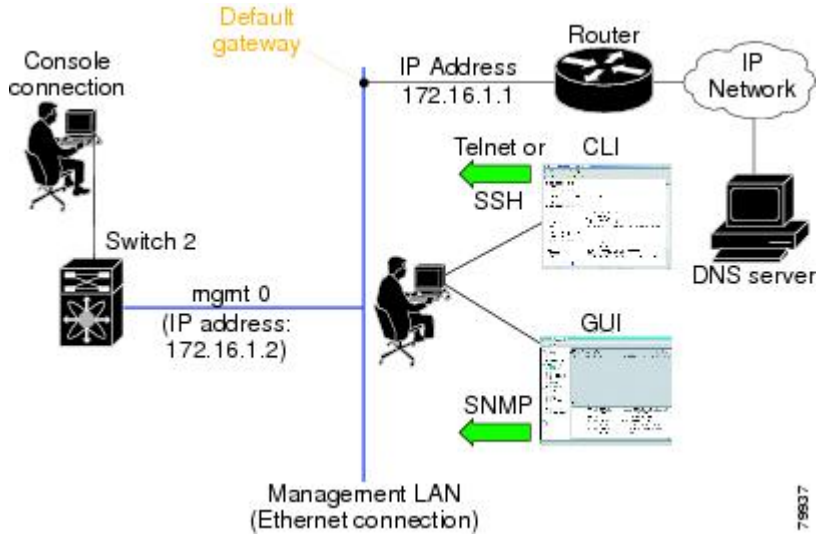
On devices with dual supervisor modules, a single IP address is used to manage the switch. The active supervisor module's mgmt0 interface uses this IP address. The mgmt0 interface on the standby supervisor module remains in an inactive state and cannot be accessed until a switchover happens. After a 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 4: 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.

Procedure

	Command or Action	Purpose

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

Step 2	{**hostname** | **switchname**} *name*
	
	Example:
	Using the **hostname** command:
	`switch(config)# hostname Engineering1`
	`Engineering1(config)#`
	Using the **switchname** command:
	`Engineering1(config)# switchname Engineering2`
	`Engineering2(config)#`
		Changes the device hostname. The *name* 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:
	`Engineering2(config)# exit`
	`Engineering2#`
		Exits global configuration mode.

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

Configuring the 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.

Procedure

	Command or Action	Purpose

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

Step 2	**interface mgmt 0**
	
	Example:
	`switch(config)# interface mgmt 0`
	`switch(config-if)#`
		Specifies the mgmt0 inteface and enters the interface configuration mode.

Step 3	**ip address** {*ipv4-address subnet-mask* | *ipv6-address*} **Example:** `switch(config-if)# ip address 1.1.1.0 255.255.255.0`	Configures the IPv4 or IPv6 address on the mgmt 0 interface.

Step 4	**exit**
	
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Returns to global configuration mode.

Step 5	**show interface mgmt 0** **Example:** `switch(config)# show interface mgmt 0`	(Optional) Dispalys the mgmt 0 interface information.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuirng 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.

Procedure

	Command or Action	Purpose

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

Step 2	**ip default gateway** *ipv4-address* **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 gataeway 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

Procedure

	Command or Action	Purpose

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

Step 2	**banner motd** *delimiting-character message delimiting-character*	Configures the MOTD banner. Do not use the *delimiting-character* in the *message* text.

	Command or Action	Purpose

	Example:
	`switch(config)# banner motd #Welcome to the Switch#`
	`switch(config)#`
		Note Do not use " or % as a delimiting character.

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

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

Configuring the Time Zone

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

Procedure

	Command or Action	Purpose

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

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

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

	Command or Action	Purpose
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.

Procedure

	Command or Action	Purpose

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

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

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

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

Manually Setting the Device Clock

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

Before You Begin

Configure the time zone.

Procedure

	Command or Action	Purpose

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

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

Related Topics

Configuring the Time Zone, on page 75

Managing Users

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

Displaying Information about the User Sessions

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

Procedure

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

Sending a Message to Users

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

Procedure

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

Enabling or Disabling a Telnet Server Connection

You can enable or disable the Telnet server connection.

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
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 starutup 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 15: Default Basic Device Parameters

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

CHAPTER 6

Using the Device File Systems, Directories, and Files

This chapter contains the following sections:

- Information About the Device File Systems, Directories, and Files, page 81
- Formatting External Flash Devices, page 83
- Working with Directories, page 84
- Working with Files, page 86
- Working with Archive Files, page 91
- Examples of Using the File System, page 93
- Default Settings for File System Parameters, page 97

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 16: 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.
nvram	—	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.

Procedure

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

	Command or Action	Purpose
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.

Procedure

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

Changing the Current Directory

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

Procedure

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

Creating a Directory

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

Procedure

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

Displaying Directory Contents

You can display the contents of a directory.

Procedure

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

Deleting a Directory

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

Before You Begin

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

Procedure

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

Accessing Directories on the Standby Supervisor Module

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

Working with Files

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

Moving Files

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

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

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

Procedure

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

Copying Files

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

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

Procedure

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

	Command or Action	Purpose
	Example: `switch# move test old_tests/test1`	specified, the filename defaults to the *source-filename* argument value.

Deleting Files

You can delete a file from a directory.

Procedure

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

Displaying File Contents

You can display the contents of a file.

Procedure

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

Displaying File Checksums

You can display checksums to check the file integrity.

Procedure

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

Compressing and Uncompressing Files

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

Procedure

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

Displaying the Last Lines in a File

You can display the last lines of a file.

Procedure

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

Redirecting show Command Output to a File

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

Procedure

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

Finding Files

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

Procedure

	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	**cd** {*filesystem*:[//*module*/][*directory*] | *directory*} **Example:** `switch# cd bootflash:test_scripts`	(Optional) Changes the default directory.
Step 3	**find** *filename-prefix* **Example:** `switch# find bgp_script`	Finds all filenames in the default directory and in its subdirectories beginning with the filename prefix. The filename prefix is case sensitive.

Working with Archive Files

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

Creating an Archive Files

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

- bzip2
- gzip
- Uncompressed

The default is gzip.

Procedure

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

	Command or Action	Purpose
		• For **uncompressed**, the extension is .tar. The **remove** keyword specifies that the Cisco NX-OS software should delete the files from the filesystem after adding them to the archive. By default, the files are not deleted. The **verbose** keyword specifies that the Cisco NX-OS software should list the files as they are added to the archive. By default, the files are listed as they are added.

This example shows how to 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.

Procedure

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

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

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

Extracting Files from an Archive File

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

Before You Begin

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

Procedure

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

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

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

Displaying the Filenames in an Archive File

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

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

The archive filename is not case sensitive.

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

Examples of Using the File System

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

Accessing Directories on Standby Supervisor Modules

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

```
switch# dir bootflash://sup-remote
   12198912     Aug 27 16:29:18 2003  m9500-sf1ek9-kickstart-mzg.1.3.0.39a.bin
```

```
    1864931     Apr 29 12:41:59 2003  dplug2
      12288     Apr 18 20:23:11 2003  lost+found/
   12097024     Nov 21 16:34:18 2003  m9500-sf1ek9-kickstart-mz.1.3.1.1.bin
   41574014     Nov 21 16:34:47 2003  m9500-sf1ek9-mz.1.3.1.1.bin

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

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

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

Moving Files

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

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

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

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

Copying Files

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

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

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

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

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

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

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.

Procedure

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

Displaying File Contents

This example displays 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 displays the contents of a file residing 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 directs the output of the **show tech-support** command to a file:

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

Finding Files

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

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

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

Default Settings for File System Parameters

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

Table 17: Default File System Settings

Parameters	Default
Default filesystem	bootflash:

CHAPTER 7

Working with Configuration Files

This chapter contains the following sections:

- Information About Configuration Files, page 99
- Managing Configuration Files, page 100
- Verifying the Device Configuration, page 109
- Examples of Working with Configuration Files, page 109

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 may 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 100
Downloading the Startup Configuration From a Remote Server, on page 102

Managing Configuration Files

This section describes how to manage configuration files.

Saving the Running Configuration to the Startup Configuration

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

Procedure

	Command or Action	Purpose
Step 1	**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.

Procedure

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

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

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.

Procedure

	Command or Action	Purpose
Step 1	**copy** *scheme*:*//server/*[*url/*]*filename* **running-config** **Example:** `switch# copy tftp://10.10.1.1/my-config running-config`	Downloads the running-configuration file from a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.
Step 2	**show running-config** **Example:** `switch# show running-config`	(Optional) Displays the running configuration.

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

Related Topics

Copying Files, on page 94

Downloading the Startup Configuration From a Remote Server

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

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

Before You Begin

Log in to a session on the console port.

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

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

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

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

Procedure

	Command or Action	Purpose
Step 1	**write erase** **Example:** `switch# write erase`	Erases the startup configuration file.
Step 2	**reload**	Reloads the Cisco NX-OS device.

	Command or Action	Purpose

	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#`
		Note Do not use the setup utility to configure the device.

Step 3	**copy** *scheme*:*//server/*[*url /*]*filename* **running-config**
	
	Example:
	`switch# copy tftp://10.10.1.1/my-config`
	
	`running-config`
		Downloads the running configuration file from a remote server.
		
		For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server.
		
		The *server*, *url*, and *filename* arguments are case sensitive.

Step 4	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Saves the running configuration file to the startup configuration file.
Step 5	**show startup-config** **Example:** `switch# show startup-config`	(Optional) Displays the running configuration.

Related Topics

Copying Files, on page 94

Copying Configuration Files to an External Flash Memory Device

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

Before You Begin

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

Procedure

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

Related Topics

Copying Files, on page 94

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.

Procedure

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

	Command or Action	Purpose
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 94

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.

Procedure

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

Related Topics

Copying Files, on page 94

Copying Configuration Files to an Internal File System

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

Procedure

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

Related Topics

Copying Files, on page 94

Rolling Back to a Previous Configuration

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

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

Procedure

	Command or Action	Purpose
Step 1	**write erase** **Example:** `switch# write erase`	Clears the current configuration of the switch.
Step 2	**reload** **Example:** `switch# reload`	Restarts the device. You will be prompted to provide a kickstart and system image file for the device to boot and run.
Step 3	**copy** *configuration_file* **running-configuration** **Example:** `switch# copy bootflash:start-config.bak running-configuration`	Copies a previously saved configuration file to the running configuration. **Note** The *configuration_file* filename argument is case-sensitive.
Step 4	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the start-up configuration.

Removing the Configuration for a Missing Module

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

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

Before You Begin

Remove the I/O module from the chassis.

Procedure

	Command or Action	Purpose
Step 1	**show hardware** **Example:** `switch# show hardware`	(Optional) Displays the installed hardware for the device.

	Command or Action	Purpose
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.

Procedure

	Command or Action	Purpose

Step 1	**write erase** [**boot** | **debug**]
	
	Example:
	`switch# write erase`
	`Warning: This command will erase the startup-configuration.`
		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.

	Command or Action	Purpose
	`Do you wish to proceed anyway? (y/n) [n] y`	**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.
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.

CHAPTER 8

Configuring CDP

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

- Information About CDP, page 111
- Configuring CDP, page 112
- Verifying the CDP Configuration, page 114
- Clearing CDP Counters and Tables, page 115
- CDP Example Configuration, page 115
- Default Settings for CDP, page 115

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 reenable 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.

Procedure

	Command or Action	Purpose

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

Step 2	**cdp enable** **Example:** `switch(config)# cdp enable`	Enables the CDP feature on the entire device. This is enabled by default .
Step 3	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(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.

Procedure

	Command or Action	Purpose

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

Step 2	**interface** *interface-type slot/port*
	
	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** *interface-type slot/port* **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:`
`switch(config)# cdp advertise v1`
	Sets the CDP version supported by the device. The default is v2.

Command	Purpose
cdp format device-id {**mac-address** | **serial-number** | **system-name**} Example: `switch(config)# cdp format device-id mac-address`	Sets the CDP device ID. The options are as follows: • **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: `switch(config)# cdp holdtime 150`	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: `switch(config)# cdp timer 50`	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 18: 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

CHAPTER 9

Configuring NTP

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

- Information About NTP, page 117
- Prerequisites for NTP , page 119
- Guidelines and Limitations for NTP, page 119
- Configuring NTP, page 119
- Verifying NTP Configuration, page 124
- NTP Example Configuration , page 125
- Default Settings for NTP, page 125

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.

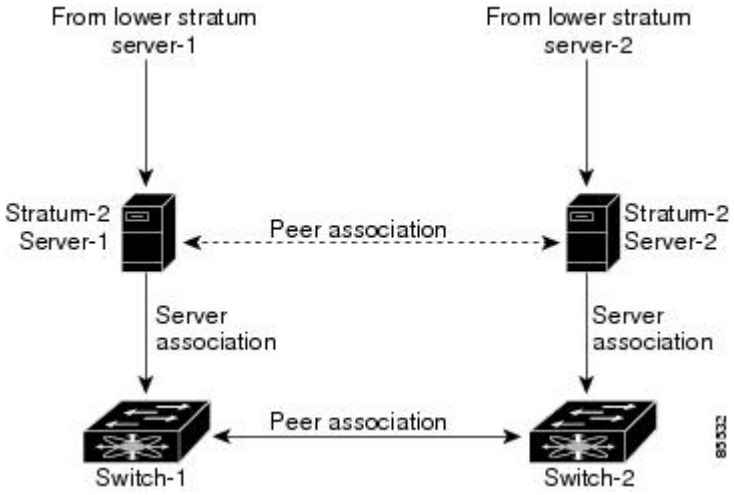
By configuring an IP address as a peer, the Cisco NX-OS device will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both of these instances point to different time servers, your NTP service is more reliable. Even if 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 5: 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 reenable it.

Procedure

	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.

Procedure

	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.

	Command or Action	Purpose
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.

Procedure

	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: • **peer**—NTP statistics for per peer. • **io**—NTP statistics for I/O devices. • **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.

Procedure

	Command or Action	Purpose

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

Step 2	**ntp distribute** **Example:** `swtich(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.
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.

Procedure

	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.
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.

Procedure

	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.

	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.

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 19: Default NTP Settings

NTP	Disabled

CHAPTER 10

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 127
- Running CompactFlash Tests, page 129
- Running the CompactFlash CRC Checksum Test On Demand, page 132
- Displaying CompactFlash CRC Test and Firmware Update Statistics, page 135
- Displaying the Switch Serial Number, page 136
- Displaying Power Usage Information, page 136
- Power Supply Modes, page 137
- About Crossbar Management, page 141
- About Module Temperature Monitoring, page 144
- About Fan Modules, page 145
- About Clock Modules, page 147
- Displaying Environment Information, page 148
- Default Settings, page 149

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 reenable the automatic update at a later time.

Procedure

	Command or Action	Purpose

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

Step 2	[**no**]**system health module** *slot-number* **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.
Step 3	**show system health module** *slot-number* **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.

Procedure

	Command or Action	Purpose

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

Step 2	**system health module** *slot-number* **cf-crc-check frequency** *seconds* **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** *slot-number* **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.

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.

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
Step 2	[**no**]**system health module** *slot-number* **cf-crc-check faliure-action** **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 the failure action. The default is enabled.
Step 3	**show system health module** *slot-number* **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.

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.

Procedure

	Command or Action	Purpose

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

Step 2	**system health module** *slot-number* **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 defauilt is enabled.
Step 3	**show system health module** *slot-number* **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.

Procedure

	Command or Action	Purpose

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

Step 2	**system health module** *slot-number* **cf-re-flash frequency** *days* **Example:** `switch(config)# system health module 2 cf-re-flash frequency 45`	Sets the automatic CompactFlash firware update interval. The range is from 30 to 255. The default is every 30 days.

	Command or Action	Purpose
Step 3	**show system health module** *slot-number* **Example:** `switch(config)# show system health module 2`	(Optional) Displays the automatic CompactFlash firmware update interface configuration 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.

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.

Procedure

	Command or Action	Purpose

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

Step 2	[**no**]**system health module** *slot-number* **cf-re-flash failure-action** **Example:** `switch(config)# system health module 2 cf-re-flash`	Enables the automatic CompactFlash firware 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** *slot-number* **Example:** `switch(config)# show system health module 2`	(Optional) Displays the automatic CompactFlash firmware update failure action 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.

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            Freqency   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            Freqency   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            Freqency   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            Freqency   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            Freqency   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     Power       Power     Power       Status
                         Requested Requested   Allocated Allocated
                         (Watts)   (Amp @42V)  (Watts)   (Amp @42V)
--- -------------------  -------   ----------  --------- ----------  ----------
```

```
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 20: 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 21: 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 22: 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.

Procedure

	Command or Action	Purpose

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

Step 2	**power redundancy-mode** {**combined** | **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 shutting 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.

Provideing 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.

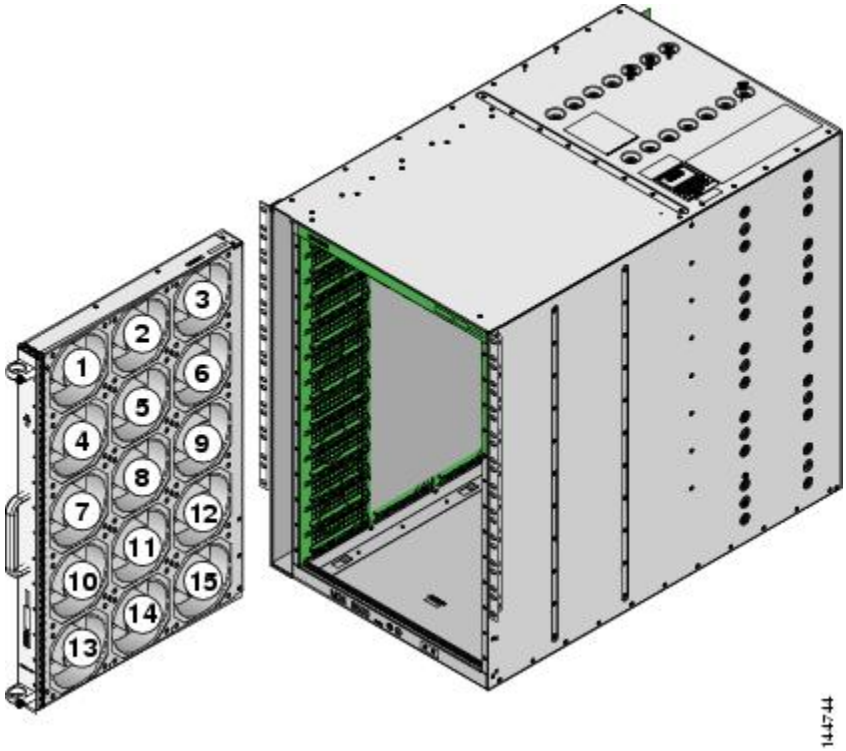
On the Cisco MDS 9513 Director, the front fan module has 15 fans. If the front fan module (DS-13SLT-FAN-F) State field contains "failure" in the **show environment fan** command output, it also displays the numbers of the failing fans.

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 6: 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)
-----------------------------------------------------------------
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 23: Default Hardware Parameter Settings

Parameter	Default Setting
Power supply mode	Redundant mode.

CHAPTER 11

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 151
- Maintaining Supervisor Modules, page 154
- Verifying the Status of a Module, page 155
- Checking the State of a Module, page 156
- Connecting to a Module, page 157
- Reloading Modules, page 158
- Saving the Module Configuration, page 159
- Purging Module Configurations, page 160
- Powering Off Switching Modules, page 160
- Identifying Module LEDs, page 161
- EPLD Images, page 168
- SSI Boot Images, page 173
- Managing SSMs and Supervisor Modules, page 181
- Default Settings, page 184

About Modules

This table describes the supervisor module options for switches in the Cisco MDS 9000 Family.

Table 24: 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	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. 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).

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                             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 25: 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.

Procedure

	Command or Action	Purpose

Step 1	**attach module** *slot*
	
	Example:
	`switch# attach module 4`
	`Attaching to module 4 ...`
	`To exit type 'exit', to abort type '$.'`
	`module-4#`
		Provides direct access to the module in the specified slot.

Step 2	**exit**
	
	Example:
	`module-4# exit`
	`rlogin: connection closed.`
	`switch#`
		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.

Procedure

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.

Procedure

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 26: 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.

Scenario	Consequence
You enter a **reload module** *number* command to reload a switching module.	The configured module information is preserved.
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. Sample scenario: **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.	The configured module information is lost from the running configuration. The default configuration is applied. The configured module information remains in startup configuration until a **copy running-config startup-config** command is issued again. Sample response: **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 address10.1.5.500. 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.

Procedure

	Command or Action	Purpose

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

Step 2	[**no**] **poweroff module** *slot* **Example:** `switch(config)# poweroff module 2`	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 27: 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 28: 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 29: 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 30: 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.

Procedure

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/pcgi-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-sf1ek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-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-sf1ek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-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-sf1ek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-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-sf1ek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-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-sf1ek9-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-sf1ek9-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 he system will automatically synchronize the ELPD 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 SANTap 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.

Procedure

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.

Procedure

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 31: 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
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.

Procedure

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/pcgi-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-sf1ek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-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-sf1ek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-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-sf1ek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-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-sf1ek9-kickstart-mz.2.1.1.bin
15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-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-sf1ek9-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-sf1ek9-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.

Procedure

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.

Procedure

	Command or Action	Purpose

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

Step 2	[**no**] **ssm upgrade delay** *seconds* **Example:** `switch(config)# ssm upgrade delay 30`	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. Use the **no** form of the command to clear the delay timer.
Step 3	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

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.

Procedure

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 32: Default Supervisor Module Settings

Parameter	Default
Administrative connection	Serial connection.
Global switch information	• No value for system name. • No value for system contact. • No value for location.

Parameter	Default
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 33: Default Supervisor Module Settings

Parameter	Default
Initial state when installed	• 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 45
  filtering output 45
  searching output 45

A

aliases, See command aliases
archive files 91, 92, 93
  appending files 92
  creating 91
  displaying the contents to the screen 92
  extracting files 92
  listing archived filenames 93

B

banners, See MOTD banners
BIOS 50
  loader> prompt 50
boot variables 108
  erasing configuration 108

C

Call Home 2
  description 2
CDP 111, 113, 114, 115
  clearing cache 114
  clearing counters 115
  clearing statistics 114
  clearing tables 115
  configuring timers, example 115
  default settings 115
  description 111
  optional parameters 113
  verifying configuration 114
characters 25
  special 25
Cisco Embedded Event Manager., See EEM
Cisco MDS 9200 Series interfaces modules 161
  LED description 161
Cisco MDS 9200 Series supervisor modules 161
  LED description 161
Cisco MDS 9200 Series switching modules 161
  LED description 161
CLI 22, 29, 46, 47, 48, 49, 50
  command history 46
  command modes 22
  command name completion 29
  command prompt 22
  configuring the edit mode 47
  disabling confirmation prompts 48
  enabling confirmation prompts 48
  examples 50
  setting display colors 49
CLI history 47
  controlling command recall 47
CLI prompt 22
  description 22
CLI variables 31, 32, 51
  characteristics 31
  description 31
  examples 51
  persistent 32
  referencing 31
  session-only 31
  system-defined variables 51
clock modules 147
  description 147
  displaying information 147
clocks 71, 77, 79
  default settings 79
  description 71
  setting manually 77
COM1 port 56
  settings 56
COM1 ports 59, 62, 67
  configuring settings 59
  default settings 67
  enabling modem connections 62

command aliases 33, 34, 50
characteristics 33
defining 33
description 33
examples 50
user session only 34
command history 46, 48
description 46
displaying 48
command modes 22, 23, 24
description 22
EXEC 22
global configuration 22
interface 23
restoring 24
saving 24
subinterface 23
summary (table) 24
command scripts 34, 35, 36, 52
delaying command actions 36
description 34
echoing text to terminals 35
examples 52
commands 28, 30, 46
abbreviations 28
no form 30
recalling 46
commands scripts 35
running 35
CompactFlash 129, 130, 131, 132, 133, 134, 135
Disabling automatic firmware update 130
disabling automatic testing 132
disabling checksum failure actions 131
disabling firmware update failure actions 134
displaying CRC test statistics 135
displaying firmware update configuration 135
displaying firmware update statistics 135
Enabling automatic firmware update 130
enabling automatic testing 132
enabling checksum failure actions 131
enabling firmware update failure actions 134
running tests 129
setting CRC checksum test intervals 131
setting firmware update intervals 133
updating firmware on demand 132
compatibility 1
software 1
configuration 79, 109
displaying 79, 109
configuration files 99, 100, 103, 106, 108, 109, 110
copying from remote servers 100
copying to external memory 103
copying to internal file systems 106
description 99
configuration files *(continued)*
erasing 108
example backup 109
example copy 109
example roll back 110
rolling back to previous configurations 106
types 99
configuration prompts 48
disabing 48
enabing 48
console ports 56, 57, 62, 67
configuring settings 57
default settings 67
enabling modem connections 62
settings 56
context-sensitive help 36
syntax checking 36
crossbar management 141, 142, 143
backward compatibility for Generation 1 modules 143
description 141
graceful shutdown 143
removing 142

D

daylight savings time, See summer time
default gateway 70
description 70
default settings 67, 79, 97, 115, 125, 149
CDP 115
clocks 79
COM1 ports 67
console ports 67
file systems 97
modems 67
MOTD banners 79
NTP 125
system hardware 149
Telnet servers 79
terminals 67
virtual terminals 67
diagnostics., See online diagnostics
diff utility 41
description 41
directories 83, 84, 85
changing current directories 84
creating 85
description 83
displaying contents 85
displaying current directory 84
working with 84

downgrading 183
guidelines 183

E

EDLD images 168
downgrading 168
EEM 2
description 2
egrep utility 43
filtering show command output 43
searching show command output 43
EPLD images 168, 172
description 168
displaying versions 172
upgrading 168
examples 93, 94, 95, 96, 109, 110
accessing directories on standby supervisor modules 93
backing up configuration files 109
compressing files 96
copying configuration files 109
copying files 94
displaying file checksums 95
displaying file contents 95
finding files 96
moving files 94
redirecting show command output 96
rolling back to a previous configuration 110
uncompressing files 96
EXEC command mode 22
description 22

F

fan modules 145
description 145
file systems 81, 84, 86, 97
accessing standby supervisor modules 86
changing current directories 84
default settings 97
description 81
specifying 81
files 83, 86, 87, 88, 89, 90, 91, 94, 95, 96
compressing 89
compressing, examples 96
copying 87
copying, examples 94
deleting 88
description 83
displaying checksums 88
displaying contents 88
files *(continued)*
displaying files checksums, examples 95
displaying files contents, examples 95
displaying last lines 89
finding 90
finding, example 96
moving 86
moving, examples 94
redirecting command output 90
renaming 86
tar files 91
uncompressing 89
uncompressing, examples 96
files systems 84
displaying current directory 84
filtering 39, 40, 41, 43, 44, 45
--More-- prompt 45
diff utility 41
egrep utility 43
grep utility 43
keywords 40
less utility 43
sed utility 44
show command output 39
Flash devices 83
formatting 83

G

global configuration command mode 22
description 22
global configuration mode 24
summary 24
grep utility 43
searching show command output 43
grep utility filtering show command output 43

H

hardware 127
displaying inventory 127
high availability 112, 119
CDP 112
NTP 112, 119
hostname 69, 71
configuring 71
description 69

I

install all command 179
  SSI boot images 179
Interface configuration command mode 23
  description 23
interface configuration mode 24
  summary 24

K

keystrokes 26
  shortcuts 26

L

LEDs 161
  descriptions 161
less utility 43
  filtering show command output 43
  searching show command output 43
licensing 5
  support 5
loader> prompt 50
  description 50

M

manageability 2
  description 2
management 15
  configuring in-band management 15
management interface 72
  configuring 72
message-of-the-day banners, See MOTD banners
modems 57, 62, 63, 65, 66, 67
  configuring connections 62
  configuring user-specific initialization strings 65
  default settings 67
  downloading initialization string 63
  enabling connections 62
  initializing connection 66
  settings 57
modes, See command modes
module temperature monitoring 144
  description 144
modules 49, 107, 144, 151, 152, 154, 155, 156, 157, 158, 159, 160
  checking states 156
  connecting to with CLI 157
  description 151
modules *(continued)*
  monitoring temperatures 144
  power cycling 158
  purging configurations 160
  reloading 158
  removing configuration after removal 107
  saving configurations 159
  sending commands from the supervisor mdoule session 49
  services modules 154
  supervisor modules 152
  switching modules 154
  verifying status 155
MOTD banner 74
  configuring 74
MOTD banners 70, 79
  default settings 79
  description 70
MSMs 181
  configuring global delay timers 181

N

NTP 4, 112, 117, 119, 120, 121, 124, 125
  configuring server 120
  clearing a session 124
  clearing statistics 121, 124
  configuration distribution 119
  configuring a server, example 125
  configuring peer 120
  default settings 125
  description 4, 117
  displaying statistics 121
  guidelines 119
  high availability 112, 119
  limitations 119
  prerequisites 119
  verifying configuration 124
NTP configuration disitribution 121
  enabling 121
NTP configuration distribution 122, 123, 124
  committing changes 122
  discarding changes 123
  releaseing the fabric session lock 124

O

online diagnostics 2
  description 2

P

power 136
  displaying usage information 136
power cycling 158
  modules 158
power supple mode 137
  description 137
power supply modes 137, 140
  configuration guidelines 137
  configuring 140
privileged EXEC mode 24
  summary 24
prompts, See confirmation prompts

Q

QoS 5
  description 5
Quality of Service., See QoS

R

RBAC 3
  description 3
regular expressions 38, 39
  anchoring 39
  filtering CLI output 38
  multiple-character patterns 38
  special characters 38
role-based access control., See RBAC
running configuration 79, 109
  displaying 79, 109
running configurations 100, 101, 104, 106, 107, 109, 110
  copying from external memory devices 104
  copying to internal file systems 106
  downloading from remote servers 101
  example backup 109
  example copy 109
  example roll back 110
  removing configuration for missing modules 107
  rolling back to previous configurations 106
  saving to startup configurations 100

S

scripts, See command scripts
searching 39, 40, 41, 43, 44, 45
  --More-- prompt 45
  diff utility 41
searching *(continued)*
  egrep utility 43
  grep utility 43
  keywords 40
  less utility 43
  sed utility 44
  show command output 39
sed utility 44
  filtering show command output 44
  searching show command output 44
serial number 136
  displaying 136
serviceability 1
  description 1
services modules 154
  description 154
setup utility 7, 9
  description 7
  prerequisites 9
shortcuts 26
  keystrokes 26
show command output 96
  redirecting, example 96
show commands 39
  filtering output 39
  searching output 39
Simple Network Management Protocol., See SNMP
SNMP 2
  description 2
software compatibility 1
  description 1
sort utility 44
  description 44
SPAN 2
  description 2
special characters 25
  description 25
sscp 40, 45, 52
  example 52
  redirecting show command output 40, 45
SSI boot images 173, 174, 176, 179
  description 173
  downgrading 174
  installing 173
  upgrading 174
  Using install all command 179
  verifying 176
SSMs 181, 182, 184
  configuring global delay timers 181
  default settings 184
  downgrading software, guidelines 181
  recovering after replacing corrupted Compact Flash 182
  replacing, guidelines 181
  replacing, guidlines 181

SSMs *(continued)*
upgrading software, guidelines **181**
standby supervisor modules **86, 93**
accessing directories, examples **93**
accessing file systems **86**
startup configuration **79, 108, 109**
displaying **79, 109**
erasing **108**
startup configurations **100, 102, 105, 106, 109, 110**
copying from external memory devices **105**
copying from running configurations **100**
copying to internal file systems **106**
downloading from remote servers **102**
example backup **109**
example copy **109**
example roll back **110**
rolling back to previous configurations **106**
streaming secure copy, See sscp
subinterface configuration command mode **23**
description **23**
subinterface configuration mode **24**
summary **24**
summer time **71, 76**
configuring **76**
description **71**
supervisor modules **152, 181, 184**
default settings **184**
description **152**
downgrading, guidelines **181**
replacing, guidelines **181**
upgrading, guidelines **181**
Switched Port Analyzer., See SPAN
switches **158**
reloading **158**
switching module **159**
reloading **159**
switching modules **154, 160**
description **154**
powering off **160**
switchname **71**
See also hostname
configuring **71**
See also hostname
syntax checking, See context-sensitive help
system hardware **149**
default settings **149**

T

Telnet servers **71, 78, 79**
connections **71**
default settings **79**
disabling connection **78**
enabling connection **78**
terminal sessions **55, 66, 67**
clearing **66**
displaying information **67**
settings **55**
terminals **67**
default settings **67**
time zones **71, 75**
configuring **75**
description **71**

U

upgrading **183**
guidelines **183**
user sessions **71, 78**
description **71**
sending messages **78**
users **77**
managing **77**
users sessions **78**
displaying information **78**

V

variables, See CLI variables
virtual terminals **57, 60, 61, 67**
configuring **60**
configuring session limits **61**
default settings **67**
settings **57**