Cisco MDS 9000 Series Fundamentals Configuration Guide, Release 9.x

First Published: 2022-09-02

Last Modified: 2024-12-06

Americas Headquarters

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

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

Full Cisco Trademarks with Software License ?

PREFACE **Preface** xv

Audience xv

Document Conventions xv

Documentation Feedback xvii

Related Documentation xvii

Communications, Services, and Additional Information xvii

CHAPTER 1 **New and Changed Information** 1

Change Summary 1

CHAPTER 2 **Overview** 3

Software Compatibility 3

Modular Software Design 3

Serviceability 3

Switched Port Analyzer 4

Call Home 4

Online Diagnostics 4

Embedded Event Manager 4

Consistency Checker 4

Manageability 6

Simple Network Management Protocol 7

Role-Based Access Control 7

Cisco NX-OS Software Configuration 7

Tools for Software Configuration 7

CLI 7

NTP 8

Licensing 9

Quality of Service 9

CHAPTER 3 Using the Cisco NX-OS Setup Utility 11

Information About the Cisco NX-OS Setup Utility 11

Prerequisites for the Setup Utility 13

Initial Setup Routine 13

Configuring Out-of-Band Management 13

Configuring In-Band Management 20

Where to Go Next 26

CHAPTER 4 Using PowerOn Auto Provisioning 27

About Power On Auto Provisioning 27

POAP Configuration Script 27

Guidelines and Limitations for POAP Configuration 28

Network Infrastructure Requirements for POAP 28

Setting Up the Network Environment to use POAP 29

Using USB 29

Using a DHCP Server 30

The POAP Process 32

The Power-Up Phase 33

The USB Discovery Phase 34

The DHCP Discovery Phase 34

Script Execution Phase 35

Post-Installation Reload Phase 36

Configuring a Switch Using POAP 36

Verifying the Device Configuration 36

CHAPTER 5 Understanding the Command-Line Interface 37

Information About the CLI Prompt 37

Command Modes 38

EXEC Command Mode 38

- Global Configuration Command Mode 38
- Interface Configuration Command Mode 39
- Subinterface Configuration Command Mode 40
- Saving and Restoring a Command Mode 40
- Command Mode Summary 41

Special Characters 41

Keystroke Shortcuts 42

Abbreviating Commands 44

Completing a Partial Command Name 44

Identifying Your Location in the Command Hierarchy 45

Using the no Form of a Command 45

Configuring CLI Variables 46
- About CLI Variables 46
- Configuring CLI Session-Only Variables 47
- Configuring Persistent CLI Variables 47

Command Aliases 48
- About Command Aliases 48
- Defining Command Aliases 49
- Configuring Command Aliases for a User Session 50

Command Scripts 50
- Running a Command Script 50
- Echoing Information to the Terminal 51
- Delaying Command Action 52

Context-Sensitive Help 52

Understanding Regular Expressions 53
- Special Characters 54
- Multiple-Character Patterns 54
- Anchoring 54

Searching and Filtering show Command Output 55
- Filtering and Searching Keywords 56
- diff Utility 57
- grep and egrep Utilities 57
- less Utility 58
- sed Utility 58

sort Utility 58

sscp Utility 59

Searching and Filtering from the --More-- Prompt 60

Using the Command History 61

Recalling a Command 61

Configuring the CLI Edit Mode 61

Controlling CLI History Recall 62

Displaying the Command History 62

Enabling or Disabling the CLI Confirmation Prompts 62

Setting CLI Display Colors 63

Sending Commands to Modules 63

BIOS Loader Prompt 64

Examples Using the CLI 64

Defining Command Aliases 64

Using CLI Session Variables 65

Using the System-Defined Timestamp Variable 65

Running a Command Script 66

Using the sscp Utility to Redirect show Command Output 67

CHAPTER 6 **Configuring Terminal Settings and Sessions** 69

Information About Terminal Settings and Sessions 69

Terminal Session Settings 69

Console Port 69

COM1 Port 70

Virtual Terminals 70

Modem Support 70

Configuring the Console Port 71

Configuring the COM1 Port 73

Configuring Virtual Terminals 74

Configuring the Inactive Session Timeout 75

Configuring the Session Limit 76

Configuring Modem Connections 77

Enabling a Modem Connection 77

Downloading the Default Initialization String 78

Configuring and Downloading a User-Specified Initialization String 79

Initializing a Modem for a Powered-Up Cisco NX-OS Device 81

Clearing Terminal Sessions 81

Displaying Terminal and Session Information 82

Default Settings for Terminal Display and Session Parameters 82

CHAPTER 7 **Basic Device Management** 85

Information About Basic Device Management 85

Device Hostname 85

Interface 86

Default Gateway 86

Message-of-the-Day Banner 86

Device Clock 87

Time Zone and Summer Time (Daylight Saving Time) 87

User Sessions 87

Telnet Server Connection 87

Changing the Device Hostname 87

Configuring the Management Interface 88

Configuirng the Default Gateway 89

Configuring the MOTD Banner 90

Configuring the Time Zone 91

Configuring Summer Time (Daylight Saving Time) 92

Manually Setting the Device Clock 93

Managing Users 94

Displaying Information about the User Sessions 94

Sending a Message to Users 95

Enabling or Disabling a Telnet Server Connection 95

Secure Erase 96

Prerequisites for Performing Secure Erase 96

Guidelines and Limitations for Secure Erase 97

Performing Secure Erase 97

Verifying the Device Configuration 98

Default Settings for Basic Device Parameters 98

CHAPTER 8

Using the Device File Systems, Directories, and Files 99
Information About Device File Systems, Directories, Files, and External Storage Devices 99
File Systems 99
Directories 100
Files 100
Working with External Storage Devices 101
Formatting an External Flash Device 101
Mounting or Unmounting a USB Drive 101
External Storage Device Support Matrix 101
Working with Directories 102
Identifying the Current Directory 102
Changing the Current Directory 103
Creating a Directory 103
Displaying Directory Contents 103
Deleting a Directory 103
Accessing the Directories on a Standby Supervisor Module 104
Working with Files 104
Moving a File 104
Copying a File 105
Deleting a File 105
Displaying a File's Contents 105
Displaying a File's Checksums 106
Compressing and Uncompressing a File 106
Displaying the Last Lines in a File 107
Redirecting show Command Output to a File 107
Finding Files 107
Working with Archive Files 107
Creating an Archive File 107
Appending Files to an Archive File 108
Extracting Files from an Archive File 109
Displaying the Filenames in an Archive File 109
Examples of Using a File System 109
Accessing Directories on a Standby Supervisor Module 110

Performing ISSU or ISSD Using a USB Drive 110

CHAPTER 9 Working with Configuration Files 111

Information About Configuration Files 111

Types of Configuration Files 111

Managing Configuration Files 112

Saving the Running Configuration to the Startup Configuration 112

Copying a Configuration File to a Remote Server 112

Downloading the Running Configuration From a Remote Server 113

Downloading the Startup Configuration From a Remote Server 114

Copying Configuration Files to an External Flash Memory Device 116

Copying the Running Configuration from an External Flash Memory Device 117

Copying the Startup Configuration from an External Flash Memory Device 118

Copying Configuration Files to an Internal File System 118

Rolling Back to a Previous Configuration 119

Removing the Configuration for a Missing Module 120

Erasing a Configuration 121

Verifying the Device Configuration 122

Examples of Working with Configuration Files 122

Copying Configuration Files 123

Backing Up Configuration Files 123

Rolling Back to a Previous Configuration 123

CHAPTER 10 Configuring CDP 125

Information About CDP 125

CDP Overview 125

High Availability for CDP 126

Configuring CDP 126

Enabling or Disabling CDP Globally 126

Enabling or Disabling CDP on an Interface 126

Configuring Optional CDP Parameters 127

Verifying the CDP Configuration 128

Clearing CDP Counters and Tables 129

CDP Example Configuration 129

Default Settings for CDP 129

CHAPTER 11 Configuring LLDP 131

About LLDP 131

About DCBX 132

High Availability 132

Virtualization Support 133

Platforms Supported 133

Guidelines and Limitations for LLDP 133

Default Settings for LLDP 134

Configuring LLDP 134

Enabling or Disabling LLDP Globally 134

Enabling or Disabling LLDP on an Interface 135

Configuring Optional LLDP Parameters 136

Verifying the LLDP Configuration 137

Configuration Example for LLDP 138

CHAPTER 12 Configuring NTP 139

Information About NTP 139

NTP 139

Prerequisites for NTP 140

Guidelines and Limitations for NTP 141

Configuring NTP 141

Enabling NTP 141

Disabling NTP 141

Configuring Authentication Keys 142

Enabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations 143

Disabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations 143

Enabling NTP Servers and Peers 143

Disabling NTP Servers and Peers 145

Enabling NTP Modes 145

Disabling NTP Modes 145

Enabling NTP Source Interface 146

Disabling NTP Source Interface 146

Enabling NTP Logging 146
Disabling NTP Logging 147
Configuring NTP Syslog Logging Level 147
Setting the Default NTP Syslog Severity Logging Level 148
Displaying and Clearing NTP Statistics 148
Resynchronizing NTP 149
Distributing the NTP Configuration Using CFS 149
Enabling NTP Configuration Distribution 149
Disabling NTP Configuration Distribution 150
Committing NTP Configuration Changes 150
Discarding NTP Configuration Changes 150
Forcing Termination of a Lost NTP Configuration Session 151
Verifying NTP 151
Troubleshooting NTP 152
Example: Configuring NTP 155
Default Settings for NTP 156

CHAPTER 13 **Managing System Hardware** 157
Displaying Switch Hardware Inventory 157
Running CompactFlash Tests 161
Displaying the Switch Serial Number 161
Displaying Power Usage Information 162
Power Supply Modes 163
Configuration Guidelines for Power Supplies 164
Configuring the Power Supply Mode 171
About Switch Temperature Monitoring 172
Displaying Switch Temperatures 173
About Fan Modules 174
Displaying Environment Information 175
Default Settings 180

CHAPTER 14 **Managing Modules** 181
About Modules 181
Supervisor Modules 182

Switching Modules 184

Services Modules 184

Maintaining Supervisor Modules 184

Replacing Supervisor Modules 184

Standby Supervisor Module Boot Variable Version 184

Standby Supervisor Module Bootflash Memory 184

Standby Supervisor Module Boot Alert 185

Verifying the Status of a Module 185

Checking the State of a Module 186

Connecting to a Module 187

Reloading Modules 187

Reloading a Switch 187

Power Cycling Modules 188

Reloading Switching Modules 188

Saving the Module Configuration 189

Purging Module Configurations 190

Powering Off Switching Modules 190

Powering off Power Supply Units 191

Identifying Module LEDs 192

EPLD Images 197

Upgrading EPLD Images 198

Displaying EPLD Image Versions 202

SSI Boot Images 203

Managing SSMs and Supervisor Modules 203

Configuring SSM and MSM Global Upgrade Delay 203

Guidelines for Replacing SSMs and Supervisor Modules 204

Recovering an SSM After Replacing Corrupted CompactFlash Memory 204

Guidelines for Upgrading and Downgrading Cisco MDS NX-OS Releases 205

Default Settings 207

CHAPTER 15 Scripting with Tcl 209

Finding Feature Information 209

Guidelines and Limitations 209

Tclsh Command Help 209

Tclsh Command History 210

Tclsh Tab Completion 210

Tclsh CLI Command 210

Tclsh Command Separation 210

Tcl Variables 211

Tclquit 211

Tclsh Security 211

Information about Tcl 211

Running the tclsh Command 212

Navigating Cisco NX-OS Modes from the tclsh Command 213

Tcl References 214

CHAPTER 16 **Intersight Device Connector** 215

Device Connector 215

Guidelines and Limitations for Device Connector 216

Configuring NXDC 216

Verify Intersight 218

Preface

This preface describes the audience, organization of, and conventions used in the Cisco MDS 9000 Series Configuration Guides. It also provides information on how to obtain related documentation, and contains the following sections:

- Audience, on page xv
- Document Conventions, on page xv
- Documentation Feedback, on page xvii
- Related Documentation, on page xvii
- Communications, Services, and Additional Information, on page xvii

Audience

This publication is for network administrators who install, configure, and maintain Cisco MDS 9000 Series Switches.

Document Conventions

Command descriptions use these 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 these 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.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Documentation Feedback

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

Related Documentation

The entire Cisco MDS 9000 Series switches documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/series.html

Documentation Roadmap

https://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/rel90.html

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

CHAPTER 1

New and Changed Information

- Change Summary, on page 1

Change Summary

The following table summarizes the new and changed information in this document, and provides information about the releases in which each feature is supported.

Note that your software release might not support all the features described in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/, and the release notes document pertaining to your software release.

Table 1: New and Changed Features

Feature Name	Description	Release	Where Documented
Displaying Module Temperatures	Support to detect overheating and ensure equipment protection is added. Alarm and warning thresholds can be lowered for air intake temperature sensors s1 and s2, and exhaust temperature sensors s3 and s4.	9.4(3)	About Switch Temperature Monitoring, on page 172
LLDP on management(0) port.	Support for LLDP reception and advertisement on the active management interface has been added for all platforms, excluding MDS 9250i, MDS 9148S, and MDS 9396S.	9.4(1)	Configuring LLDP

Feature Name	Description	Release	Where Documented
Intersight device connector	A secure way to connect devices to send information and receive control instructions on Cisco MDS 9000 Family switches.	9.3(2)	Intersight Device Connector, on page 215
Secure Erase	The Secure Erase feature allows erasure of all customer information from Cisco MDS switches.	9.2(2)	Basic Device Management, on page 85
Consistency Checker	Added support to display the access control list (ACL), forwarding information base (FIB), and persistent storage service (PSS) consistency information, using the **show consistency-checker** command.	8.4(1)	Overview, on page 3

CHAPTER 2

Overview

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

- Software Compatibility, on page 3
- Serviceability, on page 3
- Manageability, on page 6
- Cisco NX-OS Software Configuration, on page 7
- Licensing, on page 9
- Quality of Service , on page 9

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 .

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 Nexus 7000 Series NX-OS System Management Configuration Guide*.

Online Diagnostics

Cisco generic online diagnostics (GOLD) verify that hardware and internal data paths are operating as designed. Boot-time diagnostics, continuous monitoring, and on-demand and scheduled tests are part of the Cisco GOLD feature set. GOLD allows rapid fault isolation and continuous system monitoring. For information about configuring GOLD, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide.*

Embedded Event Manager

Cisco Embedded Event Manager (EEM) is a device and system management feature that helps you to customize behavior based on network events as they happen. For information about configuring EEM, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

Consistency Checker

Overview

This section describes how to use the Consistency Checker feature.

The Consistency Checker feature is a tool to assist troubleshooting a switch. It can be used to validate various internal tables that are distributed between processes and modules. Using such programmatic algorithms remove human error from checking large and complex tables manually; thereby, quickly confirming the status of the tables and reducing the mean time to resolve such issues.

The Consistency Checker commands are used to validate software and hardware table states. The result is displayed as pass or fail. A failure result causes detailed information about the detected inconsistencies to be logged for further investigation.

Each Consistency Checker command may take several minutes to execute depending on the size of the configuration and number of modules in the switch. The check may fail if any of the tables under assessment change state during the check. Checks do not differentiate if the failure is due to normal changes, such as zoning changes, port flaps, or genuine errors. Thus, it is important to verify that a failure was not caused by normal events that occurred during the check. Rerun the failed check several times over a period of minutes to confirm if the failure is persistent. Persistent failure means that the detailed failure information does not change. If a persistent failure is found, contact your vendor for further analysis.

Currently, this feature only supports *on-demand* execution of commands; they are not run automatically by the system.

The Consistency Checker feature supports verification of table consistency for the following features:

Cisco NX-OS Release 8.4(1)

- Access control list (ACL) Tables
- Forwarding information base (FIB) Tables
- Persistent Storage Service (PSS)

ACL Tables

The ACL Consistency Checker verifies the programming consistency between software and hardware for ACL tables including the following checks:

- Hardware and software synchronization: This validation checks if entries present in the hardware table is same as in the software table and vice versa. This check flags errors if there is a mismatch in the entries between the two tables or if the error is present in one of the tables.
- Hardware and software duplicate entries check: This validation compares entries in the hardware and software tables to find any duplicate entries and flags them as errors.

Use the **show consistency-checker acl-table-status** [**module** *number*] command to run the ACL Consistency Checker. The ACL Consistency Checker is not run automatically or periodically by the system.

FIB Tables

The FIB Consistency Checker verifies the programming consistency between software and hardware entries for Fibre Channel forwarding and adjacency tables. If there is an inconsistency, the CLI prints the mismatch entries between the hardware and software entries of the forwarding and adjacency tables.

Use the **show consistency-checker fib-table-status** [**module** *number*] command to run the FIB Consistency Checker. The FIB Consistency Checker is not run automatically or periodically by the system.

Persistent Storage Service (PSS)

The PSS Consistency Checker verifies the consistency between run-time and cached configuration data for the following features:

- Spanning Tree
- Certain ingress and egress forwarding parameters for interfaces (ELTM)
- Interface state (ETHPM)
- VLAN information (Vlan-manager)

Use the **show consistency-checker pss** command to run the PSS Consistency Checker. The PSS Consistency Checker is not run automatically or periodically by the system.

SAN Analytics

The SAN Analytics Consistency Checker feature identifies inconsistencies in SAN Analytics components such as NPU, modules, queries, database, analytics ACL entries, and so on.

Use the **ShowAnalyticsConsistency** command in Cisco MDS NX-OS Release 8.5(1) or the **show consistency-checker analytics** command in Cisco MDS NX-OS Release 9.2(1) or later to run the SAN Analytics Consistency Checker.

Use the command to run the SAN Analytics Consistency Checker.

This command is a troubleshooting tool that helps to identify inconsistencies in SAN Analytics components such as NPU, modules, queries, database, port-sampling configuration and so on. Such inconsistencies are abnormal and may lead to issues on the switch.

This command should be used as part of troubleshooting when SAN Analytics issues are suspected. The specified consistency check is done at the time the command is issued and the results are displayed. Detailed information about the detected inconsistencies is displayed to direct further detailed debugging.

Note The SAN Analytics Consistency Checker does not work when port sampling or smart zoning is enabled.

Guidelines and Limitations

- The Consistency Checker feature is supported only on the following hardware:
  - Cisco MDS 9132T 32-Gbps 32-Port Fibre Channel Switch
  - Cisco MDS 9148T 32-Gbps 48-Port Fibre Channel Switch
  - Cisco MDS 9396T 32-Gbps 96-Port Fibre Channel Switch
  - Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module
  - Cisco MDS 9700 48-Port 16-Gbps Fibre Channel Switching Module
- If there is a configuration change or a table state change in the environment while a Consistency Checker is running, it is possible to trigger false positives. In cases where false positives may be a concern, it is recommended to run multiple iterations of that Consistency Checker.
- When you execute the **show consistency-checker acl-table-status** command, ensure that there are no background activities that can result in addition, deletion, or modification of existing ACL TCAM entries. The ACL Consistency Checker may take some time to complete.
- Before you run the **show consistency-checker acl-table-status** command, ensure that SAN Analytics port sampling is not enabled to prevent false positive results. The SAN Analytics feature itself does not cause false positive results.
- When you execute the **show consistency-checker fib-table-status** command, ensure that no routes are added, deleted, or updated while the Consistency Checker is still running. The FIB Consistency Checker may take some time to complete.
- In Cisco MDS NX-OS Release 8.4(1), the PSS Consistency Checker is supported only on an active supervisor.

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 Nexus 7000 Series NX-OS System Management Configuration Guide*.

Role-Based Access Control

With role-based access control (RBAC), you can limit access to device operations by assigning roles to users. You can customize access and restrict it to the users who require it. For more information about RBAC, see the *Cisco Nexus 7000 Series 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.

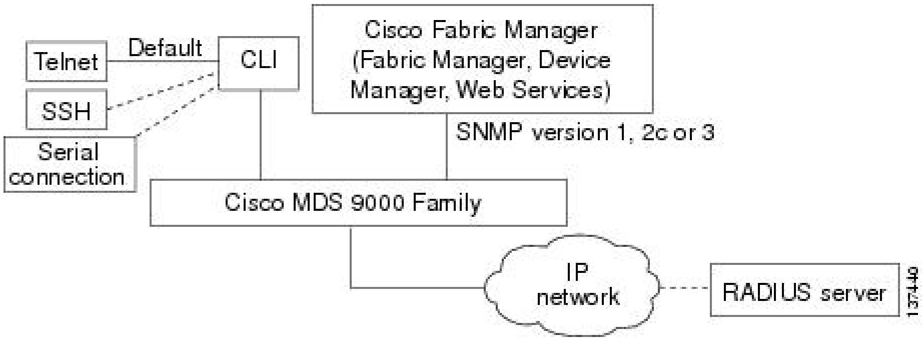
Tools for Software Configuration

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.

Figure 1: Tools for Configuring Cisco NX-OS Software

This figure shows the tools for configuring the 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.

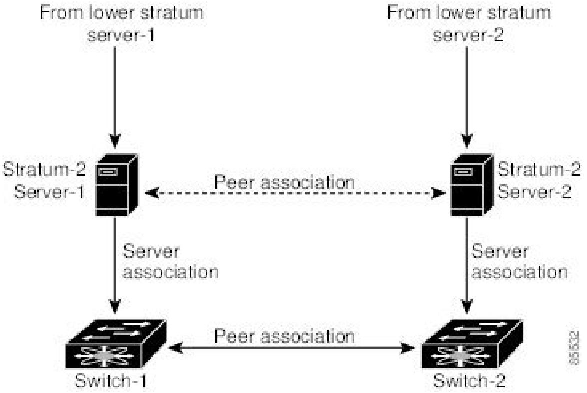
By configuring an IP address as a peer, the Cisco NX-OS device will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both of these instances point to different time servers, your NTP service is more reliable. Even if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

Figure 2: NTP Peer and Server Association

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.



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 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 NX-OS Licensing Guide*.

Quality of Service

The Cisco NX-OS software supports quality of service (QoS) functions for classification, marking, queuing, policing, and scheduling. Modular QoS CLI (MQC) supports all QoS features. You can use MQC to provide uniform configurations across various Cisco platforms. For more information, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide.*

CHAPTER 3

Using the Cisco NX-OS Setup Utility

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

- Information About the Cisco NX-OS Setup Utility, on page 11
- Prerequisites for the Setup Utility, on page 13
- Initial Setup Routine, on page 13
- Where to Go Next, on page 26

Information About the Cisco NX-OS Setup Utility

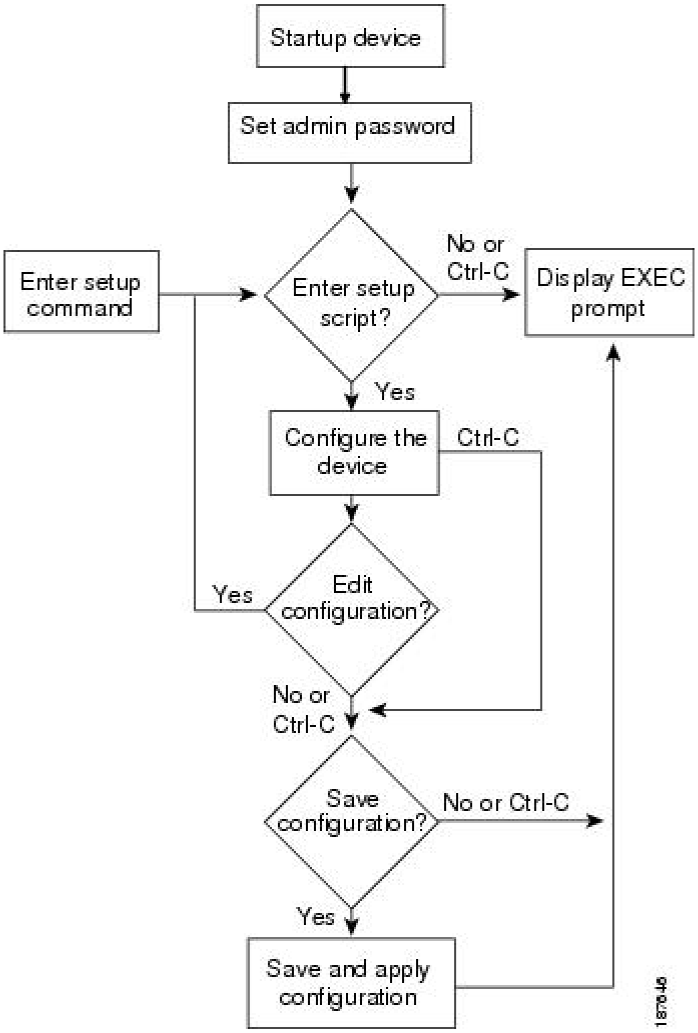
The Cisco NX-OS setup utility is an interactive command-line interface (CLI) mode that guides you through a basic (also called a startup) configuration of the system. The setup utility allows you to configure only enough connectivity for system management.

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.

Figure 3: Setup Script Flow

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



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

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

Note The setup script only supports IPv4.

Prerequisites for the Setup Utility

The setup utility has the following prerequisites:

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

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.

SUMMARY STEPS

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

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

DETAILED STEPS

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 4

Using PowerOn Auto Provisioning

This chapter describes how to deploy and use Power On Auto Provisioning (POAP).

This chapter contains the following sections:

- About Power On Auto Provisioning, on page 27
- Network Infrastructure Requirements for POAP, on page 28
- The POAP Process, on page 32
- Configuring a Switch Using POAP, on page 36
- Verifying the Device Configuration, on page 36

About Power On Auto Provisioning

When a Cisco MDS Series switch with POAP feature boots and does not find the startup configuration, the switch enters POAP mode and checks for a USB device (containing the configuration script file) in USB port 1. If it finds a USB device, it checks the device to see if the device also contains the software image files and the switch configuration file.

If the switch does not find a USB device in USB port 1, or if the USB device does not contain the required software image files or the switch configuration file, the switch locates a DHCP server and bootstraps itself with the interface IP address, gateway, DNS server IP addresses, IP address of a TFTP server or the URL of an HTTP server and the bootfile name. The switch then obtains the IP address of a TFTP server or the URL of an HTTP server from where it downloads the necessary configuration files.

Note DHCP information is used during the POAP process only when POAP fails via USB because of the following reasons:

- USB is not present.
- Script is not present or script is present with incorrect names.
- Script execution fails.

POAP Configuration Script

The reference script supplied by Cisco supports the following functionalities:

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

Guidelines and Limitations for POAP Configuration

The POAP configuration guidelines and limitations are as follows:

- Only FAT32 USB is supported. (The file system on the USB should be FAT32). For Cisco MDS 9700 series switches, POAP is supported only on USB 1 Port.
- The software image for the Cisco MDS 9000 Series Switches must support POAP.
- POAP can be initiated on any supported switch by erasing the startup configuration and reloading the switch.
- POAP does not support provisioning of the switch after it has been configured and is operational. Only auto provisioning of a switch with no startup configuration is supported.
- Important POAP updates are logged in the syslog and are available from the serial console.
- Critical POAP errors are logged to the bootflash. The filename format is date-time_poap_PID_[init,1,2].log, where date-time is in the YYYYMMDD_hhmmss format and PID is the process ID.
- Script logs are saved in the bootflash directory. The filename format is date-time_poap_PID_script.log, where date-time is in the YYYYMMDD_hhmmss format and PID is the process ID.
- You can configure the format of the script log file. These formats are specified in the script. The template of the script log file has a default format. However, you can choose a different format for the script execution log file.
- USB script execution logs are saved in the bootflash directory. The filename format is poap.log_usb_MM_DD_HR_MIN, where MM is the current month, DD is the date, HR is the current hour, and MIN is the current minute.
- The POAP feature does not require a license, and is enabled by default.

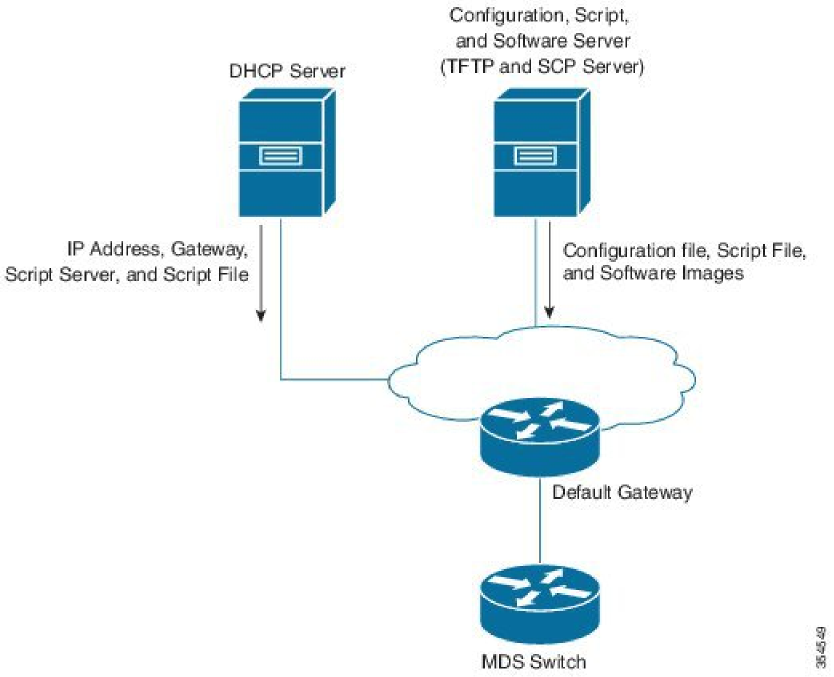
Note POAP is not supported through Nexus Dashboard Fabric Controller (NDFC), formally known as Cisco Data Center Network Management (DCNM).

Network Infrastructure Requirements for POAP

When there is no USB device with the required installation files, or the configuration files are not present in the USB, POAP requires the following network infrastructure:

- A DHCP server to bootstrap the interface IP address, gateway address, and TFTP address.
- A TFTP, SCP, FTP AND SFTP server that contains the configuration script used to automate the software image installation and configuration process.
- One or more servers containing the necessary software images and configuration files.

Figure 4: POAP Network Infrastructure



Setting Up the Network Environment to use POAP

The network environment for POAP can be set up with either a USB or a DHCP server.

Using USB

Follow these guidelines when copying software images, the configuration file, and the configuration script into a USB when setting up the network environment for POAP:

- The POAP configuration script on the USB should be titled poap_script.py.
  - The configuration file with the name *conf_<serialnum>.cfg* must be present in the USB. To obtain the serial number of the switch, run the **show sprom backplane 1** command:

```
switch# show sprom backplane 1
DISPLAY backplane sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 3
 Block Length    : 160
 Block Checksum  : 0x128e
 EEPROM Size     : 512
```

```
Block Count      : 6
FRU Major Type   : 0x6003
FRU Minor Type   : 0x0
OEM String       : Cisco Systems, Inc.
Product Number   : DS-C9148S48PK9
Serial Number    : JAF17353076
Part Number      : 73-15809-01
```

- The names of the software images copied to the USB should have standard names and must match the names specified in the POAP script.

  For example, to boot up a Cisco MDS 9396V 64-Gbps 96-Port Fibre Channel with the m9396v-s3ek9-kickstart-mz.9.4.3.bin and m9396v-s3ek9-mz.9.4.3.bin images, ensure that the POAP configuration script (poap_script.py) has the following information:

  - set m9148s_image_version 9.4.3
  - set m9396v_kickstart_image_src [format m9396v-s3ek9-kickstart-mz.%s.bin $m9396v_image_version]
  - set m9396v_system_image_src [format m9396v-s3ek9-mz.%s.bin $m9396v_image_version]

Note Ensure that the POAP script identifies the switch.

The latest versions are available here:

- Python scripts: Python Script
- Reference for documentation: README

Note

- Only FAT32 USB is supported. (The file system on the USB should be FAT32). For Cisco MDS 9700 series switches, POAP is supported only on USB 1 Port.
- Both the software images and the configuration files should be present in the USB. If no configuration is required, create an empty file named conf_serialnumber.cfg. When the configuration file is empty, the switch reloads the images twice from the USB.

Using a DHCP Server

Before you begin

Before using the POAP script, perform the following actions:

- Edit the options dictionary at the top of the script to ensure that all relevant options for your setup are included in the script. Do not change the defaults (in the default options function) directly.
- If you are updating the POAP script, update the MD5 checksum/tftpboot/poap/poap.py as shown using shell commands.

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

Every time the POAP script is updated, re-run the above script to generate a new MD5 checksum, which should then be used to update the POAP script accordingly.

Let me know if you want it more formal, technical, or casual!

Example of key update: `# md5sum="a9515da3152f222815eca4e7b8a53700"`

- If the device contains a startup configuration, execute a write erase and reload it.

Note The older 16G platforms continue to support .tcl script.

Procedure

Step 1 Deploy a TFTP server.

Step 2 Update the `poap.py` script with the following information. The `poap.py` script is present in the **/tftpboot/poap/** folder

a) Update image file

The following example shows how to update image file.

```
target_system_image = "m9148v-s8ek9-mz.9.4.3.bin" # Fill the target system image here
target_kickstart_image = "m9148v-s8ek9-kickstart-mz.9.4.3.bin" # Fill the target kickstart image
 here
```

b) Create hybrid-config folder

c) In the hybrid-config folder, create a text file with the serial number of the switch.

d) Add the running configuration of the switch to this text file.

Step 3 Ensure you have the following information in the TFTP server:

- POAP script is added to the /tftpboot/poap
- The text file with the running configuration of the switch with the correct serial number is added.

Step 4 Deploy a DHCP server.

Step 5 Configure the following parameters in the DHCP server:

- Enable the DHCP snooping
- Interface address range
- Gateway address
- Add DNS IP address
- TFTP server's IP address
- Script file name : /tftpboot/poap/poap.py
- File path: /tftpboot/poap

Step 6 Reload the switch

The POAP Process

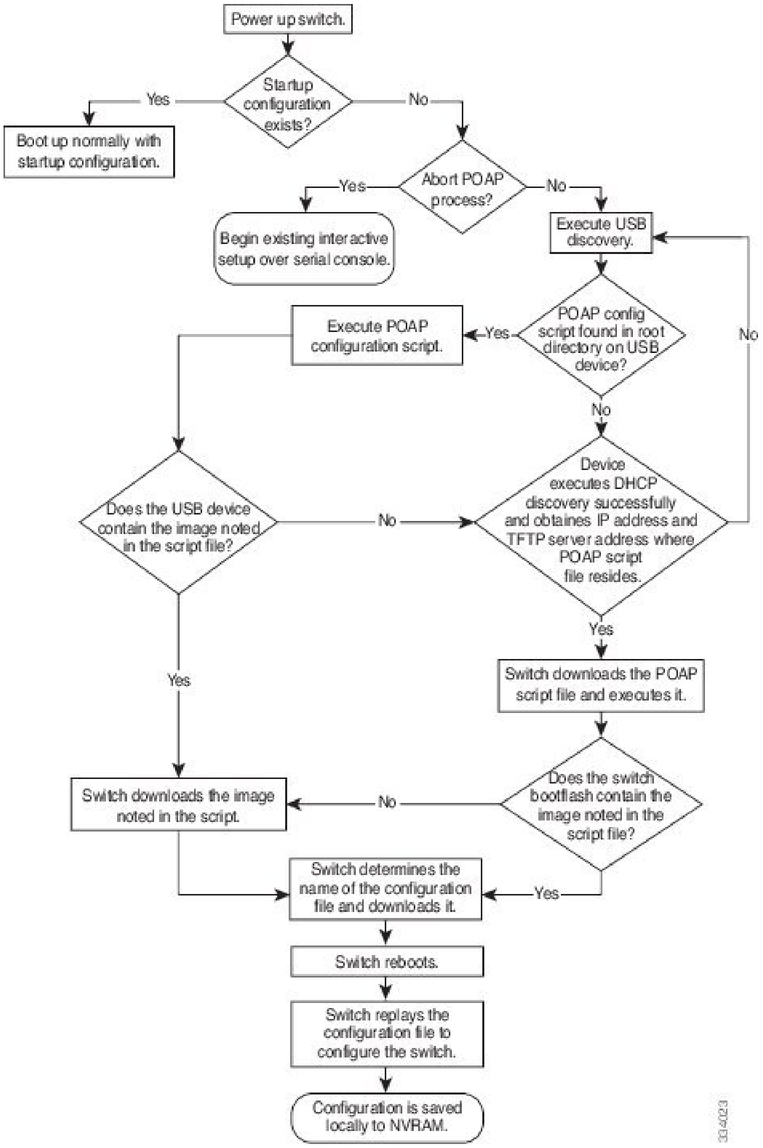
The POAP process involves the following phases:

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

Within these phases, other processes and decision points occur. The following illustration shows a POAP process flow:

See Setting Up the Network Environment to use POAP, on page 29 for more information on the POAP process.

Figure 5: The POAP Process


Power up switch.
Startup configuration exists?
Yes
No
Boot up normally with startup configuration.
Abort POAP process?
Yes
No
Begin existing interactive setup over serial console.
Execute USB discovery.
POAP config script found in root directory on USB device?
Yes
No
No
Execute POAP configuration script.
Does the USB device contain the image noted in the script file?
No
Device executes DHCP discovery successfully and obtaines IP address and TFTP server address where POAP script file resides.
Yes
Yes
Switch downloads the POAP script file and executes it.
Does the switch bootflash contain the image noted in the script file?
No
Switch downloads the image noted in the script.
Yes
Switch determines the name of the configuration file and downloads it.
Switch reboots.
Switch replays the configuration file to configure the switch.
Configuration is saved locally to NVRAM.
334023

The Power-Up Phase

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

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

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

If you exit POAP mode, you will enter a setup script that allows you to configure the system admin account and perform basic system setup through a guided dialog. If you remain in POAP mode, all front-panel interfaces will be configured with default settings.

The USB Discovery Phase

When the POAP process begins, the switch searches the root directory for the presence of accessible USB devices with the POAP configuration script file (poap_script.py), configuration files, and system and kickstart images.

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

If the software image and switch configuration files specified in the configuration script are present, POAP uses those files to install the software and configure the switch. If the software image and switch configuration files are not on the USB device, POAP performs a clean-up operation and starts the DHCP phase from the beginning.

The DHCP Discovery Phase

The switch sends out DHCP discover messages on the management interface that solicits DHCP offers from the DHCP server or servers. (See the following Figure 6: DHCP Discovery Process, on page 35.) The DHCP client on the Cisco MDS switch uses the switch serial number in the client-identifier option to identify itself to the DHCP server. The DHCP server can use this identifier to send information, such as the IP address and script filename, back to the DHCP client.

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

Note To stop the continuous looping process, the POAP process must be terminated manually.

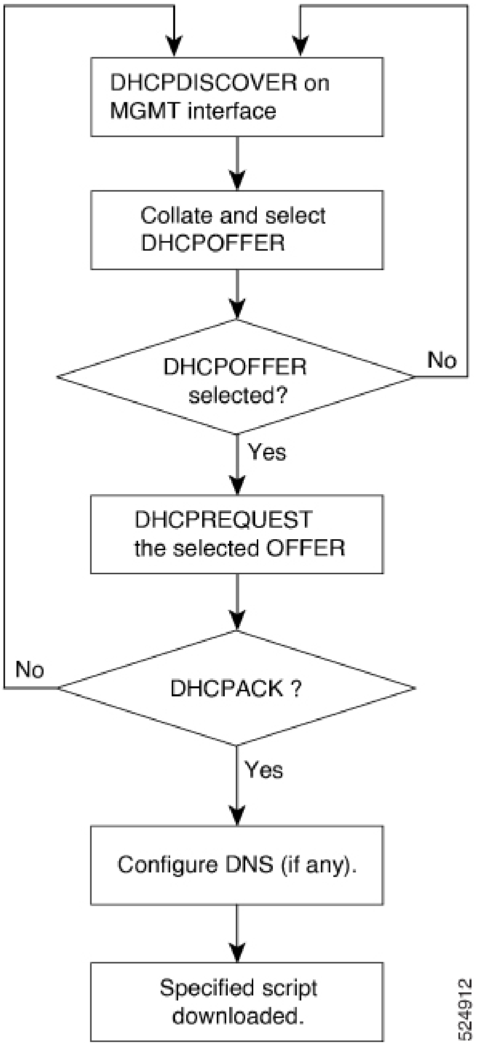
The DHCP discover message also solicits the following options from the DHCP server:

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

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

If none of the DHCP offers meet the requirements, the switch does not complete the DHCP negotiation (request and acknowledgment), and no IP address is assigned. However, the POAP process is not terminated because the switch reverts to the USB phase.

Figure 6: DHCP Discovery Process


DHCPDISCOVER on MGMT interface
Collate and select DHCPOFFER
DHCPOFFER selected?
No
Yes
DHCPREQUEST the selected OFFER
DHCPACK ?
No
Yes
Configure DNS (if any).
Specified script downloaded.
524912

Script Execution Phase

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

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

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

Note If script execution fails, the DHCP discovery process restarts.

Post-Installation Reload Phase

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

Configuring a Switch Using POAP

Before you begin

Make sure that the requisite network environment is set up to use POAP. For more information, see the Using USB, on page 29 section.

Procedure

Step 1 Install the switch in the network.

Step 2 Power on the switch.

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

No entry is required to continue booting in POAP mode.

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

What to do next

Verify the configuration.

Verifying the Device Configuration

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

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

For detailed information about these commands, see the *Cisco MDS 9000 Family Command Reference*.

CHAPTER 5

Understanding the Command-Line Interface

This chapter helps you understand the command-line interface.

- Information About the CLI Prompt, on page 37
- Command Modes, on page 38
- Special Characters, on page 41
- Keystroke Shortcuts, on page 42
- Abbreviating Commands, on page 44
- Completing a Partial Command Name, on page 44
- Identifying Your Location in the Command Hierarchy, on page 45
- Using the no Form of a Command , on page 45
- Configuring CLI Variables, on page 46
- Command Aliases, on page 48
- Command Scripts, on page 50
- Context-Sensitive Help , on page 52
- Understanding Regular Expressions, on page 53
- Searching and Filtering show Command Output, on page 55
- Searching and Filtering from the --More-- Prompt, on page 60
- Using the Command History, on page 61
- Enabling or Disabling the CLI Confirmation Prompts, on page 62
- Setting CLI Display Colors, on page 63
- Sending Commands to Modules, on page 63
- BIOS Loader Prompt, on page 64
- Examples Using the CLI , on page 64

Information About the CLI Prompt

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

```
User Access Verification
login: admin
Password:<password>
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
```

```
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
```

You can change the default device hostname.

From the CLI prompt, you can do the following:

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

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

Command Modes

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

EXEC Command Mode

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

Global Configuration Command Mode

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

SUMMARY STEPS

1. **configure terminal**

DETAILED STEPS

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.

SUMMARY STEPS

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

DETAILED STEPS

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.

SUMMARY STEPS

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

DETAILED STEPS

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 the current command mode, configure a feature, and then restore the previous command mode. The **push** command saves the command mode and the **pop** command restores the command mode.

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

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

Command Mode Summary

This table summarizes information about the main command modes.

Table 2: Command Mode Summary

Mode	Access Method	Prompt	Exit Method
EXEC	From the login prompt, enter your username and password.	`switch#`	To exit to the login prompt, use the **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 3: Special Characters

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

Keystroke Shortcuts

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

Table 4: Keystroke Shortcuts

Keystokes	Description
Ctrl-A	Moves the cursor to the beginning of the line.
Ctrl-B	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.
Ctrl-C	Cancels the command and returns to the command prompt.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Moves the cursor to the end of the line.
Ctrl-F	Moves the cursor one character to the right.
Ctrl-G	Exits to the previous command mode without removing the command string.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-L	Redisplays the current command line.
Ctrl-N	Displays the next command in the command history.
Ctrl-O	Clears the terminal screen.
Ctrl-P	Displays the previous command in the command history.
Ctrl-R	Redisplays the current command line.
Ctrl-T	Transposes the character under the cursor with the character located to the right of the cursor. The cursor is then moved one character to the right.
Ctrl-U	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-V	Removes any special meaning for the following keystroke. For example, press Ctrl-V before entering a question mark (?) in a regular expression.
Ctrl-W	Deletes the word to the left of the cursor.
Ctrl-X, H	Lists the history of commands you have entered. When using this key combination, press and release the Ctrl and X keys together before pressing H.
Ctrl-Y	Recalls the most recent entry in the buffer (press keys simultaneously).

Keystokes	Description
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.
Tab	Completes the word for you after you enter the first characters of the word and then press the Tab key. All options that match are presented. Use tabs to complete the following items: • Command names • Scheme names in the file system • Server names in the file system • Filenames in the file system

	Example:
	`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 5: Examples of Command Abbreviations

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

Completing a Partial Command Name

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

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

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

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

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

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

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

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

Identifying Your Location in the Command Hierarchy

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

SUMMARY STEPS

1. **where detail**

DETAILED STEPS

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*).

SUMMARY STEPS

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

DETAILED STEPS

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	(Optional) **show cli variables** **Example:** `switch# show cli variables`	Displays the CLI variable configuration.

Configuring Persistent CLI Variables

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

SUMMARY STEPS

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

DETAILED STEPS

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 a case-sensitive, alphanumeric string and must begin with an alphabetic character. The maximum length is 31 characters.

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

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

Command Aliases

This section provides information about command aliases.

About Command Aliases

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

Command alias support has the following characteristics:

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

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

Defining Command Aliases

You can define command aliases for commonly used commands.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

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

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

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

Configuring Command Aliases for a User Session

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

SUMMARY STEPS

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

DETAILED STEPS

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.

SUMMARY STEPS

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

DETAILED STEPS

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 6: Formatting Options for the echo Command

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

SUMMARY STEPS

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

DETAILED STEPS

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.

SUMMARY STEPS

1. **sleep** *seconds*

DETAILED STEPS

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 7: 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.

Example Outputs	Description
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 8: Special Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
^	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 9: Special Characters Used for Anchoring

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

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

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

Searching and Filtering show Command Output

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

```
switch# show running-config | ?
  cut      Print selected parts of lines.
  diff     Show difference between current and previous invocation (creates temp files:
           remove them with 'diff-clean' command and don't use it on commands with big
           outputs, like 'show tech'!)
  egrep    Egrep - print lines matching a pattern
  grep     Grep - print lines matching a pattern
  head     Display first lines
  human    Output in human format
  last     Display last lines
  less     Filter for paging
  no-more  Turn-off pagination for command output
  perl     Use perl script to filter output
  section  Show lines that include the pattern as well as the subsequent lines that are
           more indented than matching line
  sed      Stream Editor
  sort     Stream Sorter
  sscp     Stream SCP (secure copy)
  tr       Translate, squeeze, and/or delete characters
  uniq     Discard all but one of successive identical lines
  vsh      The shell that understands cli command
  wc       Count words, lines, characters
  begin    Begin with the line that matches
  count    Count number of lines
  end      End with the line that matches
  exclude  Exclude lines that match
  include  Include lines that match
```

Filtering and Searching Keywords

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

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

Table 10: Filtering and Searching Keywords

Keyword Syntax	Description

begin *string*
Example:
`show version | begin Hardware`
	Starts displaying at the line that contains the text that matches the search string. The search string is case sensitive.

count **Example:** `show running-config | count`	Displays the number of lines in the command output.

cut [**-d** *character*] {**-b** | **-c** | **-f** | **-s**}
Example:
`show file testoutput | cut -b 1-10`
	Displays only part of the output lines. You can display a number of bytes (**-b**), characters (**-vcut** [**-d** *character*] {**-b** | **-c** | **-f** | **-s**}), or fields (**-f**). You can also use the **-d** keyword to define a field delimiter other than the tag character default. The **-s** keyword suppresses the display of the lines that do not contain the delimiter.

end *string*
Example:
`show running-config | end interface`
	Displays all lines up to the last occurrence of the search string.

exclude *string* **Example:** `show interface brief | exclude down`	Displays all lines that do not include the search string. The search string is case sensitive.
head [**lines** *lines*] **Example:** `show logging logfile | head lines 50`	Displays the beginning of the output for the number of lines specified. The default number of lines is 10.
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.

Keyword Syntax	Description
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.

diff Utility

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

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

This table describes the keywords for the diff utility.

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

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

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

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

grep and egrep Utilities

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

The grep and egrep syntax is as follows:

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

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

Table 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 utility parameters.

Table 12: sort Utility Parameters

Parameter	Description
-M	Sorts by month.

Parameter	Description
-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.

sscp Utility

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 Secure Shell (SSH) connection before using the **sscp** command.

You can create an SSH connection by using the ssh name command. Password is specified only once at the time of creation of the ssh-primary-connection. So, you do not have to enter the password again. SSH server should support the **cat** command. If the SSH server is running on a Windows system, you must copy the cat.exe file from the binutils of GNU into the Windows path. The **sscp** command is used at the end of the pipe (|).

This command does not require a license.

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

```
switch# ssh name mybox admin 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
      ...

admin@172.23.152.34's password:
switch# show version | sscp mybox /users/admin/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.
[*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.

Commands	Description
{**!** | **:!**[*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.

SUMMARY STEPS

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

DETAILED STEPS

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. 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.

Displaying the Command History

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

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

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

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

```
switch# show cli history
```

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

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

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

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

Enabling or Disabling the CLI Confirmation Prompts

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

SUMMARY STEPS

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

DETAILED STEPS

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 set by the terminal emulator software.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

Sending Commands to Modules

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

The **slot** has the following syntax:

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

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

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

This example shows how to display and filter module information:

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

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

```
switch# slot 2 quoted "show version" | diff
switch# slot 4 quoted "show version" | diff -c
```

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

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

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

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

BIOS Loader Prompt

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

```
loader>
```

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

Examples Using the CLI

This section includes examples of using the CLI.

Defining Command Aliases

This example shows how to define command aliases:

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

This example shows how to use a command alias:

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

Using CLI Session Variables

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

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

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

Using the System-Defined Timestamp Variable

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

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

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

Running a Command Script

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

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

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

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

Using the sscp Utility to Redirect show Command Output

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

```
switch# ssh name MyConnection MyId 172.28.255.18

                                 WARNING!!!
                    READ THIS BEFORE ATTEMPTING TO LOGON

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

MyId@172.28.255.18's password:
switch# show version | sscp MyConnection show_version_output
switch#
```

CHAPTER 6

Configuring Terminal Settings and Sessions

This chapter describes how to configure terminal settings and sessions.

- Information About Terminal Settings and Sessions, on page 69
- Configuring the Console Port, on page 71
- Configuring the COM1 Port, on page 73
- Configuring Virtual Terminals , on page 74
- Configuring Modem Connections, on page 77
- Clearing Terminal Sessions, on page 81
- Displaying Terminal and Session Information, on page 82
- Default Settings for Terminal Display and Session Parameters, on page 82

Information About Terminal Settings and Sessions

This section includes information about terminal settings and sessions.

Terminal Session Settings

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

Terminal type
Name used by Telnet when communicating with remote hosts

Length
Number of lines of command output displayed before pausing

Width
Number of characters displayed before wrapping the line

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

Console Port

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

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

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

Parity
Specifies the odd or even parity for error detection.

Speed
Specifies the transmission speed for the connection.

Stop bits
Specifies the stop bits for an asynchronous line.

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

COM1 Port

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

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

Hardware flowcontrol
Enables the flow-control hardware.

Parity
Specifies the odd or even parity for error detection.

Speed
Specifies the transmission speed for the connection.

Stop bits
Specifies the stop bits for an asynchronous line.

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

Virtual Terminals

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

Modem Support

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

- MultiTech MT2834BA
- Hayes Accura V.92

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

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

AT
Attention

E0 (required)
No echo

Q1
Result code on

&D2
Normal data terminal ready (DTR) option

&C1
Enable tracking the state of the data carrier

S0=1
Pick up after one ring

\015 (required)
Carriage return in octal

Configuring the Console Port

You can set the following characteristics for the console port:

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

Before you begin

Log in to the console port.

SUMMARY STEPS

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

DETAILED STEPS

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 **9600**.

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

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

Step 9	(Optional) **show line console** **Example:** `switch(config)# show line console`	Displays the console settings.

	Command or Action	Purpose
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring the COM1 Port

You can set the following characteristics for the COM1 port:

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

Before you begin

Log in to the console port or COM1 port.

SUMMARY STEPS

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

DETAILED STEPS

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

Step 3	**databits** *bits* **Example:** `switch(config-com1)# databits 7`	Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.
Step 4	**flowcontrol hardware** **Example:** `switch(config-com1)# flowcontrol hardware`	Enables flow control on the hardware. The default is enabled. Use the **no flowcontrol hardware** command to disable flow control on the hardware.

Step 5	**parity** {**even** | **none** | **odd**}
	Example:
	`switch(config-com1)# parity even`
		Configures the parity. The default is **none**.

Step 6	**speed** {**300** | **1200** | **2400** | **4800** | **9600** | **38400** | **57600** | **115200**}
	Example:
	`switch(config-com1)# speed 115200`
		Configures the transmit and receive speed. The default is **9600**.

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

Configuring Virtual Terminals

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

Configuring the Inactive Session Timeout

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

SUMMARY STEPS

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

DETAILED STEPS

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*
	• **absolute-timeout** *minutes*
	Example:
	`switch(config-line)# exec-timeout 30`
	Example:
	`switch(config-line)# absolute-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.
		Sets a timeout interval on a virtual terminal (vty) line. The range is from 0 to 10000.
		The **absolute-timeout** command terminates the connection after the specified time period has elapsed, regardless of whether the connection is being used at the time of termination. You can specify an absolute-timeout value for each port. The user is given 20 seconds notice before the session is terminated. You can use this command along with the **logout-warning** command, which notifies the user of an impending logout.

Step 4	**exit** **Example:**	Exits line configuration mode.

	Command or Action	Purpose

	`switch(config-line)# exit`
	`switch(config)#`	

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

Configuring the Session Limit

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

SUMMARY STEPS

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

DETAILED STEPS

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.

	Command or Action	Purpose

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

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

Configuring Modem Connections

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

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

Enabling a Modem Connection

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

Before you begin

Log in to the console port.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

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

Downloading the Default Initialization String

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

Before you begin

Log in to the console port.

SUMMARY STEPS

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

6. (Optional) **copy running-config startup-config**

DETAILED STEPS

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

Configuring and Downloading a User-Specified Initialization String

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

Before you begin

Log in to the console port.

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Before you begin

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

Enable the modem connection on the port.

SUMMARY STEPS

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

DETAILED STEPS

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 77

Clearing Terminal Sessions

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

SUMMARY STEPS

1. (Optional) **show users**

2. **clear line** *name*

DETAILED STEPS

Procedure

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

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
Terminal width	80 columns

Parameters	Default
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 7

Basic Device Management

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

- Information About Basic Device Management, on page 85
- Changing the Device Hostname, on page 87
- Configuring the Management Interface, on page 88
- Configuirng the Default Gateway, on page 89
- Configuring the MOTD Banner, on page 90
- Configuring the Time Zone, on page 91
- Configuring Summer Time (Daylight Saving Time), on page 92
- Manually Setting the Device Clock, on page 93
- Managing Users, on page 94
- Enabling or Disabling a Telnet Server Connection, on page 95
- Secure Erase, on page 96
- Verifying the Device Configuration, on page 98
- Default Settings for Basic Device Parameters, on page 98

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.

Interface

Note If the management 10/100 Ethernet port (mgmt0) interface of the Cisco MDS 9700 Series switches has a preconfigured /0 IPv6 address that cannot be removed, use the **write erase boot** command to clear the complete configuration of the device and reload it. Perform this process before commissioning the device into production as this process is disruptive to user traffic if it is applied to the active supervisor of a system. Ensure an active console connection to the supervisor as this process will remove the IPv4 address of the mgmt0 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.

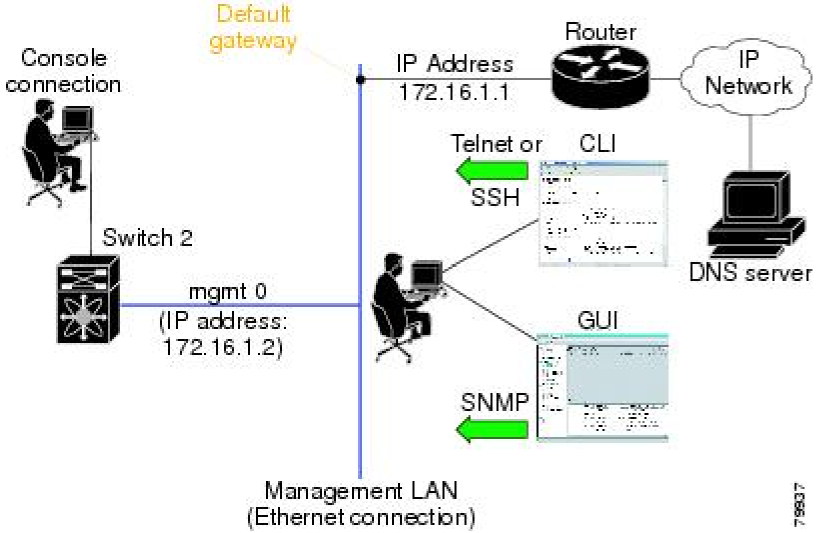
On devices with dual supervisor modules, a single IP address is used to manage the switch. The active supervisor module's mgmt0 interface uses this IP address. The mgmt0 interface on the standby supervisor module remains in an inactive state and cannot be accessed until a switchover happens. After a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

Default Gateway

Figure 7: Default Gateway

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



Message-of-the-Day Banner

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

Device Clock

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

Time Zone and Summer Time (Daylight Saving Time)

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

User Sessions

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

Telnet Server Connection

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

Note For information on connecting a terminal to the supervisor module console port, refer to the *Cisco MDS 9200 Series Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide*.

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

Changing the Device Hostname

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

SUMMARY STEPS

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

DETAILED STEPS

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 63 characters. The default name 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	(Optional) **copy running-config startup-config** **Example:** `Engineering2# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring the Management Interface

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

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

Before you begin

Establish a connection on the console port.

SUMMARY STEPS

1. **configure terminal**
2. **interface mgmt 0**

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

DETAILED STEPS

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

SUMMARY STEPS

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

DETAILED STEPS

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	(Optional) **show ip route** **Example:** `switch(config)# show ip route`	Displays the default gataeway configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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 254 characters per line
- Maximum of 40 lines

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Configuring the Time Zone

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

SUMMARY STEPS

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

DETAILED STEPS

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.

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

Configuring Summer Time (Daylight Saving Time)

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

SUMMARY STEPS

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

DETAILED STEPS

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.

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

Manually Setting the Device Clock

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

Before you begin

Configure the time zone.

SUMMARY STEPS

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

DETAILED STEPS

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

Related Topics

Configuring the Time Zone, on page 91

Managing Users

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

Displaying Information about the User Sessions

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

SUMMARY STEPS

1. **show users**

DETAILED STEPS

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.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

Enabling or Disabling a Telnet Server Connection

You can enable or disable the Telnet server connection.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	[**no**] **feature telnet** **Example:** `switch(config)# feature telnet`	Enables the Telnet server connection. Use the **no** form of the command to disable the Telnet server connection. The default is disabled.
Step 3	(Optional) **show telnet server** **Example:** `switch(config)# show telnet server`	Displays the Telnet server configuration.

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

Secure Erase

The Secure Erase feature allows erasure of all customer information from Cisco MDS switches. Cisco MDS switches can store software images, switch configuration, software logs, and operational history. The information stored can have customer-specific information such as details of network architecture, user credentials, and customer data which can be a potential target for data theft.

The Secure Erase feature is useful in the following scenarios:

- Returning a device: If you must return a device to your supplier for replacement.
- Recovering a compromised device: If the key information or credentials that are stored on a device are compromised, to reset the device to factory configuration and reconfigure it.
- Decommissioning a device: If a device is being removed from service as part of redeployment or end of life where the device may leave the security of the data center.

Prerequisites for Performing Secure Erase

- Ensure that all the software images, configurations, personal data, and so on, are backed up (if required) before performing the secure erase operation.
- Ensure that power is not interrupted while the secure erase process is in progress otherwise the erasure will not be completed.

- Ensure that neither In-Service Software Upgrade (ISSU) nor In-Service Software Downgrade (ISSD) is in progress before starting the secure erase process.

Guidelines and Limitations for Secure Erase

- The secure erase process is disruptive for any network traffic traversing the target device. Ensure that alternate links or paths are active for data traffic if this operation is done on an in-service device.
- After secure erase process is finished, the behavior is different for fabric and modular switches:
  - For supervisors in Director switches and for fabric switches, the device remains at the *loader* prompt.
  - For linecards in Director switches, the linecards will be powered down.
- Erasing a Director switch's active supervisor or any fabric switch will cause remote connectivity to be permanently lost. To verify when the process has completed and that there were no errors, execute the command on the console session. However, erasure of Director linecards and standby supervisor may be started and monitored from an SSH session.

Performing Secure Erase

Modules in Director switches must be erased individually. To erase all modules on a Director switch, erase them in the order of 1) linecards, 2) standby supervisor, and 3) active supervisor.

To securely erase all information on a Director module, perform this step:

Erase all data on a module:

switch# **factory-reset module** *number*

After the erasure process, the module will remain at the *loader* prompt if it is a supervisor and in the powered down state if it is a linecard.

If the module is a linecard that is being replaced, the new linecard will need to be powered up after it is inserted into the slot, as follows:

1. Enter global configuration mode:

   switch# **configure t**

2. Power up the linecard:

   Switch(config)# **no poweroff module** *number*

Fabric switches are single module switches and do not require the **module** option. To securely erase all information on a fabric switch, perform this step:

Erase all data on the switch:

switch# **factory-reset**

After the erasure process, the switch will remain at the *loader* prompt.

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

CHAPTER 8

Using the Device File Systems, Directories, and Files

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

- Information About Device File Systems, Directories, Files, and External Storage Devices, on page 99
- Working with External Storage Devices, on page 101
- Working with Directories, on page 102
- Working with Files, on page 104
- Working with Archive Files, on page 107
- Examples of Using a File System, on page 109

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

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

File Systems

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

Note The default *filesystem* parameter is bootflash:.

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

Table 16: File System Components

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

Directories

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

Files

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

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

Working with External Storage Devices

This section describes formatting, mounting, and unmounting of external storage devices on devices.

Formatting an External Flash Device

Insert the external flash device into the active supervisor module in a Cisco MDS device.

To format an external flash device, run the following command:

format {**slot0:** | **usb1:** | **usb2:**}

Example:

```
switch# format slot0:
```

Note You can format an external flash device to erase its contents and restore the device to its factory-shipped state. For information about recovering corrupted bootflash using formatting, see the .

Mounting or Unmounting a USB Drive

Mount or unmount a USB drive automatically by plugging or unplugging the drive from a Cisco MDS device. You can also use the **mount** or **unmount** command in either the user EXEC mode or the privileged EXEC mode to mount or unmount the device, respectively.

- To mount a USB drive on a Cisco MDS device, run the following command:

  mount {**usb1:** | **usb2:**}

  Example:

  ```
  switch# mount usb1:
  ```

- To unmount a USB drive from a Cisco MDS device, run the following command:

  unmount {**usb1:** | **usb2:**}

  Example:

  ```
  switch# unmount usb1:
  ```

External Storage Device Support Matrix

This section provides information about hardware and software support for external storage device ports on each type of Cisco MDS platform.

Cisco MDS switches support devices formatted with the FAT32 file system.

Platform	PCMCIA	USB[1]			
	slot0	First supported	slot0	usb1	usb2
Cisco MDS 9700 Series Multilayer Director	No hardware port	Cisco MDS NX-OS Release 6.2(1)	Enabled	Enabled	No hardware port
Cisco MDS 9500 Series Multilayer Director	Enabled	Cisco MDS NX-OS Release 6.2(1)	No hardware port	Enabled	Enabled
Cisco MDS 9396S 16G Multilayer Fabric Switch	No hardware port	Cisco MDS NX-OS Release 6.2(13)	No hardware port	Enabled	No hardware port
Cisco MDS 9250i Multiservice Fabric Switch	No hardware port	Cisco MDS NX-OS Release 6.2(15)	No hardware port	Enabled	No hardware port
Cisco MDS 9222i Multiservice Modular Switch	No hardware port	—	No hardware port	No hardware port	No hardware port
Cisco MDS 9148S 16G Multilayer Fabric Switch	No hardware port	Cisco MDS NX-OS Release 6.2(15)	No hardware port	Enabled	No hardware port
Cisco MDS 9148 Multilayer Fabric Switch	No hardware port	—	No hardware port	No hardware port	No hardware port
Cisco MDS 8Gb Fabric Switch for HP BladeSystem c-Class	No hardware port	—	No hardware port	No hardware port	No hardware port

[1] USB 2.0 or higher devices supported.

Working with Directories

Identifying the Current Directory

To display the name of the current directory, run the following command:

pwd

Example:

```
switch# pwd
```

Changing the Current Directory

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

Note The file system, module, and directory names are case sensitive.

To change to a new directory, run the following command:

cd {*directory* | *filesystem***:**[//*module*/][*directory*]}

Example:

```
switch# cd slot0:
```

Creating a Directory

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

Note

- The file system, module, and directory names are case sensitive.
- The *filesystem* argument is case sensitive. The *directory* argument is alphanumeric, case sensitive, and can have a maximum of 64 characters.

To create a new directory, run the following command:

mkdir [*filesystem***:**[//*module*/]]*directory*

Example:

```
switch# mkdir test
```

Displaying Directory Contents

To display the contents of a directory, run the following command:

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

Example:

```
switch# dir bootflash:
```

Deleting a Directory

You can remove directories from the file systems on a Cisco MDS device.

Note

- Ensure that the directory is empty before you delete it. If the directory is not empty, you must delete all the files before you delete the directory.
- The file system and directory names are case sensitive.

To delete a directory, run the following command:

rmdir [*filesystem* **:**[*//module/*]]*directory*

Example:

```
switch# rmdir test
```

Accessing the Directories on a Standby Supervisor Module

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

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

Working with Files

Moving a File

Files can be moved from one directory to another directory.

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

Note The file system, module, and directory names are case sensitive.

To move a file from one directory to another directory, run the following command:

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

Example:

```
switch# move test old_tests/test1
```

Note The *target-filename* argument is alphanumeric, case sensitive, and can have a maximum of 64 characters. If the *target-filename* argument is not specified, the filename defaults to the *source-filename* argument value.

Caution When you try to move a file from one directory to another, if a file with the same name already exists in the destination directory, that file is overwritten by the moved file.

Copying a File

You can make copies of files, either within the same directory or in 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 the files that are no longer required.
- The file system, module, and directory names are case sensitive.

To copy a file, run the following command:

copy [*filesystem*:[//*module*/][*directory*/] | *directory*/]*source-filename* | {*filesystem*:[//*module*/][*directory*/]] | *directory*/}[*target-filename*]

Example:

```
switch# copy test old_tests/test1
```

Note

- The *source-filename* argument is alphanumeric, case sensitive, and can have a maximum of 64 characters. If the *target-filename* argument is not specified, the filename defaults to the *source-filename* argument value.
- The **copy** command supports FTP, SCP, SFTP, TFTP, and HTTP protocols.

Deleting a File

Caution If you specify a directory, the **delete** command deletes the entire directory and all of its contents.

Note The file system name, directory name, and *source-filename* argument are case sensitive.

To delete a file, run the following command:

delete {*filesystem*:[//*module*/][*directory*/] | *directory*/}*filename*

Example:

```
switch# delete test old_tests/test1
```

Displaying a File's Contents

To display a file's contents, run the following command:

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

Example:

```
switch# show file bootflash:test-results
```

Displaying a File's Checksums

You can use checksums to verify a file's integrity.

To display the checksum or MD5 checksum of a file, run the following command:

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

Example:

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

Compressing and Uncompressing a File

You can compress and uncompress the files on a device using Lempel-Ziv 77 (LZ77) coding.

Note The file system and directory names are case sensitive.

- To compress a file, run the following command:

  gzip [*filesystem*:[//*module*/][*directory*/] | *directory*/]*filename*

  Example:

  ```
  switch# gzip show_tech
  ```

  Note After a file is compressed, it has a .gz suffix.

- To uncompress a file, run the following command:

  gunzip [*filesystem*:[//*module*/][*directory*/] | *directory*/]*filename* **.gz**

  Example:

  ```
  switch# gunzip show_tech.gz
  ```

  Note The file that has be uncompressed must have the .gz suffix. After the file is uncompressed, it does not have the .gz suffix.

- To display the contents of the current directory, run the following command:

  dir [*filesystem* :[//*module*/][*directory*]]

  Example:

  ```
  switch# dir bootflash:
  ```

Displaying the Last Lines in a File

Note The default number of lines is 10. The range is from 0 to 80 lines.

To display the last lines in a file, run the following command:

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

Example:

```
switch# tail ospf-gr.conf
```

Redirecting show Command Output to a File

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

To redirect the output from a **show** command to a file, run the following command:

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

Example:

```
switch# show tech-support > bootflash:techinfo
```

Finding Files

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

To find all the files beginning with the filename prefix in the default directory and in its subdirectories, run the following command:

find *filename-prefix*

Example:

```
switch# find bgp_script
```

Note The filename prefix is case sensitive.

Working with Archive Files

Creating an Archive File

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

- bzip2
- gzip

- Uncompressed

The default compression type is gzip.

Note The filename is alphanumeric, not case sensitive, and can have a maximum of 240 characters.

To create an archive file and add files to it, run the following command:

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

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

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

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 to use 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 default extensions are as follows:

- For **bz2-compress**, the extension is .tar.bz2.
- For **gz-compress**, the extension is .tar.gz.
- For **uncompressed**, the extension is .tar.

The **remove** keyword specifies that the software should delete the files from the file system after adding them to the archive. By default, the files are not deleted.

The **verbose** keyword specifies that the software should list the files as they are added to the archive. By default, the files are listed as they are added.

Appending Files to an Archive File

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

Note The archive filename is not case sensitive.

To add files to an existing archive file, run the following command:

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

Example:

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

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 software should delete the files from the file system after adding them to the archive. By default, the files are not deleted.

The **verbose** keyword specifies that the software should list the files as they are added to the archive. By default, the files are listed as they are added.

Extracting Files from an Archive File

You can extract files from an existing archive file on a device.

Note The archive filename is not case sensitive.

To extract files from an existing archive file, run the following command:

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

Example:

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

The **keep-old** keyword indicates that the software should not overwrite files with the same name as the files being extracted.

The **screen** keyword specifies that the software should display the contents of the extracted files to the terminal screen.

The **to** keyword specifies the target file system. You can include a directory name. The directory name is alphanumeric, case sensitive, and can have a maximum of 240 characters.

The **verbose** keyword specifies that the software should display the names of the files as they are extracted.

Displaying the Filenames in an Archive File

Note The archive filename is not case sensitive.

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

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

Example:

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

Examples of Using a File System

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

Accessing Directories on a Standby Supervisor Module

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

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

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

Performing ISSU or ISSD Using a USB Drive

This example shows how to perform an In-Service Software Upgrade (ISSU) or In-Service Software Downgrade (ISSD) using a system image or kickstart image from a USB drive:

```
switch# install all system usb1:m9300-s1ek9-mzg.6.2.13.FM.0.65.bin.S0 kickstart
usb1:m9300-s1ek9-kickstart-mzg.6.2.13.FM.0.65.bin.S0
```

CHAPTER 9

Working with Configuration Files

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

- Information About Configuration Files, on page 111
- Managing Configuration Files, on page 112
- Verifying the Device Configuration, on page 122
- Examples of Working with Configuration Files, on page 122

Information About Configuration Files

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

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

Types of Configuration Files

The Cisco NX-OS software has two types of configuration files, running configuration and startup configuration. The device uses the startup configuration (startup-config) during device startup to configure the software features. The running configuration (running-config) contains the current changes that you make to the startup-configuration file. The two configuration files can be different. You might want to change the device configuration for a short time period rather than permanently. In this case, you would change the running configuration by using commands in global configuration mode but not save the changes to the startup configuration.

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

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

Related Topics

About Command Modes

Saving the Running Configuration to the Startup Configuration, on page 112
Downloading the Startup Configuration From a Remote Server, on page 114

Managing Configuration Files

This section describes how to manage configuration files.

Saving the Running Configuration to the Startup Configuration

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

Copying a Configuration File to a Remote Server

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

SUMMARY STEPS

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

DETAILED STEPS

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. 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.

Example

Downloading the Running Configuration From a Remote Server

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

Before you begin

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

Related Topics

Copying Files

Downloading the Startup Configuration From a Remote Server

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

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

Before you begin

Log in to a session on the console port.

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**write erase** **Example:** `switch# write erase`	Erases the startup configuration file.

Step 2	**reload**
	Example:
	`switch# reload`
	`This command will reboot the system. (y/n)?  [n] y`
	`...`
	`Enter the password for "admin": <password>`
	`Confirm the password for "admin": <password>`
	`...`
	`Would you like to enter the basic configuration dialog (yes/no): n`
	`switch#`
		Reloads the Cisco NX-OS device.
		Note
		Do not use the setup utility to configure the device.

Step 3	**copy** *scheme*://*server*/[*url* /]*filename* **running-config** **Example:** `switch# copy tftp://10.10.1.1/my-config running-config`	Downloads the running configuration file from a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.
Step 4	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Saves the running configuration file to the startup configuration file.

	Command or Action	Purpose
Step 5	(Optional) **show startup-config** **Example:** `switch# show startup-config`	Displays the running configuration.

Related Topics

Copying Files

Copying Configuration Files to an External Flash Memory Device

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

Before you begin

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	(Optional) **dir** {**slot0:** | **usb1:** | **usb2:**}[*directory/*] **Example:** `switch# dir slot0:`	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

Copying the Running Configuration from an External Flash Memory Device

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

Before you begin

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

Related Topics

Copying Files

Copying the Startup Configuration from an External Flash Memory Device

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

Before you begin

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	(Optional) **dir** {**slot0:** | **usb1:** | **usb2:**}[*directory/*] **Example:** `switch# dir slot0:`	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	(Optional) **show startup-config** **Example:** `switch# show startup-config`	Displays the startup configuration.

Related Topics

Copying Files

Copying Configuration Files to an Internal File System

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

SUMMARY STEPS

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

DETAILED STEPS

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

Rolling Back to a Previous Configuration

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

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**write erase** **Example:**	Clears the current configuration of the switch.

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

Removing the Configuration for a Missing Module

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

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

Before you begin

Remove the I/O module from the chassis.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

Erasing a Configuration

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

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

- Startup
- Boot
- Debug

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**write erase boot** **Example:** `switch# write erase boot`	Erases the boot variable definitions.
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. By default, the reload command reloads the device from a binary version of the startup configuration.
Step 3	**write erase** **Example:** `switch# write erase`	Erases the boot variable definitions.
Step 4	**write erase boot** **Example:** `switch# write erase boot`	Erases the boot variable definitions and the IPv4 configuration on the management interface.
Step 5	**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. By default, the reload command reloads the device from a binary version of the startup configuration.

Verifying the Device Configuration

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

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

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

Examples of Working with Configuration Files

This section includes examples of working with configuration files.

Copying Configuration Files

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

Backing Up Configuration Files

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

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

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

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

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

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

Rolling Back to a Previous Configuration

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

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

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

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

CHAPTER 10

Configuring CDP

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

- Information About CDP, on page 125
- Configuring CDP, on page 126
- Verifying the CDP Configuration, on page 128
- Clearing CDP Counters and Tables, on page 129
- CDP Example Configuration, on page 129
- Default Settings for CDP, on page 129

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.

Note CDP is not supported on NPV devices.

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 .

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.

SUMMARY STEPS

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

DETAILED STEPS

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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves this configuration change.

Enabling or Disabling CDP on an Interface

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

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

Before you begin

Ensure that CDP is enabled on the device.

SUMMARY STEPS

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

DETAILED STEPS

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 ethernet 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	(Optional) **show cdp interface** *interface-type slot/port* **Example:** `switch(config-if)# show cdp interface ethernet 1/2`	Displays CDP information for an interface.

Step 5	(Optional) **copy running-config startup-config**
	Example:
	`switch(config-if)# copy running-config`
	`startup-config`
		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.

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 17: CDP Default Settings

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

CHAPTER 11

Configuring LLDP

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

- About LLDP, on page 131
- Platforms Supported, on page 133
- Guidelines and Limitations for LLDP, on page 133
- Default Settings for LLDP, on page 134
- Configuring LLDP, on page 134
- Verifying the LLDP Configuration, on page 137
- Configuration Example for LLDP, on page 138

About LLDP

The Cisco Discovery Protocol (CDP) is a device discovery protocol that allows network management applications to automatically discover and learn about other Cisco devices that are connected to the network.

To permit the discovery of non-Cisco devices, the switch also supports the Link Layer Discovery Protocol (LLDP), a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP is a one-way protocol that transmits information about the capabilities and status of a device and its interfaces. LLDP devices use the protocol to solicit information only from other LLDP devices.

LLDP supports a set of attributes that it uses to discover other devices. These attributes contain type, length, and value (TLV) descriptions. LLDP devices can use TLVs to send and receive information to other devices on the network. Details such as configuration information, device capabilities, and device identity can be advertised using this protocol.

LLDP advertises the following TLVs by default:

- DCBXP
- Management address
- Port description
- Port VLAN

- System capabilities
- System description
- System name

About DCBX

The Data Center Bridging Exchange Protocol (DCBXP) is an extension of LLDP. It is used to announce, exchange, and negotiate node parameters between peers. DCBXP parameters are packaged into a specific DCBXP TLV. This TLV is designed to provide an acknowledgement to the received LLDP packet. In this way, DCBXP adds a lightweight acknowledgement mechanism on top of LLDP so that any application that needs a request-response semantic from a link-level protocol can make use of DCBXP.Other applications that need to exchange and negotiate parameters with peer nodes using DCBXP are as follows:

- Priority-based Flow Control (PFC)—PFC is an enhancement to the existing Pause mechanism in Ethernet. It enables Pause based on user priorities or classes of service. A physical link divided into eight virtual links with PFC provides the capability to use Pause on a single virtual link without affecting traffic on the other virtual links. Enabling Pause on a per-user-priority basis allows administrators to create lossless links for traffic requiring no-drop service while retaining packet-drop congestion management for IP traffic.
- Enhanced Transmission Selection (ETS)—ETS enables optimal bandwidth management of virtual links. ETS is also called priority grouping. It enables differentiated treatments within the same priority classes of PFC. ETS provides prioritized processing based on bandwidth allocation, low latency, or best effort, resulting in per-group traffic class allocation. For example, an Ethernet class of traffic may have a high-priority designation and a best effort within that same class. ETS allows differentiation between traffic of the same priority class, thus creating priority groups.
- Application Priority Configuration TLV—Carries information about which VLANs will be used by specific protocols.

Note For information on the quality of service (QoS) features, see the *Cisco MDS 9000 Series Quality of Service Configuration Guide, Release 9.x*.

DCBXP is enabled by default, provided LLDP is enabled. When LLDP is enabled, DCBXP can be enabled or disabled using the [**no**] **lldp tlv-select dcbxp** command. DCBXP is disabled on ports where LLDP transmit or receive is disabled.

High Availability

The LLDP feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied.

For more information on high availability, see the *Cisco MDS 9000 Series High Availability Configuration Guide, Release 9.x*.

Virtualization Support

One instance of LLDP is supported.

Platforms Supported

- Cisco MDS 9700 series
- Cisco MDS 9148S
- Cisco MDS 9148T
- Cisco MDS 9148V
- Cisco MDS 9132T
- Cisco MDS 9396S
- Cisco MDS 9396T
- Cisco MDS 9396V
- Cisco MDS 9124V
- Cisco MDS 9220i
- Cisco MDS 9250i

Guidelines and Limitations for LLDP

LLDP has the following configuration guidelines and limitations:

- LLDP feature is enabled by default in MDS 9700 series and MDS 9250i fabric switch.LLDP feature needs to be enabled on all other MDS switches to use the LLDP support on management interfaces.
- LLDP feature cannot be disabled on on MDS 9250i and MDS 9700 series.
- LLDP must be enabled on the device before you can enable or disable it on any interfaces.
- LLDP is supported only on physical interfaces.
- LLDP can discover up to one device per port.
- LLDP can discover Linux servers, provided they are not using a converged network adapter (CNA). LLDP cannot discover other types of servers.
- DCBXP incompatibility messages might appear when you change the network QoS policy if a physical loopback connection is in the device. The incompatibility exists for only a short time and then clears.
- DCBXP is supported only on FCoE ports not on Management ports.
- LLDP is supported forFCoEon MDS 9700 series and MDS 9250i Multiservice Fabric Switch.
- LLDP is supported on management port (management port 0) for all the MDS switches.
- From Cisco MDS NX-OS Release 9.4(1), ensure that the LLDP feature is disabled before you perform the downgrade to target releases on all MDS switches except MDS 9250i Mutliservice Fabric Switch and MDS 9700 series
- LLDP is not supported on IPS ports.

Default Settings for LLDP

This table lists the LLDP default settings.

Parameters	Default
Global LLDP	Disabled
LLDP on interfaces	Enabled, after LLDP is enabled globally
LLDP hold time (before discarding)	120 seconds
LLDP reinitialization delay	2 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP TLVs	Enabled
LLDP receive	Enabled, after LLDP is enabled globally
LLDP transmit	Enabled, after LLDP is enabled globally
DCBXP	Enabled, provided LLDP is enabled

Configuring LLDP

Note Cisco NX-OS commands for this feature may differ from Cisco IOS commands for a similar feature.

Enabling or Disabling LLDP Globally

You can enable or disable LLDP globally on a device. You must enable LLDP globally to allow a device to send and receive LLDP packets.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# [**no**] **feature lldp**	Enables or disables LLDP on the device. LLDP is disabled by default.
Step 3	(Optional) switch(config)# **show running-config lldp**	Displays the global LLDP configuration. If LLDP is enabled, it shows "feature lldp." If LLDP is disabled, it shows an "Invalid command" error.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Enabling or Disabling LLDP on an Interface

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

Before you begin

Make sure that you have globally enabled LLDP on the device.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *interface slot*/*port*
3. switch(config-if)# [**no**] **lldp transmit**
4. switch(config-if)# [**no**] **lldp receive**
5. (Optional) switch(config-if)# **show lldp interface** *interface slot*/*port*
6. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *interface slot*/*port*	Specifies the interface on which you are enabling LLDP and enters the interface configuration mode.
Step 3	switch(config-if)# [**no**] **lldp transmit**	Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
Step 4	switch(config-if)# [**no**] **lldp receive**	Enables or disables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.

	Command or Action	Purpose
Step 5	(Optional) switch(config-if)# **show lldp interface** *interface slot/port*	Displays the LLDP configuration on the interface.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Configuring Optional LLDP Parameters

You can configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets.

SUMMARY STEPS

1. switch# **configure terminal**
2. (Optional) switch(config)# [**no**] **lldp holdtime** *seconds*
3. (Optional) switch(config)# [**no**] **lldp reinit** *seconds*
4. (Optional) switch(config)# [**no**] **lldp timer** *seconds*
5. (Optional) switch(config)# **show lldp timers**
6. (Optional) switch(config)# [**no**] **lldp tlv-set**
7. (Optional) switch(config)# **show lldp tlv-set**
8. (Optional) switch(config)# [**no**] **lldp tlv-select** *tlv*
9. (Optional) switch(config)# **show lldp tlv-select**
10. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	(Optional) switch(config)# [**no**] **lldp holdtime** *seconds*	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it. The range is 10 to 255 seconds; the default is 120 seconds.
Step 3	(Optional) switch(config)# [**no**] **lldp reinit** *seconds*	Specifies the delay time in seconds for LLDP to initialize on any interface. The range is 1 to 10 seconds; the default is 2 seconds.
Step 4	(Optional) switch(config)# [**no**] **lldp timer** *seconds*	Specifies the transmission frequency of LLDP updates in seconds. The range is 5 to 254 seconds; the default is 30 seconds.

	Command or Action	Purpose
Step 5	(Optional) switch(config)# **show lldp timers**	Displays the LLDP hold time, delay time, and update frequency configuration.
Step 6	(Optional) switch(config)# [**no**] **lldp tlv-set**	Sets the TLVs to send and receive in LLDP packets. The available TLVs are dcbxp, management-address, and port-vlan All available TLVs are enabled by default.
Step 7	(Optional) switch(config)# **show lldp tlv-set**	Displays the defined LLDP TLV configuration.
Step 8	(Optional) switch(config)# [**no**] **lldp tlv-select** *tlv*	Specifies the selected TLVs to send and receive in LLDP packets. The available TLVs are dcbxp, management-address, port-description, port-vlan, system-capabilities, system-description, and system-name. All available TLVs are enabled by default.
Step 9	(Optional) switch(config)# **show lldp tlv-select**	Displays the selected LLDP TLV configuration.
Step 10	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Verifying the LLDP Configuration

To display the LLDP configuration, perform one of the following tasks:

Command	Purpose
show running-config lldp	Displays the global LLDP configuration.
show lldp interface *interface slot*/*port*	Displays the LLDP interface configuration.
show lldp timers	Displays the LLDP hold time, delay time, and update frequency configuration.
show lldp tlv-set	Displays the defined LLDP TLV configuration.
show lldp tlv-select	Displays the selected LLDP TLV configuration.
show lldp dcbx interface *interface slot*/*port*	Displays the local DCBX control status.
show lldp neighbors {**detail** | **interface** *interface slot*/*port*}	Displays the LLDP neighbor device status.
show lldp traffic	Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.
show lldp traffic interface *interface slot*/*port*	Displays the number of LLDP packets sent and received on the interface.

Use the **clear lldp counters** command to clear the LLDP statistics.

Configuration Example for LLDP

This example shows how to enable LLDP on a device; disable LLDP on some interfaces; configure optional parameters such as hold time, delay time, and update frequency; and disable several LLDP TLVs:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature lldp
switch(config)# interface ethernet 7/9
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# interface ethernet 7/10
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# lldp holdtime 200
switch(config)# lldp reinit 5
switch(config)# lldp timer 50
switch(config)# no lldp tlv-select port-vlan
switch(config)# no lldp tlv-select system-name
```

CHAPTER 12

Configuring NTP

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

- Information About NTP, on page 139
- Prerequisites for NTP , on page 140
- Guidelines and Limitations for NTP, on page 141
- Configuring NTP, on page 141
- Verifying NTP, on page 151
- Troubleshooting NTP, on page 152
- Example: Configuring NTP, on page 155
- Default Settings for NTP, on page 156

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.

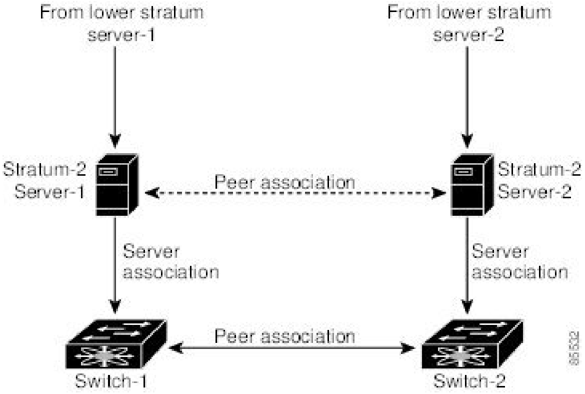
By configuring an IP address as a peer, the Cisco NX-OS device will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both of these instances point to different time servers, your NTP service is more reliable. Even if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

Figure 8: NTP Peer and Server Association

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.



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

Prerequisites for NTP

NTP has the following prerequisite:

- The switch should have IP connectivity to other NTP-enabled devices.

Guidelines and Limitations for NTP

NTP has the following configuration guidelines and limitations:

- You should allow a peer association with another device only when you are sure that the switch's clock is reliable (either it has a high quality local clock or the switch is itself 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 NTP

To enable NTP on a switch:

Note NTP is enabled by default.

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable NTP:

switch(config)# **feature ntp**

Disabling NTP

To disable NTP on a switch:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable NTP:

switch(config)# **no feature ntp**

Configuring Authentication Keys

The **ntp trusted-key** command provides protection against accidentally synchronizing the device to a time source that is not trusted. To synchronize a server device time zone with a client device time zone, the NTP authentication feature can be enabled only on the server device. To synchronize a client device time zone with a server device time zone, the NTP authentication feature must be enabled on both devices and the keys specified on the client device must be one of the keys specified on the server device. If the keys specified on the server device and the client device are different, then only the server device time zone can be synchronized with the client device time zone.

To configure the keys to be used to authenticate NTP associations, perform these steps:

Before you begin

Make sure that you configured the NTP server with the authentication keys that you plan to specify in this procedure.

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Define an authentication key:

switch(config)# **ntp authentication-key** *id* **md5** *key* [**0** | **7**]

The range for key *id* is from 1 to 65535. For the *key*, you can enter up to eight alphanumeric characters.

Step 3 Specify one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it:

switch(config)# **ntp trusted-key** *id*

The range for key *id* is from 1 to 65535.

What to do next

Enabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations, on page 143.

Enabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations

Temporary, symmetric, broadcast, or multicast updates (as opposed to server or peer updates) should be authenticated to prevent untrusted sources from injecting updates to devices.

To enable authentication of these types of NTP associations, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable NTP authentication of packets from new temporary, symmetric, broadcast, or multicast associations with remote network hosts (this does not authenticate peer associations that are created using the **ntp server** or **ntp peer** commands.):

switch# **ntp authenticate**

Disabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations

To disable authentication of these types of NTP associations, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable NTP authentication of packets from new temporary, symmetric, broadcast, or multicast associations with remote network hosts (this does not authenticate peer associations that are created using the **ntp server** or **ntp peer** commands.):

switch(config)# **no ntp authenticate**

NTP authentication is disabled by default.

Enabling NTP Servers and Peers

An NTP server is an authoritative source of NTP updates. The local device will follow the time of a server, but the server will not update from the local device's time. NTP peers send out updates and also adjust to incoming peer updates so that all peers converge to the same time. A device may have associations with multiple servers or peers.

NTP implements authentication through keys. Use NTP keys to filter exchanges to only trusted devices. This avoids trusting NTP updates from misconfigured or malicious sources.

To enable NTP server and peers, perform these steps:

Before you begin

Make sure that you know the IP address or Domain Name System (DNS) names of your NTP server and its peers.

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Form an association with a server:

switch(config)# **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *id*] [**prefer**] [**maxpoll** *interval*] [**minpoll** *interval*]

You can specify multiple server associations.

Use the **key** keyword to enable authentication with the named server using the specified key. The range for the *id* argument is from 1 to 65535.

Use the **prefer** keyword to make this server the preferred NTP server for the device.

Use the **maxpoll** and **minpoll** keywords to configure the maximum and minimum intervals in which to poll a server. The range for the *interval* is from 4 to 16 seconds, and the default values are 6 for maxpoll and 4 for minpoll.

Note
If you configure a key to be used while communicating with the NTP server, make sure that the key exists as a trusted key on the device.

Step 3 Form an association with a peer:

switch(config)# **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *id*] [**prefer**] [**maxpoll** *interval*] [**minpoll** *interval*]

You can specify multiple peer associations.

Use the **key** keyword to enable authentication with the named server using the specified key. The range for the *id* argument is from 1 to 65535.

Use the **prefer** keyword to make this peer the preferred NTP peer for the device.

Use the **maxpoll** and **minpoll** keywords to configure the maximum and minimum intervals in which to poll a peer. The range for the interval is from 4 to 17 seconds, and the default values are 6 for maxpoll and 4 for minpoll.

Note
If you configure a key to be used while communicating with the NTP peer, make sure that the key exists as a trusted key on the device.

Disabling NTP Servers and Peers

To disable NTP server and peers, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable an NTP server:

switch(config)# **no ntp server** {*ip-address* | *ipv6-address* | *dns-name*}

Step 3 Disable an NTP peer:

switch(config)# **no ntp peer** {*ip-address* | *ipv6-address* | *dns-name*}

Enabling NTP Modes

To enable processing of NTP control mode and private mode packets, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable the processing of control mode and private mode packets:

switch(config)# **ntp allow** {**private** | **control** [**rate-limit** *seconds*]}

The default time duration is 3 seconds, which means that a control mode packet is processed or responded every 3 seconds. Range is from 1 to 65535.

Disabling NTP Modes

To disable processing of NTP control mode and private mode packets, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable the processing of control mode and private mode packets:

switch(config)# **no ntp allow** {**private** | **control** [**rate-limit** *seconds*]}

Enabling NTP Source Interface

To override the default source address of NTP packets sent from the switch, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Override the default source address of NTP packets sent from the switch:

switch(config)# **ntp source-interface** {**ethernet** *slot/port.sub-interface* | **mgmt** *number* | **port-channel** *number*}

Only a single **ntp source-interface** command can be specified. All NTP packets sent through all interfaces will use the address specified by this command as the source address.

Disabling NTP Source Interface

To restore the default source address of NTP packets, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Restore the default source address of NTP packets:

switch(config)# **no ntp source-interface** {**ethernet** *slot/port.sub-interface* | **mgmt** *number* | **port-channel** *number*}

Enabling NTP Logging

To enable logging of NTP message to syslog, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable NTP logging:

switch(config)# **ntp logging**

Disabling NTP Logging

To disable logging of NTP message to syslog, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable NTP logging:

switch(config)# **no ntp logging**

Configuring NTP Syslog Logging Level

To configure the severity threshold of NTP syslog messages, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Configure the severity threshold of NTP syslog messages:

switch(config)# **logging level ntp** {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7**}

The following keywords specify the severity levels:

- **0**—Specifies to log emergency messages.
- **1**—Specifies to log alert messages.
- **2**—Specifies to log critical messages.

- **3**—Specifies to log error messages.
- **4**—Specifies to log warning messages.
- **5**—Specifies to log notification messages.
- **6**—Specifies to log informational messages.
- **7**—Specifies to log debugging messages.

Setting the Default NTP Syslog Severity Logging Level

To return to the default NTP syslog severity logging level, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Return to the default NTP syslog severity logging level:

switch(config)# **no logging level ntp** {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7**}

Displaying and Clearing NTP Statistics

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

To display and clear NTP statistics, perform these steps:

Procedure

Step 1 Display NTP statistics:

switch# **show ntp statistics** {**peers** | **io** | **local** | **memory**}

You can display the following NTP statistics:

- **peer**—NTP statistics per peer.
- **io**—Statistics of NTP packet handling.
- **local**—Statistics of NTP packet types.
- **memory**—Statistics of memory usage by NTP.

Step 2 Clear NTP statistics:

```
switch# clear ntp statistics {peer | io | local | memory}
```

Resynchronizing NTP

If the NTP client on a switch has lost synchronization with servers or peers, you may need to restart the NTP client. This will restart the synchronization process with all NTP servers and peers configured on the local switch. To check the status of NTP servers and clients, see the Troubleshooting NTP section.

To restart the NTP client on the switch, perform the following steps:

Procedure

Retry synchronization:

```
switch# ntp sync-retry
```

Distributing the NTP Configuration Using CFS

You can distribute local NTP configuration to other switches in the fabric using CFS.

Note Only NTP server and peer configuration is distributed through CFS.

Enabling NTP Configuration Distribution

To enable CFS distribution of NTP configuration, perform these steps:

Before you begin

- Ensure that CFS is enabled. For more information, see the "Verifying CFS Distribution Status" section in the "Cisco MDS 9000 Series System Management Configuration Guide."
- Ensure that NTP is enabled. For more information, see "Verifying NTP, on page 151."

Procedure

Step 1 Enter configuration mode:

```
switch# configure terminal
```

Step 2 Enable NTP configuration distribution to all switches in a fabric:

```
switch(config)# ntp distribute
```

This command acquires a fabric lock and stores all future configuration changes in the pending database.

Disabling NTP Configuration Distribution

To disable CFS distribution of NTP configuration, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable NTP configuration distribution:

switch(config)# **no ntp distribute**

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 a fabric that can receive NTP configuration distributions.

To apply pending NTP configuration to an NTP CFS enabled peers in a fabric, perform these steps:

Before you begin

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

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Distribute the pending NTP configuration to an NTP CFS enabled peers in the fabric:

switch(config)# **ntp commit**

Discarding NTP Configuration Changes

In NTP distribution mode, configuration changes are buffered until committed by the user. You can discard the changes before they are committed with the **abort** command.

To terminate and unlock the existing NTP CFS distribution session on a switch, perform these steps:

Procedure

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Terminate and unlock the existing NTP CFS distribution session on a switch:

switch(config)# **ntp abort**

Forcing Termination of a Lost NTP Configuration Session

When a user starts making NTP configuration changes in distribute mode, a session is created and CFS creates a fabric wide session lock. The session lock is to prevent other users from simultaneously creating sessions and making NTP configuration changes. If the user does not commit or cancel the changes, further NTP configuration sessions will be prevented until the lock is cleared. In this case, the session lock can be released by another user and this action causes all pending NTP configuration changes in the session to be discarded and the lock to be released. Releasing the session lock can be performed from any switch in the fabric. If the administrator performs this task, pending configuration changes are discarded and the fabric lock is released.

To use administrative privileges and release the locked NTP session, perform this step:

Procedure

Release the locked NTP session:

switch# **clear ntp session**

Verifying NTP

Use the following commands to verify NTP:

This example shows how to verify if NTP is enabled:

```
switch(config)# show running-config all | include "feature ntp"
feature ntp
```

This example shows how to display the current NTP configuration:

```
switch# show running-config ntp

!Command: show running-config ntp
!Time: Fri Jan 1 1:23:45 2018
```

```
version 8.2(1)
logging level ntp 6
ntp peer 192.168.12.34
ntp server 192.168.86.42
ntp authentication-key 1 md5 fewhg12345 7
ntp logging
```

This example shows the uncommitted (pending) NTP configuration for the current session:

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# ntp peer 192.168.12.34
switch(config)# show ntp pending peers

ntp peer 192.168.12.34

switch(config)# ntp commit
switch(config)# show ntp pending peers
```

This example shows the difference between the pending CFS database and the current NTP configuration:

```
switch# show ntp pending-diff
```

This example shows if the time stamp check is enabled using the **time-stamp** command:

```
switch# show ntp timestamp status
Linecard 3 does not support Timestamp check.
```

Troubleshooting NTP

Use the following information for troubleshooting NTP:

This example shows the NTP CFS status:

```
switch# show ntp status
Distribution : Disabled
Last operational state: No session
```

This example shows how to verify to which switches NTP configuration changes will be distributed to:

```
switch1# show cfs peers name ntp

Scope : Physical-fc-ip
-------------------------------------------------------------------------
Switch                  WWN IP Address
-------------------------------------------------------------------------
20:00:8c:60:4f:0d:2b:b0 192.168.12.34 [Local]
                        [switch1]
20:00:8c:60:4f:0d:32:d0 192.168.56.78 [Merged]
                        [switch2.mydomain.com]

Total number of entries = 2
```

This example shows the NTP session information:

```
switch# show ntp session status
Last Action Time Stamp     : None
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : none
```

This example shows all the NTP peers:

```
switch# show ntp peers
--------------------------------------------------
  Peer IP Address               Serv/Peer
--------------------------------------------------
  10.105.194.169                Server (configured)
```

This example shows the difference between **show ntp pending peers** and **show ntp pending-diff** commands. The outputs are similar when adding NTP servers or peers.

```
switch1# configure terminal
switch1(config)# ntp authenticate
switch1(config)# ntp authentication-key 1 md5 aNiceKey
switch1(config)# ntp server 192.168.12.34 key 1
switch1(config)# ntp authentication-key 2 md5 goodTime
switch1(config)# ntp peer 192.168.56.78 key 2
switch1(config)# show ntp pending peers

ntp server 192.168.12.34


ntp peer 192.168.56.78

switch1(config)# show ntp pending-diff
+ntp peer 192.168.56.78
+ntp server 192.168.12.34
switch1(config)# ntp commit
switch1(config)# show ntp pending peers
switch1(config)# show ntp pending-diff
```

Caution Only the server and peer commands are distributed to the NTP peer switches. Other parameters such as enabling authentication and configuring authentication keys must be configured on each switch.

Continuing the example on switch1, the outputs differ when deleting servers or peers:

```
switch1(config)# no ntp peer 192.168.56.78
switch1(config)# show ntp pending peers

ntp server 192.168.12.34

switch1(config)# show ntp pending-diff
-ntp peer 192.168.56.78
switch1(config)# ntp commit
switch1(config)# show ntp pending peers
switch1(config)# show ntp pending-diff
```

```
switch1(config)# end
```

This example shows the status of a peer. Information about each peer is displayed in the table, one peer per line. The first character of each line is a status flag. A legend above the table shows the meaning of this flag. NTP servers and peers that are in synchronization and used for local time updates have an equal (=) flag. There must be at least one device with this flag for the time on the local switch to be updated. Passive peers are peers that are currently unsynchronized. This means the local switch will not use time updates from these peers. The *remote* column shows the source IP address of the peer. The accuracy of the peer's source clock, or stratum, is shown in the *st* column. The higher the stratum value, the lower the accuracy of the peer's clock source, 16 being the lowest accuracy. The polling interval, in seconds, is shown in the *poll* column. The reachability field in the *reach* column is a circular bit map of the last 8 transactions with that peer, '1' indicating success and '0' indicating failure, the most recent transaction in the lowest significant bit. This peer has not lost any of the last 6 poll messages. The round trip time between the local switch and peer, in seconds, is shown in the *delay* column.

```
switch# show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode
    remote           local    st   poll   reach delay
-----------------------------------------------------------------
*10.105.194.169     0.0.0.0    4     16      77   0.00099
```

This example shows the detailed NTP information for a single server or peer.

The *time last received* parameter will return to zero each time frame is received from that server or peer. Consequently, this parameter will steadily increment if the peer is unreachable or not sending to the local switch NTP client.

```
switch# show ntp statistics  peer ipaddr 10.105.194.169
remote host:          10.105.194.169
local interface:      Unresolved
time last received:   9s
time until next send: 54s
reachability change:  54705s
packets sent:         3251
packets received:     3247
bad authentication:   0
bogus origin:         0
duplicate:            0
bad dispersion:       0
bad reference time:   0
candidate order:      6
```

This example shows the counters maintained by the local NTP client on the switch:

```
switch# show ntp statistics local
system uptime:          24286
time since reset:       24286
old version packets:    13
new version packets:    0
unknown version number: 0
bad packet format:      0
packets processed:      13
```

```
bad authentication:     0
```

Example: Configuring NTP

This example displays how to enable the NTP protocol:

```
switch# configure terminal
switch(config)# feature ntp
```

This example displays how to disable the NTP protocol:

```
switch# configure terminal
switch(config)# no feature ntp
```

This example displays how to configure an NTP server:

```
switch# configure terminal
switch(config)# ntp server 192.0.2.10
```

This example displays how to configure an NTP peer:

```
switch# configure terminal
switch(config)# ntp peer 2001:0db8::4101
```

This example displays how to configure NTP authentication:

```
switch# configure terminal
switch(config)# ntp authentication-key 42 md5 key1_12
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
```

This example displays how to enable the processing of private mode packets:

```
switch# configure terminal
switch(config)# ntp allow private
```

This example displays how to enable the processing of control mode packets with a rate-limit of 10 seconds:

```
switch# configure terminal
switch(config)# ntp allow control rate-limit 10
```

This example displays how to configure an NTP source interface:

```
switch# configure terminal
switch(config)# ntp source-interface ethernet 2/2
```

This example enables logging of NTP messages to syslog and changes the syslog logging threshold to 'information':

```
switch# configure terminal
switch(config)# ntp logging
switch(config)# logging logfile messages 6
switch(config)# end
switch# show logging | include "logfile:" next 1
Logging logfile: enabled
Name - messages: Severity - information Size - 4194304
switch# show logging logfile | include %NTP
2017 Jan 1 1:02:03 switch %NTP-6-NTP_SYSLOG_LOGGING: : Peer 192.168.12.34 is reachable
2017 Jan 1 2:34:56 switch %NTP-6-NTP_SYSLOG_LOGGING: : System clock has been updated,
offset= sec
```

This example displays how to disable NTP logging:

```
switch# configure terminal
switch(config)# no ntp logging
```

Default Settings for NTP

This table lists the default settings for NTP parameters.

Table 18: Default NTP Settings

NTP	Disabled
NTP Modes	Disabled
NTP Source Interface	mgmt0
NTP Logging	Disabled
NTP Distribution	Disabled

CHAPTER 13

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, on page 157
- Running CompactFlash Tests, on page 161
- Displaying the Switch Serial Number, on page 161
- Displaying Power Usage Information, on page 162
- Power Supply Modes, on page 163
- About Switch Temperature Monitoring, on page 172
- About Fan Modules, on page 174
- Displaying Environment Information, on page 175
- Default Settings, on page 180

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 9710 (10 Slot) Chassis "
PID: DS-C9710            ,  VID: V00 ,  SN: JAF1647AQTL

NAME: "Slot 2",  DESCR: "2/4/8/10/16 Gbps Advanced FC Module"
PID: DS-X9448-768K9      ,  VID: V02 ,  SN: JAE192008U7

NAME: "Slot 3",  DESCR: "4/8/16/32 Gbps Advanced FC Module"
PID: DS-X9648-1536K9     ,  VID: V01 ,  SN: JAE203901Z0

NAME: "Slot 5",  DESCR: "Supervisor Module-3"
PID: DS-X97-SF1-K9       ,  VID: V02 ,  SN: JAE17360E6B

NAME: "Slot 6",  DESCR: "Supervisor Module-3"
PID: DS-X97-SF1-K9       ,  VID:     ,  SN: JAE164300E8

NAME: "Slot 7",  DESCR: "1/10/40G IPS,2/4/8/10/16G FC Module"
PID: DS-X9334-K9         ,  VID: V00 ,  SN: JAE195001TJ

NAME: "Slot 8",  DESCR: "4/8/16/32 Gbps Advanced FC Module"
PID: DS-X9648-1536K9     ,  VID: V01 ,  SN: JAE203901ZJ
```

```
NAME: "Slot 10",  DESCR: "1/10 Gbps Ethernet Module"
PID: DS-X9848-480K9      ,  VID: V01 ,  SN: JAE172603Q9

NAME: "Slot 11",  DESCR: "Fabric card module"
PID: DS-X9710-FAB1       ,  VID: V01 ,  SN: JAE18040A1N

NAME: "Slot 12",  DESCR: "Fabric card module"
PID: DS-X9710-FAB        ,  VID: V01 ,  SN: JAE164705RF

NAME: "Slot 13",  DESCR: "Fabric card module"
PID: DS-X9710-FAB1       ,  VID: V01 ,  SN: JAE18040A22

NAME: "Slot 14",  DESCR: "Fabric card module"
PID: DS-X9710-FAB1       ,  VID: V01 ,  SN: JAE1640085T

NAME: "Slot 15",  DESCR: "Fabric card module"
PID: DS-X9710-FAB        ,  VID: V01 ,  SN: JAE16410AR4

NAME: "Slot 16",  DESCR: "Fabric card module"
PID: DS-X9710-FAB1       ,  VID: V00 ,  SN: JAE19500864

NAME: "Slot 33",  DESCR: "MDS 9710 (10 Slot) Chassis Power Supply"
PID: DS-CAC97-3KW        ,  VID: V01 ,  SN: DTM1649022W

NAME: "Slot 34",  DESCR: "MDS 9710 (10 Slot) Chassis Power Supply"
PID: DS-CAC97-3KW        ,  VID: V01 ,  SN: DTM16490239

NAME: "Slot 35",  DESCR: "MDS 9710 (10 Slot) Chassis Power Supply"
PID: DS-CAC97-3KW        ,  VID: V01 ,  SN: DTM164602ZP

NAME: "Slot 40",  DESCR: "MDS 9710 (10 Slot) Chassis Power Supply"
PID: DS-CAC97-3KW        ,  VID: V01 ,  SN: DTM164602XH

NAME: "Slot 41",  DESCR: "MDS 9710 (10 Slot) Chassis Fan Module"
PID: DS-C9710-FAN        ,  VID: V00 ,  SN: JAF1647ADCN

NAME: "Slot 42",  DESCR: "MDS 9710 (10 Slot) Chassis Fan Module"
PID: DS-C9710-FAN        ,  VID: V00 ,  SN: JAF1647ACHH

NAME: "Slot 43",  DESCR: "MDS 9710 (10 Slot) Chassis Fan Module"
PID: DS-C9710-FAN        ,  VID: V00 ,  SN: JAF1647ADCE
```

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

```
switch# show hardware
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2017, 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

Software
  BIOS:      version 3.1.0
  kickstart: version 8.2(1)
  system:    version 8.2(1)
  BIOS compile time:       02/27/2013
  kickstart image file is: bootflash:///m9700-sf3ek9-kickstart-mz.8.2.1.bin.S46
  kickstart compile time:  8/30/2017 23:00:00 [09/27/2017 12:00:46]
  system image file is:    bootflash:///m9700-sf3ek9-mz.8.2.1.bin.S46
  system compile time:     8/30/2017 23:00:00 [09/27/2017 14:57:51]


Hardware
  cisco MDS 9710 (10 Slot) Chassis ("Supervisor Module-3")
  Intel(R) Xeon(R) CPU C5528 @ 2.13GHz with 8167228 kb of memory.
  Processor Board ID JAE17360E6B

  Device name: sw-9710-101
  bootflash:    3915776 kB
  slot0:              0 kB (expansion flash)

Kernel uptime is 0 day(s), 2 hour(s), 25 minute(s), 2 second(s)

Last reset at 969755 usecs after  Wed Nov  8 06:28:35 2017

  Reason: Reset Requested by CLI command reload
  System version: 8.2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
--------------------------------
Switch hardware ID information
--------------------------------

Switch is booted up
  Switch type is : MDS 9710 (10 Slot) Chassis
  Model number is DS-C9710
  H/W version is 0.2
  Part Number is 73-14586-02
  Part Revision is 02
  Manufacture Date is Year 16 Week 47
  Serial number is JAF1647AQTL
  CLEI code is 0

--------------------------------
Chassis has 10 Module slots and 6 Fabric slots
--------------------------------

Module1  empty

Module2  powered-dn
  Module type is : 2/4/8/10/16 Gbps Advanced FC Module
  0 submodules are present
  Model number is DS-X9448-768K9
  H/W version is 1.3
  Part Number is 73-15110-04
  Part Revision is A0
  Manufacture Date is Year 19 Week 20
  Serial number is JAE192008U7
  CLEI code is CMUIAHUCAC
.
.
.
Module10  ok
  Module type is : 1/10 Gbps Ethernet Module
  0 submodules are present
  Model number is DS-X9848-480K9
  H/W version is 1.0
  Part Number is 73-15258-05
  Part Revision is A0
  Manufacture Date is Year 17 Week 26
  Serial number is JAE172603Q9
  CLEI code is CMUCAD5BAA

Xbar1  ok
  Module type is : Fabric card module
  0 submodules are present
  Model number is DS-X9710-FAB1
  H/W version is 1.2
  Part Number is 73-15234-02
  Part Revision is C0
  Manufacture Date is Year 18 Week 4
  Serial number is JAE18040A1N
  CLEI code is CMUCAD1BA
.
.
.
Xbar6  powered-dn
  Module type is : Fabric card module
  0 submodules are present
  Model number is DS-X9710-FAB1
  H/W version is 1.0
  Part Number is 73-100994-01
  Part Revision is 03
  Manufacture Date is Year 19 Week 50
  Serial number is JAE19500864
  CLEI code is CLEI987656

---------------------------------------
Chassis has 8 PowerSupply Slots
---------------------------------------

PS1 ok
  Power supply type is: 3000.00W 220v AC
  Model number is DS-CAC97-3KW
  H/W version is 1.0
  Part Number is 341-0428-01
  Part Revision is A0
  Manufacture Date is Year 16 Week 49
  Serial number is DTM1649022W
  CLEI code is CMUPABRCAA
.
.
.
PS8 ok
  Power supply type is: 3000.00W 220v AC
  Model number is DS-CAC97-3KW
  H/W version is 1.0
  Part Number is 341-0428-01
  Part Revision is A0
  Manufacture Date is Year 16 Week 46
  Serial number is DTM164602XH
  CLEI code is CMUPABRCAA

----------------------------------
Chassis has 3 Fan slots
----------------------------------

Fan1(sys_fan1) ok
  Model number is DS-C9710-FAN
  H/W version is 0.2
  Part Number is 73-15236-02
  Part Revision is 02
  Manufacture Date is Year 16 Week 47
  Serial number is JAF1647ADCN
  CLEI code is

Fan2(sys_fan2) ok
  Model number is DS-C9710-FAN
  H/W version is 0.2
  Part Number is 73-15236-02
  Part Revision is 02
  Manufacture Date is Year 16 Week 47
  Serial number is JAF1647ACHH
  CLEI code is

Fan3(sys_fan3) ok
  Model number is DS-C9710-FAN
  H/W version is 0.2
  Part Number is 73-15236-02
  Part Revision is 02
  Manufacture Date is Year 16 Week 47
  Serial number is JAF1647ADCE
  CLEI code is
```

Running CompactFlash Tests

You can run the test on demand by using the **system health check bootflash fix-errors** or **system health check logflash bad-blocks** CLI command in EXEC mode.

Use the GOLD (Generic Online Diagnostics) feature on the Cisco MDS 9700 Series Multilayer Directors to tests and verifies the hardware devices and data path in a live system. For more information on GOLD, see the Configuring Online Diagnostics chapter in Cisco MDS 9000 Series NX-OS System Management Configuration Guide.

Displaying the Switch Serial Number

You can display the serial number of your Cisco MDS 9000 Series 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   : 3
 Block Length    : 160
 Block Checksum  : 0x134f
 EEPROM Size     : 65535
 Block Count     : 5
 FRU Major Type  : 0x6001
 FRU Minor Type  : 0x0
 OEM String      : Cisco Systems, Inc.
 Product Number  : DS-C9710
 Serial Number   : JAF1647AQTL
 Part Number     : 73-14586-02
 Part Revision   : 02
 Mfg Deviation   : 0
 H/W Version     : 0.2
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 0.0.0.0.0.0.0.0
 Power Consump   : 0
 RMA Code        : 0-0-0-0
 CLEI Code       : 0
 VID             : V00
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 Series 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 9700 Series switch, power usage is reserved for both supervisors regardless of whether one or both supervisor modules are present.

```
switch# show environment power

Power Supply:
Voltage: 50 Volts
Power                              Actual        Total
Supply    Model                    Output     Capacity    Status
-------  -------------------  -----------  -----------  --------------
1        DS-CAC97-3KW              549 W       3000 W     Ok
2        DS-CAC97-3KW              535 W       3000 W     Ok
3        DS-CAC97-3KW              539 W       3000 W     Ok
4        DS-CAC97-3KW              535 W       3000 W     Ok
5        ------------                0 W          0 W     Absent
6        ------------                0 W          0 W     Absent
7        ------------                0 W          0 W     Absent
8        ------------                0 W          0 W     Absent


                                  Actual        Power
Module    Model                     Draw    Allocated    Status
-------  -------------------  -----------  -----------  --------------
2        DS-X9448-768K9            N/A            0 W    Powered-Dn
3        DS-X9648-1536K9           265 W        750 W    Powered-Up
5        DS-X97-SF1-K9             113 W        190 W    Powered-Up
6        DS-X97-SF1-K9             106 W        190 W    Powered-Up
7        DS-X9334-K9               441 W        480 W    Powered-Up
8        DS-X9648-1536K9           252 W        750 W    Powered-Up
10       DS-X9848-480K9            363 W        500 W    Powered-Up
Xb1      DS-X9710-FAB1              95 W        150 W    Powered-Up
```

```
Xb2      DS-X9710-FAB                91 W        150 W    Powered-Up
Xb3      DS-X9710-FAB1               94 W        150 W    Powered-Up
Xb4      DS-X9710-FAB1               90 W        150 W    Powered-Up
Xb5      DS-X9710-FAB                98 W        150 W    Powered-Up
Xb6      DS-X9710-FAB1              N/A          150 W    Powered-Dn
fan1     DS-C9710-FAN                50 W        600 W    Powered-Up
fan2     DS-C9710-FAN                40 W        600 W    Powered-Up
fan3     DS-C9710-FAN                45 W        600 W    Powered-Up

N/A - Per module power not available


Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)                Redundant
Power Supply redundancy mode (operational)               Redundant

Total Power Capacity (based on configured mode)               6000 W
Total Power of all Inputs (cumulative)                       12000 W
Total Power Output (actual draw)                              2158 W
Total Power Allocated (budget)                                5560 W
Total Power Available for additional modules                   440 W
```

Note When a switch experiences a power failure, the line cards and supervisor modules log the reset reason as **reset due to bad voltage**. This information can be accessed by using the **show system reset-reason module.** command. The reset reason is logged during the next system reboot.

Power Supply Modes

Cisco MDS 9000 Series Multilayer Switches support different number and capabilities of power supplies. This section describes the power modes that are available on Cisco MDS 9000 Series Multilayer Switches.

Cisco MDS 9710 Multilayer Switches can support up to four power supplies when they have only Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Modules installed on them. By default, the four power supplies are installed in the power supply bays 1 to 4.

You can configure one of the following power modes to use the combined power provided by the installed power supply units (no power redundancy) or to provide power redundancy when there is power loss. We recommend that you configure the full redundancy power mode on your switch for optimal performance.

- Combined mode—This mode uses the combined capacity of all the power supplies. In case of power supply failure, the entire switch can be shut down (depending on the power used) causing traffic disruption. This mode is seldom used, except in cases when the switch requires more power.

- Input Source (grid) redundancy mode—This mode allocates half of the power supplies to the available category and the other half to the reserve category. You must use different power supplies for the available and reserve categories so that if the power supplies used for the active power fails, the power supplies used for the reserve power can provide power to the switch. If the grid-redundancy mode is lost, the power mode reverts to combined mode.

- Power-supply (N+1) redundancy mode—This mode allocates one power supply as reserve to provide power to the switch in case an active power supply fails. The remaining power supplies are allocated for the available category. The reserve power supply must be at least as powerful as each of the power supplies used for the active power.

- Full-redundancy mode—This mode is a combination of input-source (grid) and power-supply (N+1) redundancy modes. Similar to the input-source redundancy mode, this mode allocates half of the power supplies to the available category and the remaining power supplies to reserve category. One of the reserve power supplies can alternatively be used to provide power if a power supply used for the active power fails.

For more information on the power supply modes supported on your switch, see the *Hardware Installation Guide* corresponding to your switch.

Configuration Guidelines for Power Supplies

For information that is specific to the power supplies supported on your switch, see the *Hardware Installation Guide* corresponding to your switch.

Note

- Some Cisco MDS switches support DC and high-voltage DC (HVDC) power supplies. HVDC power supplies support 440 V (higher voltage), whereas DC power supplies support up to 110 or 220 V. Also, HVDC power supplies are efficient in transmitting power over a long distance.
- The Cisco MDS 9250i switch has three power supplies whose power supply mode is configured to N+1 mode. Cisco MDS 9250i switch can also be operated with only two power supplies when 1+1 grid redundancy is required. All the other Cisco MDS 9000 switches (excluding Directors) have a nonconfigurable power supply mode set to 1+1 grid redundancy.

A Cisco MDS 9700 Series switch ships with enough power supplies to power a fully populated chassis in the grid-redundant (N+N) mode. For example, depending on your switch's configuration, Cisco MDS 9710 switch may ship with six power supplies, by default, and can power a fully populated chassis in the grid-redundant power-configuration (N+N) mode. All the power supplies are always powering the chassis. However, for managing, reporting, and budgeting the power supplies, Cisco MDS NX-OS supports various configurable power supply modes. One of the features of the power supply modes is to make assumptions, especially in grid configuration, to identify power supplies that are connected to grid A and grid B power whips. For information on connecting power supplies, see the "Product Overview" section in the *Cisco MDS 9700 Series Hardware Installation Guide*.

The following table provides information about the power supply bays with respect to grid configurations:

Table 19: Cisco MDS 9700 Grid-Slot Location

Cisco MDS Switch	Grid A	Grid B
Cisco MDS 9718	PSU1, PSU2, PSU5, PSU6, PSU9, PSU10, PSU13, PSU14	PSU3, PSU4, PSU7, PSU8, PSU11, PSU12, PSU15, PSU16
Cisco MDS 9710	PSU1, PSU2, PSU5, PSU6	PSU3, PSU4, PSU7, PSU8
Cisco MDS 9706	PSU1, PSU2	PSU3, PSU4

The following is a list of power supply modes supported on Cisco MDS switches:

Note Changing between power modes is non disruptive and is possible only if there is enough power available in the target mode. If enough power is not available, MDS NX-OS rejects the command with “Insufficient capacity” message.

- Ps-redundant mode—The default power supply mode is the ps-redundant mode, which is equivalent to the N+1 redundant mode because this mode is flexible enough to cover the deployments in the most diverse environments. In this mode, N functioning power supplies are used for budgeting, alerting, reporting, and monitoring, and one power supply is used as reserve. The total available power is the sum of capacities of the N power supplies.

  In the ps-redundant mode, there is no restriction for the placement of power supplies in the chassis slots. The power supplies need not be placed in grid A or grid B as recommended. Even if the power supplies are placed as recommended in grid A or grid B, MDS NX-OS will not support budgeting, alerting, reporting, and monitoring as per a grid configuration because of the N+1 redundancy mode.

Table 20: ps-redundant Mode

Scenario	Grid A			Grid B			Available Capacity (Watts)	Power Supply Operational Mode
	Power Supply 1 (Watts)	Power Supply 2 (Watts)	Power Supply 5 (Watts)	Power Supply 3 (Watts)	Power Supply 4 (Watts)	Power Supply 7 (Watts)		
1	3000	3000	3000	3000	3000	3000	15000	N+1 redundant mode. Available power capacity is the sum of power capacities of all the operational power supply units (PSUs), except one, which is used as reserve.
2	3000	3000	3000	3000	3000	Off	12000	
3	3000	3000	3000	3000	Off	Off	9000	
4	3000	3000	3000	Off	Off	Off	6000	

- insrc-redundant mode—If a grid (N+N) mode is required in a chassis for proper budgeting, alerting, reporting, and monitoring purposes, power supplies must be configured, as shown in Table 20: ps-redundant Mode, on page 165 and then the ps-redundant mode should be changed to the insrc-redundant mode.

  After the insrc-redundant mode is configured, and if a power supply fails, the power supply mode is changed to combined (nonredundant) mode in relation to the least-populated grid.

When the insrc-redundant mode is configured and a grid fails, the insrc-redundant mode is disabled until the grid is back online. In the meantime, the operational power supply mode is changed to combined (nonredundant) mode and power is used from all the power supplies for budgeting, alerting, reporting, and monitoring.

Table 21: insrc-redundant Mode

Scenario	Grid A			Grid B			Available Capacity (Watts)	Power Supply Operational Mode
	Power Supply 1 (Watts)	Power Supply 2 (Watts)	Power Supply 5 (Watts)	Power Supply 3 (Watts)	Power Supply 4 (Watts)	Power Supply 7 (Watts)		
1	3000	3000	3000	3000	3000	3000	9000	3+3 redundant mode. Available capacity is the sum of power capacities of three PSUs, which are used as reserve.
2	3000	3000	3000	3000	3000	Off	6000	Combined (nonredundant) mode because of uneven distribution of PSUs in grids. Available capacity is the sum of power capacities of PSUs of the least populated grid.

Scenario	Grid A			Grid B			Available Capacity (Watts)	Power Supply Operational Mode
3	3000	3000	3000	3000	Off	Off	3000	Combined (nonredundant) mode because of uneven distribution of PSUs in grids. Available capacity is the sum of power capacities of PSUs of the least populated grid.
4	3000	3000	3000	Off	Off	Off	9000	Combined (nonredundant) mode because of the grid B failure.

- Redundant mode—Redundant mode is a combination of grid (N+N) and ps-redundant (N+1) modes. If the MDS NX-OS power supply mode is set to redundant mode and if there are an equal number of functioning power supplies in each grid location (grid A and grid B), the operational power supply mode is set to the grid (insrc-redundant) mode. If a grid fails, the operational power supply mode is changed to ps-redundant (N+1) mode. The ps-redundant mode is different from the insrc-redundant mode because a grid failure in insrc-redundant mode defaults to combined (nonredundant) mode.

  When configured in redundant mode and if a power supply fails, the power supply mode is changed to combined (nonredundant) mode in relation to the least-populated grid.

Table 22: Redundant Mode

[illegible]

[illegible]

Note When the insrc-redundant or redundant mode is configured, the grid power supply with an unbalanced configuration (that is, 2+4, and so on) results in the power supply mode to change to combined (nonredundant) operational mode and insufficient power may be budgeted. We recommend that you do not use a grid power supply with an unbalanced configuration when the insrc-redundant or redundant mode is configured.

- Combined (nonredundant) mode—This has no restrictions on how external power sources are connected to a Cisco MDS 9710 switch. The power that is available to the switch is the sum of all the working power supplies in the chassis. You can change from other power modes to the combined mode without disrupting the traffic.

Table 23: Combined (Nonredundant) Mode

Scenario	Grid A			Grid B			Available Capacity (Watts)	Power Supply Operational Mode
	Power Supply 1 (Watts)	Power Supply 2 (Watts)	Power Supply 5 (Watts)	Power Supply 3 (Watts)	Power Supply 4 (Watts)	Power Supply 7 (Watts)		
1	3000	3000	3000	3000	3000	3000	18000	In the combined (non redundant) mode, the position of PSUs do not matter. All PSUs are available for budgeting.
2	3000	3000	3000	3000	3000	Off	15000	
3	3000	3000	3000	3000	Off	Off	12000	
4	3000	3000	3000	Off	Off	Off	9000	

The following table provides information about moving from combined (nonredundant) mode to other power supply modes:

Table 24: Moving from Combined (Nonredundant) Mode to Other Power Supply Modes

Scenario	Grid A			Grid B			Current Usage (Watts)	Cu
	Power Supply 1 (Watts)	Power Supply 2 (Watts)	Power Supply 5 (Watts)	Power Supply 3 (Watts)	Power Supply 4 (Watts)	Power Supply 7 (Watts)		

Scenario	Grid A			Grid B			Current Usage (Watts)
1	3000	3000	3000	3000	3000	3000	6500
	3000	3000	3000	3000	3000	3000	6500
2	3000	3000	3000	3000	3000	Off	6500
	3000	3000	3000	3000	3000	Off	6500
3	3000	3000	3000	3000	3000	Off	5500
	3000	3000	3000	3000	3000	Off	5500
4	3000	3000	3000	3000	3000	Off	6500
	3000	3000	3000	3000	3000	Off	6500

Configuring the Power Supply Mode

You can configure power supply modes.

SUMMARY STEPS

1. **configure terminal**
2. **power redundancy-mode** {**combined** | **insrc-redundant** | **ps-redundant** |**redundant**}
3. (Optional) **show environment power**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

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	**power redundancy-mode** {**combined** | **insrc-redundant** | **ps-redundant** |**redundant**}
	Example:
	`switch(config)# power redundancy-mode combined`
		Configures the power supply mode. The default is **redundant**.

Step 3	(Optional) **show environment power** **Example:** `switch(config)# show environment power`	Displays the power mode configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

About Switch Temperature Monitoring

Multiple temperature sensors are built in to all modules and Fabric switches in the Cisco MDS 9000 Family to protect your switch at all times.

Each switching and supervisor module has three types of temperature sensors: air flow intake, air flow exhaust, and onboard. Each sensor has a minor and major threshold in degress Celcius. The software behaviour at each of the thresholds is as follows:

- Minor threshold: When a minor threshold is exceeded, a minor alarm occurs and the following actions are taken for the sensors:
  - Related syslog messages are logged.
  - Call Home alerts are sent (if configured).
  - SNMP notifications are sent (if configured).

  If a minor temperature alarm occurs, reduce the ambient air temperature or clear intake and exhaust air flow from obstructions, as necessary, to ensure adequate switch cooling.
- Major threshold: When a major threshold is exceeded, a major alarm occurs and the following actions are taken:
  - For onboard and air flow exhaust sensors:
    - Related syslog messages are logged.
    - Call Home alerts are sent (if configured).
    - SNMP notifications are sent (if configured).
  - For air flow intake sensors:
    - Related syslog messages are logged.
    - Call Home alerts are sent (if configured).

- SNMP notifications are sent (if configured).

If a major temperature threshold is exceeded in a Director switch on the active supervisor module then only that module is powered down. If an HA standby supervisor is present then it becomes the active supervisor nondisruptively. If a standby supervisor is not present then the whole switch is powered down disruptively after two minutes unless the temperature is reduced below the major threshold. Configured alerts are sent every 5 seconds until power down. If a major temperature threshold is exceeded on a switching module then only that module is powered down. If a major temperature threshold is exceeded on a Fabric switch then the whole switch is powered down.

If a major temperature alarm occurs, investigate the environment for the source of the high temperature and remedy before repowering the switch.

Note Cisco MDS 9000 Series Fabric Switches with NX-OS Release 9.4(3) or later has default sprom values as 70,45 for all the sensors (S1-S4). Due to this condition, if you perform an ISSD to an earlier release, the intake temperature sensor threshold values are displayed higher than the outlet temperature threshold sensor values, which is incorrect.

Note A threshold value of –127 indicates that no thresholds are configured or applicable.

Tip To realize the benefits of these built-in automatic sensors on any Cisco MDS 9700 Director switch, we highly recommend that you install dual supervisor modules to prevent system shutdown in the event of a supervisor major temperature event. If you are using a Cisco MDS 9700 Director switch without dual supervisor modules, it is recommended to replace a failed fan module immediately if even a single fan is not functioning. This ensures the switch operates within safe temperature limits.

Displaying Switch Temperatures

Use the **show environment temperature** command to display information for all temperature sensors for each module.

The following example shows the temperature alarm thresholds and the current temperature of the system on a Cisco MDS 9396T 32-Gbps 96-Port Fibre Channel Switch.

```
switch# show environment temperature
Temperature:
--------------------------------------------------------------------
Module   Sensor        MajorThresh   MinorThres   CurTemp     Status
                       (Celsius)     (Celsius)    (Celsius)
--------------------------------------------------------------------
1        Intake1  (s1)   60              45          40         Ok
1        Intake2  (s2)   60              45          36         Ok
1        Outlet1  (s3)   70              55          50         Ok
1        Outlet2  (s4)   70              55          47         Ok
1        AXE35  (s5)     125             105         62         Ok
1        IOSlice0 (s6)   125             115         53         Ok
```

```
1        IOSlice1 (s7)   125            115         54         Ok
1        IOSlice2 (s8)   125            115         52         Ok
1        CPU      (s9)   85             80          49         Ok
1        Crossbar (s10)  125            115         60         Ok
1        Arbiter  (s11)  125            115         43         Ok
1        IOSlice3 (s12)  125            115         46         Ok
1        IOSlice4 (s13)  125            115         45         Ok
1        IOSlice5 (s14)  125            115         46         Ok
```

Starting from MDS NX-OS Release 9.4(3), alarm and warning thresholds have been lowered for air intake temperature sensors s1 and s2, and exhaust temperature sensors s3 and s4 for the following switches:

- Cisco MDS 9132T 32-Gbps 32-Port Fibre Channel Switch
- Cisco MDS 9396T 32-Gbps 96-Port Fibre Channel Switch
- Cisco MDS 9148T 32-Gbps 48-Port Fibre Channel Switch
- Cisco MDS 9220i 32-Gbps Multiservice Fabric Switch
- Cisco MDS 9148V 64-Gbps 48-Port Fibre Channel
- Cisco MDS 9124V 64-Gbps 24-Port Fibre Channel
- Cisco MDS 9396V 64-Gbps 96-Port Fibre Channel

Note All other switches retain their original temperature alarm thresholds.

Modified Temperature Thresholds for Alarms and Warnings:

Table 25: Temperature thresholds of Intake and Outlet Sensors

	Temperature thresholds from MDS NX-OS Release 9.4(2) and earlier		**Temperature thresholds from MDS NX-OS Release 9.4(3) and later**		
Module	**Major Threshold (Celsius)**	**Minor Threshold (Celsius)**	**Major Threshold (Celsius)**	**Minor Threshold (Celsius)**	
Intake (s1)	70	60	60	45	
Intake (s2)	70	60	60	45	
Outlet (s3)	80	70	70	55	
Outlet (s4)	80	70	70	55	

About Fan Modules

Hot-swappable fan modules (fan trays) are provided in all switches in the Cisco MDS 9000 Series 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 Series 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:
-------------------------------------------------------
Fan              Model                Hw         Status
-------------------------------------------------------
Fan1(sys_fan1)   DS-C9710-FAN         0.2        Ok
Fan2(sys_fan2)   DS-C9710-FAN         0.2        Ok
Fan3(sys_fan3)   DS-C9710-FAN         0.2        Ok
Fan_in_PS1       --                   --         Ok
Fan_in_PS2       --                   --         Ok
Fan_in_PS3       --                   --         Ok
Fan_in_PS4       --                   --         Absent
Fan_in_PS5       --                   --         Absent
Fan_in_PS6       --                   --         Absent
Fan_in_PS7       --                   --         Absent
Fan_in_PS8       --                   --         Ok
Fan Zone Speed %(Hex): Zone 1: 40.78(0x68)
```

The possible Status field values for a fan module on the Cisco MDS 9700 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.

Displaying Environment Information

Use the **show environment** command to display all environment-related switch information.

```
switch# show environment
Power Supply:
Voltage: 50 Volts
Power                              Actual        Total
Supply    Model                    Output     Capacity    Status
-------  -------------------  -----------  -----------  --------------
1        DS-CAC97-3KW               548 W       3000 W     Ok
2        DS-CAC97-3KW               535 W       3000 W     Ok
3        DS-CAC97-3KW               535 W       3000 W     Ok
4        ------------                 0 W          0 W     Absent
5        ------------                 0 W          0 W     Absent
6        ------------                 0 W          0 W     Absent
7        ------------                 0 W          0 W     Absent
8        DS-CAC97-3KW               535 W       3000 W     Ok


                                  Actual        Power
Module    Model                     Draw    Allocated    Status
-------  -------------------  -----------  -----------  --------------
2        DS-X9448-768K9             N/A            0 W    Powered-Dn
3        DS-X9648-1536K9            265 W        350 W    Powered-Up
5        DS-X97-SF1-K9              107 W        190 W    Powered-Up
6        DS-X97-SF1-K9              106 W        190 W    Powered-Up
7        DS-X9334-K9                441 W        480 W    Powered-Up
8        DS-X9648-1536K9            252 W        750 W    Powered-Up
10       DS-X9848-480K9             363 W        500 W    Powered-Up
Xb1      DS-X9710-FAB1               95 W        150 W    Powered-Up
Xb2      DS-X9710-FAB1               94 W        150 W    Powered-Up
Xb3      DS-X9710-FAB1               91 W        150 W    Powered-Up
Xb       DS-X9710-FAB1               N/A         150 W    Powered-Dn
fan1     DS-C9710-FAN                45 W        600 W    Powered-Up
fan2     DS-C9710-FAN                45 W        600 W    Powered-Up
fan3     DS-C9710-FAN                50 W        600 W    Powered-Up

N/A - Per module power not available


Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)                Redundant
Power Supply redundancy mode (operational)               Redundant

Total Power Capacity (based on configured mode)               6000 W
Total Power of all Inputs (cumulative)                       12000 W
Total Power Output (actual draw)                              2153 W
Total Power Allocated (budget)                                5560 W
Total Power Available for additional modules                   440 W

Clock:
----------------------------------------------------------
Clock           Model                Hw         Status
----------------------------------------------------------
A               Clock Module         --         NotSupported/None
B               Clock Module         --         NotSupported/None


Fan:
------------------------------------------------------
Fan             Model                Hw         Status
------------------------------------------------------
Fan1(sys_fan1)  DS-C9710-FAN         0.2         Ok
Fan2(sys_fan2)  DS-C9710-FAN         0.2         Ok
Fan3(sys_fan3)  DS-C9710-FAN         0.2         Ok
```

```
Fan_in_PS1      --                   --         Ok
Fan_in_PS2      --                   --         Ok
Fan_in_PS3      --                   --         Ok
Fan_in_PS4      --                   --         Absent
Fan_in_PS5      --                   --         Absent
Fan_in_PS6      --                   --         Absent
Fan_in_PS7      --                   --         Absent
Fan_in_PS8      --                   --         Ok
Fan Zone Speed %(Hex): Zone 1: 40.78(0x68)


Temperature:
--------------------------------------------------------------------
Module   Sensor        MajorThresh   MinorThres   CurTemp     Status
                       (Celsius)     (Celsius)    (Celsius)
--------------------------------------------------------------------
3        Crossbar0 (s1)  125             115         46         Ok
3        Crossbar1 (s2)  125             115         54         Ok
3        Arb-mux  (s3)   125             105         49         Ok
3        CPU      (s4)   125             105         48         Ok
3        PCISW    (s5)   125             105         66         Ok
3        IOSlice0 (s6)   125             115         38         Ok
3        IOSlice1 (s7)   125             115         39         Ok
3        IOSlice2 (s8)   125             115         40         Ok
5        Inlet  (s1)     60              42          24         Ok
5        Crossbar(s2)    125             115         71         Ok
5        Arbiter (s3)    125             105         51         Ok
5        L2L3Dev1(s4)    125             110         42         Ok
5        CPU1CORE1(s5)   85              75          35         Ok
5        CPU1CORE2(s6)   85              75          29         Ok
5        CPU1CORE3(s7)   85              75          35         Ok
5        CPU1CORE4(s8)   85              75          30         Ok
5        DDR3DIMM1(s9)   95              85          31         Ok
6        Inlet  (s1)     60              42          26         Ok
6        Crossbar(s2)    125             115         70         Ok
6        Arbiter (s3)    125             105         52         Ok
6        L2L3Dev1(s4)    125             110         41         Ok
6        CPU1CORE1(s5)   85              70          36         Ok
6        CPU1CORE2(s6)   85              70          34         Ok
6        CPU1CORE3(s7)   85              70          36         Ok
6        CPU1CORE4(s8)   85              70          33         Ok
6        DDR3DIMM1(s9)   95              85          31         Ok
7        Crossbar0 (s1)  125             115         83         Ok
7        Crossbar1 (s2)  125             115         82         Ok
7        Arb-mux  (s3)   125             115         52         Ok
7        CPU      (s4)   125             115         53         Ok
7        L2L3Dev0 (s5)   125             115         66         Ok
7        IOSlice0 (s6)   125             115         56         Ok
7        IOSlice1 (s7)   125             115         57         Ok
7        IOSlice2 (s8)   125             115         57         Ok
7        FC-IP 0 (s9)    95              85          56         Ok
7        FC-IP 1 (s10)   95              85          56         Ok
8        Crossbar0 (s1)  125             115         52         Ok
8        Crossbar1 (s2)  125             115         52         Ok
8        Arb-mux  (s3)   125             105         50         Ok
8        CPU      (s4)   125             105         47         Ok
8        PCISW    (s5)   125             105         56         Ok
8        IOSlice0 (s6)   125             115         40         Ok
8        IOSlice1 (s7)   125             115         41         Ok
8        IOSlice2 (s8)   125             115         42         Ok
10       Crossbar1(s1)   125             115         79         Ok
10       Crossbar2(s2)   125             115         79         Ok
10       Arb-mux (s3)    125             105         56         Ok
10       L2L3Dev1(s5)    125             110         61         Ok
```

```
10       L2L3Dev2(s6)    125             110         61         Ok
10       L2L3Dev3(s7)    125             110         57         Ok
10       L2L3Dev4(s8)    125             110         56         Ok
10       L2L3Dev5(s9)    125             110         61         Ok
10       L2L3Dev6(s10)   125             110         52         Ok
10       L2L3Dev7(s11)   125             110         58         Ok
10       L2L3Dev8(s12)   125             110         66         Ok
10       L2L3Dev9(s13)   125             110         57         Ok
10       L2L3Dev10(s14)  125             110         59         Ok
10       L2L3Dev11(s15)  125             110         66         Ok
10       L2L3Dev12(s16)  125             110         62         Ok
xbar-1   Crossbar1(s1)   125             115         49         Ok
xbar-1   Crossbar2(s2)   125             115         54         Ok
xbar-2   Crossbar1(s1)   125             115         56         Ok
xbar-2   Crossbar2(s2)   125             115         63         Ok
xbar-3   Crossbar1(s1)   125             115         51         Ok
xbar-3   Crossbar2(s2)   125             115         64         Ok
xbar-4   Crossbar1(s1)   125             115         59         Ok
xbar-4   Crossbar2(s2)   125             115         67         Ok
xbar-5   Crossbar1(s1)   125             115         61         Ok
xbar-5   Crossbar2(s2)   125             115         68         Ok
```

use the **show environment power detail**to display power capacity and power distribution information.

```
switch# show environment power detail
Power Supply:
Voltage: 50 Volts
Power                              Actual       Actual        Total
Supply    Model                    Output        Input     Capacity         Status
-------  -------------------  -----------  -----------  -----------  --------------
1        DS-CAC97-3KW              243 W        290 W       3000 W        Ok
2        DS-CAC97-3KW                0 W          0 W          0 W        Powered-dn
3        DS-CAC97-3KW              252 W        320 W       3000 W        Ok
4        DS-CAC97-3KW              293 W        345 W       3000 W        Ok

Mod  Power-Status  Reason
---  ------------  ---------------------------
2    Powered-dn     Configured Power down


                                  Actual        Power
Module    Model                     Draw    Allocated     Status
-------  -------------------  -----------  -----------  --------------
1        DS-X9448-768K9             N/A           650 W    Powered-Up
2        DS-X9648-1536K9            N/A             0 W    Present
3        DS-X97-SF4-K9               88 W         120 W    Powered-Up
4        supervisor                 N/A           120 W    Powered-Up
5        DS-X9748-3072K9            N/A             0 W    Present
Xb1      DS-X9706-FAB3               33 W          85 W    Powered-Up
Xb2      xbar                       N/A            85 W    Absent
Xb3      DS-X9706-FAB3               31 W          85 W    Powered-Up
Xb4      DS-X9706-FAB3               42 W          85 W    Powered-Up
Xb5      DS-X9706-FAB3               41 W          85 W    Powered-Up
Xb6      DS-X9706-FAB3               41 W          85 W    Powered-Up
fan1     DS-C9706-FAN                 0 W         250 W    Powered-Up
fan2     DS-C9706-FAN                 0 W         250 W    Powered-Up
fan3     DS-C9706-FAN                 0 W         250 W    Powered-Up

N/A - Per module power not available


Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)                PS-Redundant
Power Supply redundancy mode (operational)               PS-Redundant

Total Power Capacity (based on configured mode)              6000 W
Total Power of all Inputs (cumulative)                       9000 W
Total Power Output (actual draw)                              788 W
Total Power Input  (actual draw)                              955 W
Total Power Allocated (budget)                               3264 W
Total Power Available for additional modules                 2736 W


Power Usage details:
--------------------
Power reserved for Supervisor(s):                             240 W
Power reserved for Fabric Module(s):                          510 W
Power reserved for Fan Module(s):                             750 W
Total power reserved for Sups,Fabrics,Fans:                  1500 W

Are all inlet cables connected: Yes

Power supply details:
---------------------
PS_1
50V Voltage: 50.943V
50V Current: 5.470A
3.4V Voltage: 3.388V
3.4V Current: 1.710A
50V Temperature: 52C
3.4V Temperature: 46C
Total Capacity    3000 W   Voltage:50V
Cable 1    capacity:    3000 W
Cable 1    connected to 220v AC
Software-Alarm: No
Hardware alarm_bits reg0: 0x02
Reg0 bit1: restarted successfully

PS_2
50V Voltage: 0.000V
50V Current: 0.000A
3.4V Voltage: 0.000V
3.4V Current: 0.000A
50V Temperature: 34C
3.4V Temperature: 36C
Total Capacity       0 W   Voltage:50V
Cable 1    capacity:       0 W
Cable 1    connected to 220v AC
Software-Alarm: Yes
Hardware alarm_bits reg0: 0x40, reg1: 0x40, reg3: 0x03
Reg0 bit6: Invalid access
Reg1 bit6: powercycle had occured, forceshut bit was set
Reg3 bit0: 3.4V output under voltage
Reg3 bit1: 50V output1 under voltage

PS_3
50V Voltage: 51.060V
50V Current: 5.660A
3.4V Voltage: 3.363V
3.4V Current: 1.632A
50V Temperature: 53C
3.4V Temperature: 43C
Total Capacity    3000 W   Voltage:50V
Cable 1    capacity:    3000 W
Cable 1    connected to 220v AC
Software-Alarm: No
Hardware alarm_bits reg0: 0x02
```

```
Reg0 bit1: restarted successfully

PS_4
50V Voltage: 50.900V
50V Current: 6.400A
3.4V Voltage: 3.415V
3.4V Current: 1.765A
50V Temperature: 49C
3.4V Temperature: 52C
Total Capacity    3000 W   Voltage:50V
Cable 1    capacity:    3000 W
Cable 1    connected to 220v AC
Software-Alarm: No
Hardware alarm_bits reg0: 0x42, reg3: 0x10
Reg0 bit1: restarted successfully
Reg0 bit6: Invalid access
Reg3 bit4: reserved
```

Default Settings

This table lists the default hardware settings

Table 26: Default Hardware Parameter Settings

Parameter	Default Setting
Power supply mode	PS redundant mode.

CHAPTER 14

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, on page 181
- Maintaining Supervisor Modules, on page 184
- Verifying the Status of a Module, on page 185
- Checking the State of a Module, on page 186
- Connecting to a Module, on page 187
- Reloading Modules, on page 187
- Saving the Module Configuration, on page 189
- Purging Module Configurations, on page 190
- Powering Off Switching Modules, on page 190
- Powering off Power Supply Units, on page 191
- Identifying Module LEDs, on page 192
- EPLD Images, on page 197
- SSI Boot Images, on page 203
- Managing SSMs and Supervisor Modules, on page 203
- Default Settings, on page 207

About Modules

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

Table 27: 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.

Product	Number of Supervisor Modules	Supervisor Module Slot Number	Switching and Services Module Features
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.
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 Series 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

Modules in a chassis can be in various states which can be displayed using the **show module** command. The state updates as the module steps through the boot sequence. When it reaches 'ok' state it is ready for operation. If any faults are detected during bootup or operation then the state will be updated to show the type of error.

This table describes the module states listed in the **show module** command output.

Table 28: Module States

Module Status Output	Description
`powered up`	The module is receiving electrical power. Once the module is powered up, the software begins booting.
`testing`	The module has established connection with the supervisor module and is performing bootup diagnostics.
`initializing`	The diagnostics have completed successfully and the configuration is being downloaded.
`failure`	The module has failed to initialize successfully after three attempts. This may be due to a software or hardware issue.
`ok`	The module is online and ready for use.
`power-dn`	The module is powered off in the configuration.
`power-denied`	There is insufficient power for the module to power up.
`active`	This module is the active supervisor module and the switch is ready to be configured.
`ha-standby`	The standby supervisor is synchronised with the active supervisor and ready to take over in the event of failure of the active supervisor.
`standby`	The warm switchover mechanism is enabled on the standby supervisor module.

Connecting to a Module

At any time, you can connect to any module using the **attach module** command. Once you are at the module prompt, you can obtain further details about the module using module-specific commands.

You can also use the **attach module** command as follows:

- To display the standby supervisor module information. You cannot configure the standby supervisor module using this command.
- To display the switching module portion of the Cisco MDS 9200 Series supervisor module which resides in slot 1.

SUMMARY STEPS

1. **attach module** *slot*
2. **exit**

DETAILED STEPS

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.

SUMMARY STEPS

1. Identify the module that needs to be reset.
2. Issue the **reload module** command to reset the identified module. This command power cycles the selected module.

DETAILED STEPS

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.

SUMMARY STEPS

1. Identify the switching module that requires the new image.
2. Issue the **reload module** command to update the image on the switching module.

DETAILED STEPS

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 29: Switching Module Configuration Status

Scenario	Consequence
You remove a switching module and issue the **copy running-config startup-config** command.	The configured module information is lost.
You remove a switching module and reinsert the same switching module before issuing the **copy running-config startup-config** command.	The configured module information is saved.
You remove a switching module, insert the same type switching module in the same slot, and issue a **reload module** *number* command.	The configured module information is saved.
You enter a **reload module** *number* command to reload a switching module.	The configured module information is preserved.

Scenario	Consequence
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.

SUMMARY STEPS

1. **configure terminal**

2. [**no**] **poweroff module** *slot*

DETAILED STEPS

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.

Powering off Power Supply Units

You can power off a power supply unit from the command line interface (CLI). Powering down PSUs that are not connected to external power or not switched on prevents them from triggering system power warnings.

SUMMARY STEPS

1. **configure terminal**
2. **poweroff power-supply**<*psu*>
3. [**no**] **poweroff module** *slot*

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**poweroff power-supply**<*psu*> **Example:** `switch(config)# poweroff power-supply 3`	Power off an individual power supply unit.
Step 3	[**no**] **poweroff module** *slot* **Example:** `switch(config)# no poweroff module 3`	Power on an individual power supply unit.

Identifying Module LEDs

This table describes the LEDs for the Cisco MDS 9200 Series integrated supervisor modules.

Table 30: 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 31: 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 32: 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 33: LEDs for the Cisco MDS 9500 Series Supervisor Modules

LED	Status	Description
Status	Green	All diagnostics pass. The module is operational (normal initialization sequence).
	Orange	The module is booting or running diagnostics (normal initialization sequence). or An over temperature condition has occurred (a minor threshold has been exceeded during environmental monitoring).
	Red	The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence. or An over temperature condition occurred (a major threshold was exceeded during environmental monitoring).

LED	Status	Description
System **Note** The System and Pwr Mgmt LEDs on a redundant supervisor module are synchronized to the active supervisor module.	Green	All chassis environmental monitors are reporting OK.
	Orange	The power supply has failed or the power supply fan has failed. or Incompatible power supplies are installed. or The redundant clock has failed.
	Red	The temperature of the supervisor module major threshold has been exceeded.
Active	Green	The supervisor module is operational and active.
	Orange	The supervisor module is in standby mode.
Pwr Mgmt[1]	Green	Sufficient power is available for all modules.
	Orange	Sufficient power is not available for all modules.
MGMT 10/100 Ethernet Link LED	Green	Link is up.
	Off	No link.
MGMT 10/100 Ethernet Activity LED	Green	Traffic is flowing through port.
	Off	No link or no traffic.
Compact Flash	Green	The external CompactFlash card is being accessed.
	Off	No activity.

EPLD Images

Switches and directors in the Cisco MDS 9000 Family contain several electrical programmable logical devices (EPLDs) that provide hardware functionalities in all modules. EPLD image upgrades are periodically provided to include enhanced hardware functionality or to resolve known issues.

Tip Refer to the Cisco MDS NX-OS Release Notes to verify if the EPLD has changed for the Cisco NX-OS image version being used.

Upgrading EPLD Images

You can upgrade the EPLD images on the modules.

Note The same procedure used to upgrade the EPLD images on a module can be used to downgrade the EPLD images.

SUMMARY STEPS

1. Log into the switch through the console port, an SSH session, or a Telnet session.
2. Enter the **show version** command to verify the Cisco MDS NX-OS software release running on the MDS switch.
3. If necessary, upgrade the Cisco MDS NX-OS software running on your switch (see the *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*).
4. Issue the **dir bootflash:** or **dir slot0:** command to verify that the EPLD software image file corresponding to your Cisco MDS NX-OS release is present on the active supervisor module. For example, if your switch is running Cisco MDS SAN-OS Release 2.1(2), you must have m9000-epld-2.1.2.img in bootflash: or slot0: on the active supervisor module.
5. If you need to obtain the appropriate EPLD software image file, follow these steps:
6. Use the **install module** *number* **epld** *url* command on the active supervisor module to upgrade EPLD images for a module.

DETAILED STEPS

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:

a. Download the EPLD software image file from Cisco.com to your FTP server.

b. 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#
```

c. 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#
```

d. 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

From Cisco MDS NX-OS Release 8.1(1) and later releases, SSI images are no longer supported. Any SSI images installed in boot commands must be removed using the **no boot ssi** command and then reloading the modules before upgrading to Cisco MDS NX-OS Release 8.1(1) and later releases.

Managing SSMs and Supervisor Modules

This section describes the guidelines for replacing SSMs and supervisor modules and for upgrading and downgrading Cisco MDS NX-OS and SAN-OS releases.

Configuring SSM and MSM Global Upgrade Delay

When there are multiple SSMs or MSMs in the same chassis, you can set the amount of time to delay between upgrading the SSMs or MSMs in a rolling SSI upgrade.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ssm upgrade delay** *seconds*
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

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**] **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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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.

SUMMARY STEPS

1. Log into the switch through the console port, an SSH session, or a Telnet session.
2. Display the values assigned to the SSI image boot variable for each module and note the values for later reference.
3. Clear the values assigned to the SSI image boot variable.
4. Reload the SSM to initialize in Fibre Channel switching mode.
5. After the SSM initializes, upgrade the SSI boot image.
6. Reassign the SSI boot variables cleared in Step 3.

DETAILED STEPS

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 34: 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.
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 35: 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.

CHAPTER 15

Scripting with Tcl

This chapter describes how to run tcl interactively and in scripts on a Cisco NX-OS device.

- Finding Feature Information, on page 209
- Guidelines and Limitations, on page 209
- Information about Tcl, on page 211

Finding Feature Information

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

Guidelines and Limitations

Tcl has the following configuration guidelines and limitations:

Tclsh Command Help

Command help is not available for tcl commands. You can still access the help functions of Cisco NX-OS commands from within an interactive tcl shell.

This example shows the lack of tcl command help in an interactive tcl shell:

```
switch# tclsh
switch-tcl# set x 1
switch-tcl# puts ?
          ^
% Invalid command at '^' marker.
switch-tcl# configure ?
  <CR>
  session   Configure the system in a session
  terminal  Configure the system from terminal input

switch-tcl#
```

Note In the above example, the Cisco NX-OS command help function is still available but the tcl **puts** command returns an error from the help function.

Tclsh Command History

You can use the arrow keys on your terminal to access commands you previously entered in the interactive tcl shell.

Note The **tclsh** command history is not saved when you exit the interactive tcl shell.

Tclsh Tab Completion

You can use tab completion for Cisco NX-OS commands when you are running an interactive tcl shell. Tab completion is not available for tcl commands.

Tclsh CLI Command

Although you can directly access Cisco NX-OS commands from within an interactive tcl shell, you can only execute Cisco NX-OS commands in a tcl script if they are prepended with the tcl **cli** command.

In an interactive tcl shell, the following commands are identical and will execute properly:

```
switch-tcl# cli show module 1 | incl Mod
switch-tcl# cli "show module 1 | incl Mod"
switch-tcl# show module 1 | incl Mod
```

In a tcl script, you must prepend Cisco NX-OS commands with the tcl **cli** command as shown in this example:

```
set x 1
cli show module $x | incl Mod
cli "show module $x | incl Mod"
```

If you use the following commands in your script, the script will fail and the tcl shell will display an error:

```
show module $x | incl Mod
"show module $x | incl Mod"
```

Tclsh Command Separation

The semicolon (`;`) is the command separator in both Cisco NX-OS and tcl. To execute multiple Cisco NX-OS commands in a tcl command, you must enclose the Cisco NX-OS commands in quotes (`""`).

In an interactive tcl shell, the following commands are identical and will execute properly:

```
switch-tcl# cli "configure terminal ; interface loopback 10 ; description loop10"
switch-tcl# cli configure terminal ; cli interface loopback 10 ; cli description loop10
switch-tcl# cli configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

switch(config-tcl)# cli interface loopback 10
switch(config-if-tcl)# cli description loop10
switch(config-if-tcl)#
```

In an interactive tcl shell, you can also execute Cisco NX-OS commands directly without prepending the tcl **cli** command:

```
switch-tcl# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(config-tcl)# interface loopback 10
switch(config-if-tcl)# description loop10
switch(config-if-tcl)#
```

Tcl Variables

You can use tcl variables as arguments to the Cisco NX-OS commands. You can also pass arguments into tcl scripts. Tcl variables are not persistent.

This example shows how to use a tcl variable as an argument to a Cisco NX-OS command:

```
switch# tclsh
switch-tcl# set x loop10
switch-tcl# cli "configure terminal ; interface loopback 10 ; description $x"
switch(config-if-tcl)#
```

Tclquit

The **tclquit** command exits the tcl shell regardless of which Cisco NX-OS command mode is currently active. You can also press **Ctrl-C** to exit the tcl shell. The **exit** and **end** commands change Cisco NX-OS command modes. The **exit** command will terminate the tcl shell only from the EXEC command mode.

Tclsh Security

The tcl shell is executed in a sandbox to prevent unauthorized access to certain parts of the Cisco NX-OS system. The system monitors CPU, memory, and file system resources being used by the tcl shell to detect events such as infinite loops, excessive memory utilization, and so on.

You configure the intial tcl environment with the **scripting tcl init** *init-file* command.

You can define the looping limits for the tcl environment with the **scripting tcl recursion-limit** *iterations* command. The default recursion limit is 1000 interations.

Information about Tcl

Tool Command Language (Tcl) is a scripting language created by John Ousterhout at the University of California, Berkeley. Tcl 8.5 was added to Cisco NX-OS Release 5.1(1) to provide scripting abilities. With tcl, you gain more flexibility in your use of the CLI commands on the device. You can use tcl to extract certain values in the output of a **show** command, perform switch configurations, run Cisco NX-OS commands in a loop, or define EEM policies in a script.

This section describes how to run tcl scripts or run tcl interactively on Cisco NX-OS devices.

Running the tclsh Command

You can run tcl commands from either a script or on the command line using the **tclsh** command.

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

SUMMARY STEPS

1. **tclsh** [**bootflash:***filename* [*argument* ...]]

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**tclsh** [**bootflash:***filename* [*argument* ...]]
	Example:
	`switch# tclsh ?`
	`  <CR>`
	`  bootflash:  The file to run`
		Starts a tcl shell.
		If you run the **tclsh** command with no arguments, the shell runs interactively, reading tcl commands from standard input and printing command results and error messages to the standard output. You exit from the interactive tcl shell by entering **tclquit** or pressing **Ctrl-C**.
		If you enter the **tclsh** command with arguments, the first argument is the name of a script file that contains tcl commands and any additional arguments are made available to the script as variables.

Example

This example shows an interactive tcl shell:

```
switch# tclsh
switch-tcl# set x 1
switch-tcl# cli show module $x | incl Mod
Mod  Ports  Module-Type                         Model              Status
1    32     1/10 Gbps Ethernet Module           N7K-F132XP-15      ok
Mod  Sw               Hw
Mod  MAC-Address(es)                            Serial-Num
Mod  Online Diag Status
Left ejector CLOSE, Right ejector CLOSE, Module HW does support ejector based shutdown.
switch-tcl# exit
switch#
```

This example shows how to run a tcl script:

```
switch# show file bootflash:showmodule.tcl
set x 1
while {$x < 19} {
cli show module $x | incl Mod
set x [expr {$x + 1}]
}

switch# tclsh bootflash:showmodule.tcl
Mod  Ports  Module-Type                         Model              Status
1    32     1/10 Gbps Ethernet Module        N7K-F132XP-15      ok
Mod  Sw              Hw
Mod  MAC-Address(es)                         Serial-Num
Mod  Online Diag Status
Left ejector CLOSE, Right ejector CLOSE, Module HW does support ejector based shutdown.
switch#
```

Navigating Cisco NX-OS Modes from the tclsh Command

You can change modes in Cisco NX-OS while you are running an interactive tcl shell.

SUMMARY STEPS

1. **tclsh**
2. **configure terminal**
3. **tclquit**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**tclsh**
	Example:
	`switch# tclsh`
	`switch-tcl#`
		Starts an interactive tcl shell.

Step 2	**configure terminal**
	Example:
	`switch-tcl# configure terminal`
	`switch(config-tcl)#`
		Runs a Cisco NX-OS command in the tcl shell, changing modes.
		Note
		The tcl prompt changes to indicate the Cisco NX-OS command mode.

Step 3	**tclquit**
	Example:
	`switch-tcl# tclquit`
	`switch#`
		Terminates the tcl shell and returns to the starting mode.

Example

This example shows how to change Cisco NX-OS modes from an interactive tcl shell:

```
switch# tclsh
switch-tcl# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-tcl)# interface loopback 10
switch(config-if-tcl)# ?
  description  Enter description of maximum 80 characters
  inherit      Inherit a port-profile
  ip           Configure IP features
  ipv6         Configure IPv6 features
  logging      Configure logging for interface
  no           Negate a command or set its defaults
  rate-limit   Set packet per second rate limit
  shutdown     Enable/disable an interface
  this         Shows info about current object (mode's instance)
  vrf          Configure VRF parameters
  end          Go to exec mode
  exit         Exit from command interpreter
  pop          Pop mode from stack or restore from name
  push         Push current mode to stack or save it under name
  where        Shows the cli context you are in

switch(config-if-tcl)# description loop10
switch(config-if-tcl)# tclquit
Exiting Tcl
switch#
```

Tcl References

The following titles are provided for your reference:

- Mark Harrison (ed), *Tcl/Tk Tools*, O'Reilly Media, ISBN 1-56592-218-2, 1997
- Mark Harrison and Michael McLennan, *Effective Tcl/Tk Programming*, Addison-Wesley, Reading, MA, USA, ISBN 0-201-63474-0, 1998
- John K. Ousterhout, *Tcl and the Tk Toolkit*, Addison-Wesley, Reading, MA, USA, ISBN 0-201-63337-X, 1994.
- Brent B. Welch, *Practical Programming in Tcl and Tk*, Prentice Hall, Upper Saddle River, NJ, USA, ISBN 0-13-038560-3, 2003.
- J Adrian Zimmer, *Tcl/Tk for Programmers*, IEEE Computer Society, distributed by John Wiley and Sons, ISBN 0-8186-8515-8, 1998.

CHAPTER 16

Intersight Device Connector

This chapter describes how to connect devices in a secure way to send information and receive control instructions on Cisco MDS 9000 Family switches.

- Device Connector, on page 215
- Guidelines and Limitations for Device Connector, on page 216
- Configuring NXDC, on page 216
- Verify Intersight, on page 218

Device Connector

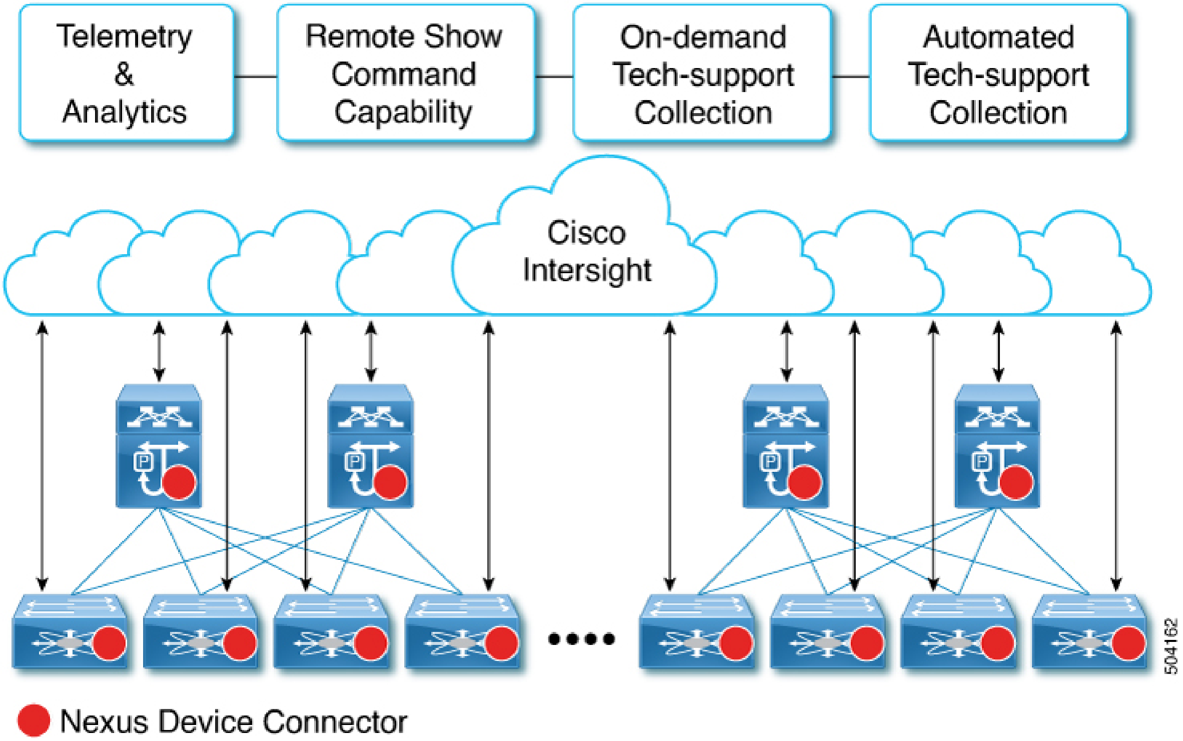
Beginning with Cisco NX-OS MDS 9000 Release 9.3(2), the Device Connector on NX-OS feature is supported which provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure Internet connection.

The Cisco MDS 9000 switch must properly resolve svc.intersight.com and allow outbound initiated HTTPS connections on port 443. To resolve svc.intersight.com, you must configure DNS on the Cisco MDS 9000 devices. If a proxy is required for an HTTPS connection to svc.intersight.com, the proxy can be configured in the NXDC user interface. .

The NXDC is enabled by default on all Cisco MDS 9000 series switches and it starts at boot by default, and attempts to connect to the cloud service. Once a secure connection has been established and the device connector is registered with the Intersight service, the device connector collects detailed inventory, health status and sends the adoption telemetry data to the Intersight database. Inventory is refreshed once in a day.

The NXDC feature integration resolves not managed switches with the following capabilities:

- It provides fast and quick solution to gather basic data from unmanaged switches.
- It stores private and organized data of all devices in a single location.
- It manages the data securely in the cloud.
- It is flexible for future extensions and upgradability.


Telemetry & Analytics
Remote Show Command Capability
On-demand Tech-support Collection
Automated Tech-support Collection
Cisco Intersight
504162
● Nexus Device Connector

Guidelines and Limitations for Device Connector

The following are the guidelines and limitations for Device Connector.

- Extra port may be displayed during a port scan. The ports are seen only in the local IPv4 or IPv6.

Supported Platforms

The following platforms support Intersight device connector feature:

- MDS 9124V 64 Gbps 24-Port Fibre Channel switch
- MDS 9132T 32 Gbps 32-Port Fibre Channel switch
- MDS 9148T 32 Gbps 48-Port Fibre Channel switch
- MDS 9148V 64 Gbps 48-Port Fibre Channel switch
- MDS 9396T 32 Gbps 96-Port Fibre Channel switch
- MDS 9396V 64 Gbps 96-Port Fibre Channel switch

Configuring NXDC

To configure NXDC, follow the below steps:

Note By default the NXDC feature is enabled.

Procedure

Step 1 Configure **terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 **feature intersight**

Example:

```
switch(config)# feature intersight
```

Step 3 (Optional)**intersight proxy** *<proxy-name>* **port** *<proxy-port>*

Example:

```
switch(config)# intersight proxy proxy.esl.cisco.com port 8080
```

Configures the proxy server for intersight connection.

- *proxy-name*: IPv4 or IPv6 address or DNS name of proxy server.
- *proxy-port*: Proxy port number. The range is 1-65535. The default value is 8080.

Note
If Proxy is enabled with the smart license configuration on Cisco MDS 9000 switches, the NXDC inherits this configuration and attempts to connect with Cisco Intersight Cloud.

Step 4 (Optional)**intersight connection** *<name>*

Example:

```
switch(config)# intersight connection qaconnect.starshipcloud.com
```

Sets the DNS name for intersight connection. It can be used to change from intersight to NDSaaS.

- *name*: Name value is string. The maximum size is 128.

Step 5 (Optional)**intersight trustpoint** *<trustpoint-label>*

Example:

```
switch(config)#intersight trustpoint mds-stage-onprem
```

Configures certificates for intersight connection.

trustpoint-label: Crypto ca truspoint label. For more information refer to *Cisco MDS 9000 Series NX-OS Security Configuration Guide*.

Verify Intersight

Verify the Intersight feature for these components:

- device connector system information: system status and connectivity
- device connections: network path and status
- device details: specifications and operation details

Verify NXDC

Use **show system internal intersight info** to display the device connector system information.

```
switch(config)# show system internal intersight info
Intersight connector.db Info:
AccountOwnershipState   :Not Claimed
AccountOwnershipUser    :
AccountOwnershipTime    :0001-01-01T00:00:00Z
AccountOwnershipId      :
DomainGroupMoid         :1234567890abcd
AccountMoid             :1234567890abcd
CloudDns                :svc.example.com
CloudDnsList:
        1.              :svc-static1.ucs-connect.com
        2.              :svc.ucs-connect.com
        3.              :svc.intersight.com
        4.              :svc-static1.intersight.com
Identity                :1234567890
CloudEnabled            :true
ReadOnlyMode            :false
LocalConfigLockout      :false
TunneledKVM             :false
HttpProxy:
        ProxyHost       :proxy.example.com
        ProxyPort       :80
        Preferenc       :0
        ProxyType       :Manual
    Target[1]:
        ProxyHost       :proxy.example.com
        ProxyPort       :80
        Preference      :0
LogLevel                :info
DbVersion               :1
AutoUpgradeAdminState   :Automatic
```

Use **show system internal intersight connection-state** to display the device connections.

```
switch(config)# show system internal intersight connection-state
AdminState                :  true
ReadOnlyMode              :  false
ConnectionState           :  Connected
ConnectionStateQualifier  :
ConnectionLastDownTimeTs  :  2022-12-09T11:21:33.653652476Z
AccountOwnershipState     :  Not Claimed
AccountOwnershipUser      :
AccountOwnershipTime      :  0001-01-01T00:00:00Z
AccountOwnershipName      :
Leadership                :  Primary
DeviceRegistrationMoid    :  1234567890abcd
```

Verify device details

Use **show system device-connector claim-info** to display the device details such as device id and claim code.

```
switch# show system device-connector claim-info
  SerialNumber: ABCD1234
  SecurityToken: XYZ1234
  Duration: 599
  Message:
  Claim state: Not Claimed
```

Telemetry data collected for Intersight

Telemetry data from the switch is sent to Intersight as described in the table:

Table 36: Telemetry collected for Intersight

Type	Data
Inventory	Device Name
	Product Type
	Version
	Serial number
	CPU average load
	Memory usage
	Disk name, usage
	Device Up Time
	Device ID
	Interface information such as: • **name** • **up count** • **down count** • **operational state** • **transceiver status**
	Telnet enable status
	Bootflash model, serial number
	Last Reboot Time
	Last Reset Reason
	System Up Time

Type	Data
License details	List of activated licenses
Feature details	List of activated features
Power Supply details	Product Id
	Serial Number
	Vendor Id
Fan details	Product Id
	Serial Number
	Vendor Id
Module details	Product Id
	Serial Number
	Vendor Id
Transceiver Details	Product Id
	Serial Number
	Vendor Id
	Part Number
Neighbor details	WWN of the neighbor switches in the fabric