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, LOSS 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.

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

© 2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

Full Cisco Trademarks with Software License  

PREFACE

Preface xiii
  Audience xiii
  Document Conventions xiii
  Related Documentation xiv
  Communications, Services, and Additional Information xvi

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 6
    Role-Based Access Control 6
  Cisco NX-OS Software Configuration 6
    Tools for Software Configuration 7
      CLI 7
# Cisco MDS 9000 Series Fundamentals Configuration Guide, Release 8.x

## Contents

### CHAPTER 3

**Using the Cisco NX-OS Setup Utility**
- Information About the Cisco NX-OS Setup Utility
- Prerequisites for the Setup Utility
- Initial Setup Routine
  - Configuring Out-of-Band Management
  - Configuring In-Band Management
- Where to Go Next

### CHAPTER 4

**Using PowerOn Auto Provisioning**
- Using Power On Auto Provisioning
  - About Power On Auto Provisioning
  - POAP Configuration Script
    - Guidelines and Limitations for POAP Configuration
    - Network Infrastructure Requirements for POAP
  - Setting Up the Network Environment to use POAP
- The POAP Process
  - The Power-Up Phase
  - The USB Discovery Phase
  - The DHCP Discovery Phase
  - Script Execution Phase
  - Post-Installation Reload Phase
- Configuring a Switch Using POAP
- Verifying the Device Configuration

### CHAPTER 5

**Understanding the Command-Line Interface**
- Information About the CLI Prompt
- Command Modes
  - EXEC Command Mode
  - Global Configuration Command Mode
  - Interface Configuration Command Mode
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subinterface Configuration Command Mode</td>
<td>39</td>
</tr>
<tr>
<td>Saving and Restoring a Command Mode</td>
<td>40</td>
</tr>
<tr>
<td>Command Mode Summary</td>
<td>40</td>
</tr>
<tr>
<td>Special Characters</td>
<td>41</td>
</tr>
<tr>
<td>Keystroke Shortcuts</td>
<td>41</td>
</tr>
<tr>
<td>Abbreviating Commands</td>
<td>43</td>
</tr>
<tr>
<td>Completing a Partial Command Name</td>
<td>44</td>
</tr>
<tr>
<td>Identifying Your Location in the Command Hierarchy</td>
<td>44</td>
</tr>
<tr>
<td>Using the no Form of a Command</td>
<td>45</td>
</tr>
<tr>
<td>Configuring CLI Variables</td>
<td>46</td>
</tr>
<tr>
<td>About CLI Variables</td>
<td>46</td>
</tr>
<tr>
<td>Configuring CLI Session-Only Variables</td>
<td>47</td>
</tr>
<tr>
<td>Configuring Persistent CLI Variables</td>
<td>47</td>
</tr>
<tr>
<td>Command Aliases</td>
<td>48</td>
</tr>
<tr>
<td>About Command Aliases</td>
<td>48</td>
</tr>
<tr>
<td>Defining Command Aliases</td>
<td>49</td>
</tr>
<tr>
<td>Configuring Command Aliases for a User Session</td>
<td>49</td>
</tr>
<tr>
<td>Command Scripts</td>
<td>50</td>
</tr>
<tr>
<td>Running a Command Script</td>
<td>50</td>
</tr>
<tr>
<td>Echoing Information to the Terminal</td>
<td>50</td>
</tr>
<tr>
<td>Delaying Command Action</td>
<td>51</td>
</tr>
<tr>
<td>Context-Sensitive Help</td>
<td>52</td>
</tr>
<tr>
<td>Understanding Regular Expressions</td>
<td>53</td>
</tr>
<tr>
<td>Special Characters</td>
<td>53</td>
</tr>
<tr>
<td>Multiple-Character Patterns</td>
<td>54</td>
</tr>
<tr>
<td>Anchoring</td>
<td>54</td>
</tr>
<tr>
<td>Searching and Filtering show Command Output</td>
<td>55</td>
</tr>
<tr>
<td>Filtering and Searching Keywords</td>
<td>55</td>
</tr>
<tr>
<td>diff Utility</td>
<td>57</td>
</tr>
<tr>
<td>grep and egrep Utilities</td>
<td>57</td>
</tr>
<tr>
<td>less Utility</td>
<td>58</td>
</tr>
<tr>
<td>sed Utility</td>
<td>58</td>
</tr>
<tr>
<td>sort Utility</td>
<td>58</td>
</tr>
<tr>
<td>Redirecting show Command Output Using sscp</td>
<td>59</td>
</tr>
</tbody>
</table>
Format an External Flash Device 97
Mounting or Unmounting a USB Drive 97
External Storage Device Support Matrix 97

Working with Directories 98
Identifying the Current Directory 98
Changing the Current Directory 99
Creating a Directory 99
Displaying Directory Contents 99
Deleting a Directory 99
Accessing the Directories on a Standby Supervisor Module 100

Working with Files 100
Moving a File 100
Copying a File 101
Deleting a File 101
Displaying a File's Contents 101
Displaying a File's Checksums 102
Compressing and Uncompressing a File 102
Displaying the Last Lines in a File 103
Redirecting show Command Output to a File 103
Finding Files 103

Working with Archive Files 103
Creating an Archive File 103
Appending Files to an Archive File 104
Extracting Files from an Archive File 105
Displaying the Filenames in an Archive File 105

Examples of Using a File System 105
Accessing Directories on a Standby Supervisor Module 106
Performing ISSU or ISSD Using a USB Drive 106

CHAPTER 9

Working with Configuration Files 107
Information About Configuration Files 107
Types of Configuration Files 107
Managing Configuration Files 108
Saving the Running Configuration to the Startup Configuration 108

Cisco MDS 9000 Series Fundamentals Configuration Guide, Release 8.x
<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>Information About CDP</th>
<th>Configuring CDP</th>
<th>Default Settings for CDP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuring CDPP 122</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabling or Disabling CDP Globally 122</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabling or Disabling CDP on an Interface 122</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verifying the CDP Configuration 124</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clearing CDP Counters and Tables 124</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CDP Example Configuration 125</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11</th>
<th>Information About NTP</th>
<th>Configuring NTP</th>
<th>Prerequisites for NTP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NTP 127</td>
<td></td>
<td>Guidelines and Limitations for NTP 129</td>
</tr>
</tbody>
</table>
Configuring NTP  129
Enabling NTP  129
Disabling NTP  129
Configuring Authentication Keys  130
Enabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations  130
Disabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations  131
Enabling NTP Servers and Peers  131
Disabling NTP Servers and Peers  132
Enabling NTP Modes  132
Disabling NTP Modes  133
Enabling NTP Source Interface  133
Disabling NTP Source Interface  133
Enabling NTP Logging  134
Disabling NTP Logging  134
Configuring NTP Syslog Logging Level  134
Setting the Default NTP Syslog Severity Logging Level  135
Displaying and Clearing NTP Statistics  135
Resynchronizing NTP  136
Distributing the NTP Configuration Using CFS  136
   Enabling NTP Configuration Distribution  136
   Disabling NTP Configuration Distribution  137
   Committing NTP Configuration Changes  137
   Discarding NTP Configuration Changes  137
   Forcing Termination of a Lost NTP Configuration Session  138
Verifying NTP  138
Troubleshooting NTP  139
Example: Configuring NTP  141
Default Settings for NTP  143

CHAPTER 12  Managing System Hardware  145
   Displaying Switch Hardware Inventory  145
   Running CompactFlash Tests  149
   Displaying the Switch Serial Number  149
   Displaying Power Usage Information  150
Power Supply Modes 151
  Configuration Guidelines for Power Supplies 152
  Configuring the Power Supply Mode 159
About Module Temperature Monitoring 160
  Displaying Module Temperatures 160
About Fan Modules 162
Displaying Environment Information 163
Default Settings 165

CHAPTER 13 Managing Modules 167
About Modules 167
  Supervisor Modules 168
  Switching Modules 169
  Services Modules 170
Maintaining Supervisor Modules 170
  Replacing Supervisor Modules 170
  Standby Supervisor Module Boot Variable Version 170
  Standby Supervisor Module Bootflash Memory 170
  Standby Supervisor Module Boot Alert 170
Verifying the Status of a Module 171
Checking the State of a Module 172
Connecting to a Module 172
Reloading Modules 173
  Reloading a Switch 173
  Power Cycling Modules 173
  Reloading Switching Modules 174
Saving the Module Configuration 174
Purging Module Configurations 175
Powering Off Switching Modules 176
Identifying Module LEDs 177
EPLD Images 182
  Upgrading EPLD Images 183
  Displaying EPLD Image Versions 187
SSI Boot Images 188
Preface

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

- Audience, on page xiii
- Document Conventions, on page xiii
- Related Documentation, on page xiv
- Communications, Services, and Additional Information, on page xvi

Audience

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

Document Conventions

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

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates the commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text indicates arguments for which the user supplies the values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
</tbody>
</table>
### Related Documentation

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


Cisco DCNM documentation is available at the following URL:

Release Notes

- Cisco MDS 9000 Series Release Notes for Cisco MDS NX-OS Releases
- Cisco MDS 9000 Series Release Notes for MDS SAN-OS Releases
- Cisco MDS 9000 Series Release Notes for Storage Services Interface Images
- Cisco MDS 9000 Series Release Notes for Cisco MDS 9000 EPLD Images
- Cisco Data Center Network Manager Release Notes

Regulatory Compliance and Safety Information

Regulatory Compliance and Safety Information for the Cisco MDS 9000 Series

Compatibility Information

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

Hardware Installation

- Cisco MDS 9700 Director Hardware Installation Guide
- Cisco MDS 9500 Series Hardware Installation Guide
- Cisco MDS 9250i Multiservice Switch Hardware Installation Guide
- Cisco MDS 9200 Series Hardware Installation Guide

Software Installation and Upgrade

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

Cisco NX-OS

- Cisco MDS 9000 Series NX-OS Fundamentals Configuration Guide
- Cisco MDS 9000 Series NX-OS Licensing Guide
- Cisco MDS 9000 Series NX-OS System Management Configuration Guide
- Cisco MDS 9000 Series NX-OS Interfaces Configuration Guide
Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
<th>Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistency Checker</td>
<td>Added support to display the access control list (ACL), forwarding information base (FIB), and persistent storage service (PSS) consistency information, using the <code>show consistency-checker</code> command.</td>
<td>8.4(1)</td>
<td>Overview, on page 3</td>
</tr>
</tbody>
</table>
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 6
- Licensing, on page 8
- 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.

**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](image)

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.
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.
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 25

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.
Prerequisites for the Setup Utility

The setup utility has the following prerequisites:

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

Initial Setup Routine

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

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

Configuring Out-of-Band Management

You can configure out-of-band management on the mgmt0 interface.

Note

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

Step 1

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

Step 2

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

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

Note

You can also enable secure password standard using the password strength-check command. A secure password should contain characters from at least three of the classes: lower case letters, upper case letters, digits, and special characters.
Step 3

Enter the new password for the administrator.

Enter the password for admin: admin-password

Confirm the password for admin: admin-password

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

Step 4

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

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

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

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

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

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

Step 5

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

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

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

**Note** User login IDs must contain non-numeric characters.

a) Enter the user login ID.

   Enter the user login ID: user_name

b) Enter and confirm the user password.

   Enter the password for user_name: user-password

   Confirm the password for user_name: user-password

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

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

Step 6

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

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

b) Enter the SNMP community string.

```
SNMP community string: snmp_community
```

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

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

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

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

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

a) Enter the mgmt0 IPv4 address.

```
Mgmt0 IPv4 address: ip_address
```

b) Enter the mgmt0 IPv4 subnet mask.

```
Mgmt0 IPv4 netmask: subnet_mask
```

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

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

a) Enter the default gateway IP address.

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

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

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

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

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

b) Enter **yes** (**yes** is the default) to enable IPv4 routing capabilities.
Enable ip routing capabilities? (yes/no) [y]: yes

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

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

Enter the destination prefix.

Destination prefix: dest_prefix

Enter the destination prefix mask.

Destination prefix mask: dest_mask

Enter the next hop IP address.

Next hop ip address: next_hop_address

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

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

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

Enter the default network IPv4 address.

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

Default network IP address [dest_prefix]: dest_prefix

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

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

Enter the DNS IP address.

DNS IP address: name_server

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

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

Enter the default domain name.
Default domain name: `domain_name`

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

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

Enter the SSH key type.

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

Enter the number of key bits within the specified range.

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

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

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

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

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

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

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

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

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

**Step 16**  
Enter a mode for congestion or no_credit drop.

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

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

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

Enter the NTP server IPv4 address.

NTP server IP address: `ntp_server_IP_address`

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

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

**Note**  
The management Ethernet interface is not shut down at this point. Only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.
Step 19 Enter on (off is the default) to configure the switch port trunk mode.

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

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

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

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

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

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

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

Permits traffic flow to all members of the default zone.

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

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

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

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

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

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

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

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

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

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

Overrides the switch-wide default zone mode as enhanced.
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
do 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 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.
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 switchport trunk mode.
18. Enter **yes** (yes is the default) to configure the switchport mode F.
19. Enter **off** (off is the default) to configure the PortChannel auto-create state.
20. Enter **deny** (deny is the default) to deny a default zone policy configuration.
21. Enter **no** (no is the default) to disable a full zone set distribution.
22. Enter **enhanced** (basic is the default) to configure default-zone mode as enhanced.
23. Enter **no** (no is the default) if you are satisfied with the configuration.
24. Enter **yes** (yes is default) to use and save this configuration.

**DETAILED STEPS**

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

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 shutdown
  ip default-gateway default_gateway
  no telnet server
disable
  ssh key rsa 2048 force
  ssh server enable
  system default switchport shutdown
  autosystem default switchport mode
  system 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) for the Cisco MDS 9148, 9148s, 9250i, and 9396s Multilayer Fabric Switches and Cisco MDS 9700 and MDS 9500 Multilayer Director-class switches.

This chapter contains the following sections:

• Using Power On Auto Provisioning, on page 27

Using Power On Auto Provisioning

This chapter describes how to deploy and use Power On Auto Provisioning (POAP) for Cisco Multilayer Director Switch (MDS) 9148, Cisco MDS 9148S, Cisco MDS 9250i, Cisco MDS 9396S Multilayer Fabric Switches, and Cisco MDS 9700 and MDS 9500 Multilayer Director-class switches.

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 server’s interface IP address, gateway, and DNS server IP addresses. 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.

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 both Cisco MDS 9700 and 9500 series switches, POAP is supported only on USB 1 Port.
- The software image for the Cisco MDS 9000 Series Switches, including the Cisco MDS 9396S Multilayer Fabric Switch, must support POAP.
  POAP via USB is supported from Cisco MDS NX-OS Release 7.3(0)D1(1).
- POAP can be initiated on any 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_hhmms 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_hhmms 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 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 and SCP 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.tcl.
- 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:

  ```bash
  switch# show sprom backplane 1
  DISPLAY backplane sprom contents:
  Common block:
  ```
• 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 9148s switch with the m9100-s5ek9-kickstart-mz.7.3.0.D1.0.159.bin and m9100-s5ek9-mz.7.3.0.D1.0.159.bin images, ensure that the POAP configuration script (poap_script.tcl) has the following information:

• set m9148s_image_version 7.3.0.D1.0.159

• set m9148s_kickstart_image_src [format m9100-s5ek9-kickstart-mz.%s.bin $m9148s_image_version]

• set m9148s_system_image_src [format m9100-s5ek9-mz.%s.bin $m9148s_image_version]

---

**Note**  
Ensure that the POAP script identifies the switch.

---

**Note**  
• Only FAT32 USB is supported. (The file system on the USB should be FAT32). For both Cisco MDS 9700 and 9500 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

**Step 1**  
Deploy a TFTP server to host the configuration script, software images, and configuration files.

**Step 2**  
Deploy a DHCP server.

**Step 3**  
Configure the following parameters in the DHCP server:

• Interface address

• Gateway address

• TFTP server’s IP address

• Boot file name
The following example of dhcpd.conf on Linux, with boot file name, TFTP server, and script file name:

```conf
option vlan-id code 132 = unsigned integer 32;
subnet 10.105.188.0 netmask 255.255.255.0 {
  max-lease-time 7200;
  class "cisco MDS" {
    match if substring(option vendor-class-identifier, 0, 15) = "cisco MDS - tcl";
    option bootfile-name "poap_script.tcl";
    option subnet-mask 255.255.255.0;
    option domain-name "cisco.com";
  }
  option routers 10.105.188.1;
  option tftp-server-name "10.105.188.159";
}
```

**Step 4** To obtain the serial number of the switch, execute the `show sprom backplane 1` command.

**Step 5** Create a separate directory for each switch in the base directory of the TFTP server. The name of each directory should be the same as the serial number of the switch. Creating a separate directory for each switch enables you to have separate software images or configuration files for different switches.

**Note** The base directory should contain the software images (kickstart and system images) and the server-list.cfg file. The file names of the software images should match poap_script.tcl and device-recipe.cfg.

In the newly created directory for each switch, maintain the device-recipe.cfg and the conf_SN.cfg file.

(Replace SN with the exact serial number of the corresponding switch.)

The following is an example of device-recipe.cfg:

```json
{"serial-number":"JAF1735307V","kick-start-image":{"image-name":"MDS9148S_boot","download-server": "Default_SCP_Repository"},"system-image":{"image-name":"MDS9148S_isan","download-server": "Default_SCP_Repository"},"startup-config":{"config-name":"conf_JAF1735307V.cfg","download-server": "Default_SCP_Repository"}}
```

The following is an example of server-list.cfg:

```json
{
    "repositories": {"Default_SCP_Repository":{"url":"scp://server_IP/directory_path","username": "user","password": "password","last-modified-time":"Mon Mar 24 00:22:33 PDT 2014"} },
    "resources":{ }
}
```

**Note** You can download all the sample files for the POAP process from the following link:


**Note** Ensure that you select the correct version of the Cisco MDS NX-OS release before downloading the sample files.

---

**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**

---

**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 abort 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 abort POAP remains available until the POAP process is complete.

If you exit the POAP mode, you enter a script. If you continue in the POAP mode, all the front-panel interfaces are set up in the default configuration.
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.tcl), 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 abort 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 34.) 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

The POAP process has to be aborted 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 bootfile name includes the complete path to the bootfile on the TFTP server. The DHCP client uses this information to download the script file.

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

If 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 aborted because the switch reverts to the USB phase.
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.

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.

---

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 abort 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).

The switch boots, and the POAP process begins.

---

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Displays the running configuration.</td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays the startup configuration.</td>
</tr>
</tbody>
</table>

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 41
- Abbreviating Commands, on page 43
- Completing a Partial Command Name, on page 44
- Identifying Your Location in the Command Hierarchy, on page 44
- 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 59
- Using the Command History, on page 60
- Enabling or Disabling the CLI Confirmation Prompts, on page 62
- Setting CLI Display Colors, on page 62
- 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.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
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

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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal switch(config)#</td>
</tr>
</tbody>
</table>

| **Step 2** | Specifies the VLAN interface to be configured. |
| interface type number.subint | |
| Example: | switch(config)# interface ethernet 2/2.1 switch(config-subif)# |

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>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>From the login prompt, enter your username and password.</td>
<td>switch#</td>
<td>To exit to the login prompt, use the exit command.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>From EXEC mode, use the configure terminal command.</td>
<td>switch(config)#</td>
<td>To exit to EXEC mode, use the end or exit command or press Ctrl-Z.</td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>Percent</td>
</tr>
<tr>
<td>#</td>
<td>Pound, hash, or number</td>
</tr>
<tr>
<td>...</td>
<td>Ellipsis</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Less than or greater than</td>
</tr>
<tr>
<td>[ ]</td>
<td>Brackets</td>
</tr>
<tr>
<td>{ }</td>
<td>Braces</td>
</tr>
</tbody>
</table>

### Keystroke Shortcuts

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

**Table 4: Keystroke Shortcuts**

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-A</td>
<td>Moves the cursor to the beginning of the line.</td>
</tr>
<tr>
<td>Keystrokes</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ctrl-B</td>
<td>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.</td>
</tr>
<tr>
<td>Ctrl-C</td>
<td>Cancels the command and returns to the command prompt.</td>
</tr>
<tr>
<td>Ctrl-D</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Moves the cursor to the end of the line.</td>
</tr>
<tr>
<td>Ctrl-F</td>
<td>Moves the cursor one character to the right.</td>
</tr>
<tr>
<td>Ctrl-G</td>
<td>Exits to the previous command mode without removing the command string.</td>
</tr>
<tr>
<td>Ctrl-K</td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl-L</td>
<td>Redisplays the current command line.</td>
</tr>
<tr>
<td>Ctrl-N</td>
<td>Displays the next command in the command history.</td>
</tr>
<tr>
<td>Ctrl-O</td>
<td>Clears the terminal screen.</td>
</tr>
<tr>
<td>Ctrl-P</td>
<td>Displays the previous command in the command history.</td>
</tr>
<tr>
<td>Ctrl-R</td>
<td>Redisplays the current command line.</td>
</tr>
<tr>
<td>Ctrl-T</td>
<td>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.</td>
</tr>
<tr>
<td>Ctrl-U</td>
<td>Deletes all characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl-V</td>
<td>Removes any special meaning for the following keystroke. For example, press Ctrl-V before entering a question mark (?) in a regular expression.</td>
</tr>
<tr>
<td>Ctrl-W</td>
<td>Deletes the word to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl-X, H</td>
<td>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.</td>
</tr>
<tr>
<td>Ctrl-Y</td>
<td>Recalls the most recent entry in the buffer (press keys simultaneously).</td>
</tr>
<tr>
<td>Ctrl-Z</td>
<td>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.</td>
</tr>
<tr>
<td>Up arrow key</td>
<td>Displays the previous command in the command history.</td>
</tr>
<tr>
<td>Down arrow key</td>
<td>Displays the next command in the command history.</td>
</tr>
</tbody>
</table>
### 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.

#### Abbreviations

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right arrow key</td>
<td>Moves your cursor through the command string, either forward or backward, allowing you to edit the current command.</td>
</tr>
<tr>
<td>Left arrow key</td>
<td>?</td>
</tr>
<tr>
<td>Tab</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Command names</td>
</tr>
<tr>
<td></td>
<td>• Scheme names in the file system</td>
</tr>
<tr>
<td></td>
<td>• Server names in the file system</td>
</tr>
<tr>
<td></td>
<td>• Filenames in the file system</td>
</tr>
</tbody>
</table>

#### 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-
```
This table lists examples of command abbreviations.

### Table 5: Examples of Command Abbreviations

<table>
<thead>
<tr>
<th>Command</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>con t</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>copy run start</td>
</tr>
<tr>
<td>interface ethernet 1/2</td>
<td>int e 1/2</td>
</tr>
<tr>
<td>show running-config</td>
<td>sh run</td>
</tr>
</tbody>
</table>

### 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 you 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>where detail</td>
<td>Displays the PWC.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)# interface mgmt0</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# where detail</td>
<td></td>
</tr>
<tr>
<td>mode: conf</td>
<td></td>
</tr>
<tr>
<td>interface mgmt0</td>
<td></td>
</tr>
<tr>
<td>username: admin</td>
<td></td>
</tr>
</tbody>
</table>

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
```
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 $\text{(variable-name)}$.

**SUMMARY STEPS**

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

**DETAILED STEPS**

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

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example: | switch# configure terminal  
switch(config)# |
| **Step 2**  |  |
| `cli var name variable-name variable-text` | 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. |
| Example: |  |
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:**  
  switch# configure terminal  
  switch(config)# | |
| **Step 2** `cli alias name alias-name alias-text` | 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. |
| **Example:**  
  switch(config)# cli alias name ethint interface ethernet | |
| **Step 3** `exit` | Exits global configuration mode. |
| **Example:**  
  switch(config)# exit  
  switch# | |
| **Step 4** (Optional) `alias` | Displays the command alias configuration. |
| **Example:**  
  switch# alias | |
| **Step 5** (Optional) `copy running-config startup-config` | Copies the running configuration to the startup configuration. |
| **Example:**  
  switch# copy running-config startup-config | |

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>terminal alias [persist] alias-name command -string</code></td>
<td>Configures a command alias for the current user session. Use the <code>persist</code> keyword to save the alias for future use by the user account.</td>
</tr>
<tr>
<td>Example: <code>switch# terminal alias shintbr show interface brief</code></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 `run-script [bootflash:</td>
<td>slot0:</td>
</tr>
<tr>
<td>Example: <code>switch# run-script testfile</code></td>
<td></td>
</tr>
</tbody>
</table>

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

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>echo [backslash-interpret] [text]</td>
<td>The <code>backslash-interpret</code> keyword indicates that the text string contains formatting options. The <code>text</code> argument is alphanumeric, case sensitive, and can contain blanks. The maximum length is 200 characters. The default is a blank line.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> sleep seconds</td>
<td>Causes a delay for a number of seconds. The range is from 0 to 2147483647.</td>
</tr>
<tr>
<td>Example: switch# sleep 30</td>
<td></td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Example Outputs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# clock ?</td>
<td>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.</td>
</tr>
<tr>
<td>set HH:MM:SS Current Time</td>
<td></td>
</tr>
<tr>
<td>switch# clock</td>
<td></td>
</tr>
<tr>
<td>switch# clock set ?</td>
<td>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.</td>
</tr>
<tr>
<td>WORD HH:MM:SS Current Time</td>
<td></td>
</tr>
<tr>
<td>switch# clock set</td>
<td></td>
</tr>
<tr>
<td>switch# clock set 13:32:00&lt;CR&gt;</td>
<td>Adds the current time. The CLI indicates the command is incomplete.</td>
</tr>
<tr>
<td>% Incomplete command</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td>switch# &lt;Ctrl-P&gt;</td>
<td>Displays the previous command that you entered.</td>
</tr>
<tr>
<td>switch# clock set 13:32:00</td>
<td></td>
</tr>
<tr>
<td>switch# clock set 13:32:00 ?</td>
<td>Displays the additional arguments for the clock set command.</td>
</tr>
<tr>
<td>&lt;1-31&gt; Day of the month</td>
<td></td>
</tr>
<tr>
<td>switch# clock set 13:32:00</td>
<td></td>
</tr>
</tbody>
</table>
**Example Outputs**

<table>
<thead>
<tr>
<th>Description</th>
<th>Example Outputs</th>
</tr>
</thead>
</table>
| 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 | Adds the date to the clock setting. The CLI indicates an error with the caret symbol (^) at 08. |
| Displays the correct arguments for the year.                                | `switch# clock set 13:32:00 18 April ?
<2000-2030> Enter the year (no abbreviation)
switch# clock set 13:32:00 18 April | 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*

<table>
<thead>
<tr>
<th>Character</th>
<th>Special Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Matches any single character, including white space.</td>
</tr>
<tr>
<td>*</td>
<td>Matches 0 or more sequences of the pattern.</td>
</tr>
<tr>
<td>+</td>
<td>Matches 1 or more sequences of the pattern.</td>
</tr>
<tr>
<td>?</td>
<td>Matches 0 or 1 occurrences of the pattern.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Matches the beginning of the string.</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of the string.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Keyword Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>begin string</code></td>
<td>Starts displaying at the line that contains the text that matches the search string. The search string is case sensitive.</td>
</tr>
<tr>
<td><code>count</code></td>
<td>Displays the number of lines in the command output.</td>
</tr>
</tbody>
</table>

```
switch# show running-config | count
```
<table>
<thead>
<tr>
<th>Keyword Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cut [-d character] { -b</td>
<td>-c</td>
</tr>
<tr>
<td>end string</td>
<td>Displays all lines up to the last occurrence of the search string. Example: show running-config</td>
</tr>
<tr>
<td>exclude string</td>
<td>Displays all lines that do not include the search string. The search string is case sensitive. Example: show interface brief</td>
</tr>
<tr>
<td>head [lines lines]</td>
<td>Displays the beginning of the output for the number of lines specified. The default number of lines is 10. Example: show logging logfile</td>
</tr>
<tr>
<td>include string</td>
<td>Displays all lines that include the search string. The search string is case sensitive. Example: show interface brief</td>
</tr>
<tr>
<td>last [lines]</td>
<td>Displays the end of the output for the number of lines specified. The default number of lines is 10. Example: show logging logfile</td>
</tr>
<tr>
<td>no-more</td>
<td>Displays all the output without stopping at the end of the screen with the --More-- prompt. Example: show interface brief</td>
</tr>
<tr>
<td>sscp SSH-connection-name filename</td>
<td>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. Example: show version</td>
</tr>
<tr>
<td>wc [bytes</td>
<td>lines</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-sessions</td>
<td>Removes diff temporary files from all sessions (past and present sessions) of the current user.</td>
</tr>
<tr>
<td>all-users</td>
<td>Removes diff temporary files from all sessions (past and present sessions) of all users.</td>
</tr>
</tbody>
</table>

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 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**

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

```
```

This table describes the sort utility parameters.

Table 12: sort Utility Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-M</td>
<td>Sorts by month.</td>
</tr>
<tr>
<td>-b</td>
<td>Ignores leading blanks (space characters). The default sort includes the leading blanks.</td>
</tr>
<tr>
<td>-d</td>
<td>Sorts by comparing only blanks and alphanumeric characters. The default sort includes all characters.</td>
</tr>
<tr>
<td>-f</td>
<td>Folds lowercase characters into uppercase characters.</td>
</tr>
<tr>
<td>-g</td>
<td>Sorts by comparing a general numeric value.</td>
</tr>
<tr>
<td>-i</td>
<td>Sorts only using printable characters. The default sort includes nonprintable characters.</td>
</tr>
<tr>
<td>-k field-number,char-position][ordering]</td>
<td>Sorts according to a key value. There is no default key value.</td>
</tr>
<tr>
<td>-n</td>
<td>Sorts according to a numeric string value.</td>
</tr>
</tbody>
</table>
### Table 13: --More-- Prompt Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[lines]&lt;space&gt;</td>
<td>Displays output lines for either the specified number of lines or the current screen size.</td>
</tr>
<tr>
<td>[lines]z</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

```plaintext
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
```
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] terminal edit-mode vi [persist]</code></td>
<td>Changes the CLI edit mode to vi for the user session. The <code>persist</code> keyword makes the setting persistent across sessions for the current username. Use the <code>no</code> to revert to using emacs.</td>
</tr>
</tbody>
</table>

### 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:
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>[no] terminal dont-ask [persist]</td>
</tr>
</tbody>
</table>

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

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

SUMMARY STEPS

1. terminal color [evening] [persist]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>terminal color [evening] [persist]</td>
</tr>
</tbody>
</table>

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
```

```diff
*** /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)
--- 12,16 ----
! 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
```
Using the System-Defined Timestamp Variable

This example uses $\text{(TIMESTAMP)}$ when redirecting \textit{show} command output to a file:

```
switch# \texttt{show running-config > rcfg.$\text{(TIMESTAMP)}}
Preparing to copy....done
switch# \texttt{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# \texttt{show file testfile}
configure terminal
interface ethernet 2/1
no shutdown
end
show interface ethernet 2/1
```

This example displays the \textit{run-script} command execution output:

```
switch# \texttt{run-script testfile}
`configure terminal`
`interface ethernet 2/1`
`no shutdown`
`end`
`show interface ethernet 2/1`
Ethernet2/1 is down (Link not connected)
```
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 67
- Configuring the Console Port, on page 69
- Configuring the COM1 Port, on page 71
- Configuring Virtual Terminals, on page 72
- Configuring Modem Connections, on page 75
- Clearing Terminal Sessions, on page 79
- Displaying Terminal and Session Information, on page 79
- Default Settings for Terminal Display and Session Parameters, on page 80

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

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

The Cisco NX-OS software has the default initialization string (ATE0Q1&D2&C1S0=1\015) to detect connected modems. The default string is defined as follows:
AT
  Attention
E0 (required)
  No echo
Q1
  Result code on
&D2
  Normal data terminal ready (DTR) option
&C1
  Enable tracking the state of the data carrier
S0=1
  Pick up after one ring
\015 (required)
  Carriage return in octal

Configuring the Console Port

You can set the following characteristics for the console port:
  • Data bits
  • Inactive session timeout
  • Parity
  • Speed
  • Stop bits

Before you begin

Log in to the console port.

SUMMARY STEPS

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

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch# configure terminal  
switch(config)# | |
| **Step 2** | line console | Enters console configuration mode. |
| **Example:** | switch# line console  
switch(config-console)# | |
| **Step 3** | databits bits | Configures the number of data bits per byte. The range is from 5 to 8. The default is 8. |
| **Example:** | switch(config-console)# databits 7 | |
| **Step 4** | exec-timeout minutes | 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. |
| **Example:** | switch(config-console)# exec-timeout 30 | |
| **Step 5** | parity {even | none | odd} | Configures the parity. The default is none. |
| **Example:** | switch(config-console)# parity even | |
| **Step 6** | speed {300 | 1200 | 2400 | 4800 | 9600 | 38400 | 57600 | 115200} | Configures the transmit and receive speed. The default is 9600. |
| **Example:** | switch(config-console)# speed 115200 | |
| **Step 7** | stopbits {1 | 2} | Configures the stop bits. The default is 1. |
| **Example:** | switch(config-console)# stopbits 2 | |
| **Step 8** | exit | Exits console configuration mode. |
| **Example:** | switch(config-console)# exit  
switch(config)# | |
| **Step 9** | (Optional) show line console | Displays the console settings. |
| **Example:** | switch(config)# show line console | |
| **Step 10** | (Optional) copy running-config startup-config | Copies the running configuration to the startup configuration. |
| **Example:** | switch(config)# copy running-config startup-config | |
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 \textit{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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>line com1</td>
<td>Enters COM1 configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# line com1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-com1)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>databits \textit{bits}</td>
<td>Configures the number of data bits per byte. The range is from 5 to 8. The default is 8.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-com1)# databits 7</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Terminal Settings and Sessions

#### 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`

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><code>flowcontrol hardware</code></td>
<td>Enables flow control on the hardware. The default is enabled. Use the <code>no flowcontrol hardware</code> command to disable flow control on the hardware.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-com1)# flowcontrol hardware</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>`parity {even</td>
<td>none</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-com1)# parity even</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>`speed {300</td>
<td>1200</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-com1)# speed 115200</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>`stopbits {1</td>
<td>2}`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-com1)# stopbits 2</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>exit</code></td>
<td>Exits COM1 configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config-com1)# exit</code></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>(Optional) show line com1</code></td>
<td>Displays the COM1 port settings.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# show line com1</code></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td><code>(Optional) copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;&lt;br&gt;Example:&lt;br&gt;switch# configure terminal&lt;br&gt;switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>line vty</strong>&lt;br&gt;&lt;br&gt;Example:&lt;br&gt;switch# line vty&lt;br&gt;switch(config-line)#</td>
</tr>
</tbody>
</table>
| **Step 3** | • **exec-timeout minutes**  
• **absolute-timeout minutes**<br><br>Example:<br>switch(config-line)# exec-timeout 30<br>Example:<br>switch(config-line)# absolute-timeout 30 |
| **Step 4** | **exit**<br><br>Example:<br>switch(config-line)# exit<br>switch(config)# |
| **Step 5** | (Optional) **show running-config all | begin vty**<br><br>Example:<br>switch(config)# show running-config all | begin vty |
| **Step 6** | (Optional) **copy running-config startup-config**<br><br>Example:<br>switch(config)# copy running-config startup-config |
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>switch(config)# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters line configuration mode.</td>
</tr>
<tr>
<td><code>line vty</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>switch(config)# line vty</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-line)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the maximum number of virtual sessions for the Cisco NX-OS device. The range is from 1 to 60. The default is 32.</td>
</tr>
<tr>
<td><code>session-limit sessions</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>switch(config-line)# session-limit 10</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-line)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Exits line configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>switch(config-line)# exit</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the virtual terminal configuration.</td>
</tr>
<tr>
<td>(Optional) `show running-config all</td>
<td>being vty`</td>
</tr>
<tr>
<td>`switch(config)# show running-config all</td>
<td>begin vty`</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>(Optional) <code>copy running-config startup-config</code></td>
<td>Example:</td>
</tr>
<tr>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>Enter one of the following commands:</td>
<td>Enters COM1 configuration mode or console configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>line com1</td>
<td>Enters COM1 configuration mode.</td>
</tr>
<tr>
<td>line console</td>
<td>Enters console configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# line com1</td>
</tr>
<tr>
<td></td>
<td>switch(config-com1)#</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>modem in</td>
<td>Enables modem input on the COM1 or console port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-com1)# modem in</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Exits COM1 or console configuration mode.</td>
</tr>
<tr>
<td><strong>Exit</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>switch(config-com1)# exit</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 5** | Displays the console and COM1 settings. |
| **(Optional) show line** | **Example:** |
| switch(config)# show line |

| **Step 6** | Copies the running configuration to the startup configuration. |
| **(Optional) copy running-config startup-config** | **Example:** |
| switch(config)# copy running-config startup-config |

---

## 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>Enter one of the following commands:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>line com1</td>
<td>Enters COM1 configuration mode.</td>
</tr>
<tr>
<td>line console</td>
<td>Enters console configuration mode.</td>
</tr>
</tbody>
</table>
### 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**
3. **exit**
4. (Optional) **show line**
5. (Optional) **copy running-config startup-config**

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

- **Command or Action**: configure terminal
- **Example**:
  ```
  switch# configure terminal
  switch(config)#
  ```
### Command or Action

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch# configure terminal</code>&lt;br&gt;<code>switch(config)#</code></td>
<td></td>
</tr>
</tbody>
</table>

### Step 2

Enter one of the following commands:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>line com1</code></td>
<td>Enters COM1 configuration mode.</td>
</tr>
<tr>
<td><code>line console</code></td>
<td>Enters console configuration mode.</td>
</tr>
</tbody>
</table>

**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.

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>modem connect line {com1</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# modem connect line com1</td>
</tr>
</tbody>
</table>

Initializes the modem connected to the device.

Related Topics

Enabling a Modem Connection, on page 75

Clearing Terminal Sessions

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

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>(Optional) show users</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# show users</td>
</tr>
<tr>
<td>Step 2</td>
<td>clear line name</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# clear line pts/0</td>
</tr>
</tbody>
</table>

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:
### Default Settings for Terminal Display and Session Parameters

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal type</td>
<td>ansi</td>
</tr>
<tr>
<td>Terminal length</td>
<td>0 lines for console sessions</td>
</tr>
<tr>
<td></td>
<td>31 lines for virtual terminal sessions</td>
</tr>
<tr>
<td>Terminal width</td>
<td>80 columns</td>
</tr>
<tr>
<td>Terminal inactive session timeout</td>
<td>Disabled (0 minutes)</td>
</tr>
<tr>
<td>Console session data bits</td>
<td>8</td>
</tr>
<tr>
<td>Console inactive session timeout</td>
<td>Disabled (0 minutes)</td>
</tr>
<tr>
<td>Console session parity</td>
<td>none</td>
</tr>
<tr>
<td>Console session speed</td>
<td>11520 bps</td>
</tr>
<tr>
<td>Console session stop bits</td>
<td>1</td>
</tr>
<tr>
<td>COM1 session data bits</td>
<td>8</td>
</tr>
<tr>
<td>COM1 hardware flow control</td>
<td>Enabled</td>
</tr>
<tr>
<td>COM1 session parity</td>
<td>none</td>
</tr>
<tr>
<td>COM1 session speed</td>
<td>9600 bps</td>
</tr>
<tr>
<td>COM1 session stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Virtual terminal inactive session timeout</td>
<td>Disabled (0 minutes)</td>
</tr>
<tr>
<td>Parameters</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Virtual terminal sessions limit</td>
<td>32</td>
</tr>
<tr>
<td>Modem default initialization string</td>
<td>ATE0Q1&amp;D2&amp;C1S0=1'015</td>
</tr>
</tbody>
</table>
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 83
- Changing the Device Hostname, on page 85
- Configuring the Management Interface, on page 86
- Configuring the Default Gateway, on page 87
- Configuring the MOTD Banner, on page 88
- Configuring the Time Zone, on page 89
- Configuring Summer Time (Daylight Saving Time), on page 90
- Manually Setting the Device Clock, on page 91
- Managing Users, on page 92
- Enabling or Disabling a Telnet Server Connection, on page 93
- Verifying the Device Configuration, on page 93
- Default Settings for Basic Device Parameters, on page 94

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 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td>Changes the device hostname. The name argument is alphanumeric, case sensitive, and has a maximum length of 63 characters. The default name is switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The switchname command performs the same function as the hostname command.</td>
</tr>
<tr>
<td>{hostname</td>
<td>switchname} name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Using the hostname command:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# hostname Engineering1</td>
<td></td>
</tr>
<tr>
<td>Engineering1(config)#</td>
<td></td>
</tr>
<tr>
<td>Using the switchname command:</td>
<td></td>
</tr>
<tr>
<td>Engineering1(config)# switchname Engineering2</td>
<td></td>
</tr>
<tr>
<td>Engineering2(config)#</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Engineering2(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Engineering2#</td>
<td></td>
</tr>
<tr>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Engineering2# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

## 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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 interface 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 | Displays 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. |

## Configuring the Default Gateway

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

**Before you begin**  
Establish a connection on the console port.

**SUMMARY STEPS**

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

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

### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:**
  switch# configure terminal
  switch(config)# |
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>clock timezone zone-name offset-hours offset-minutes</code></td>
<td>Configures the time zone. The <code>zone-name</code> argument is a 3-character string for the time zone acronym (for example, PST or EST). The <code>offset-hours</code> argument is the offset from the UTC and the range is from –23 to 23 hours. The range for the <code>offset-minutes</code> argument is from 0 to 59 minutes.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# clock timezone EST -5 0</code></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures summer time or daylight saving time. The <em>zone-name</em> argument is a three character string for the time zone acronym (for example, PST and EST). The values for the <em>start-day</em> and <em>end-day</em> arguments are Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.</td>
</tr>
<tr>
<td>clock summer-time</td>
<td></td>
</tr>
<tr>
<td>zone-name</td>
<td></td>
</tr>
<tr>
<td>start-week</td>
<td></td>
</tr>
<tr>
<td>start-day</td>
<td></td>
</tr>
<tr>
<td>start-month</td>
<td></td>
</tr>
<tr>
<td>start-time</td>
<td></td>
</tr>
<tr>
<td>end-week</td>
<td></td>
</tr>
<tr>
<td>end-day</td>
<td></td>
</tr>
<tr>
<td>end-month</td>
<td></td>
</tr>
<tr>
<td>end-time</td>
<td></td>
</tr>
<tr>
<td>offset-minutes</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# clock summer-time PDT 1 Sunday March 02:00 1 Sunday November 02:00 60</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# exit switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays the time and time zone.</td>
</tr>
<tr>
<td>(Optional) <code>show clock</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show clock</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>(Optional) <code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configures the device clock.</td>
</tr>
<tr>
<td></td>
<td>The format for the time argument is hh:mm:ss.</td>
</tr>
<tr>
<td></td>
<td>The range for the day argument is from 1 to 31.</td>
</tr>
<tr>
<td></td>
<td>The values for the month argument are January, February, March, April, May, June, July, August, September, October, November, and December.</td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show users</code></td>
<td>Displays the user sessions.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# show users</code></td>
</tr>
</tbody>
</table>

#### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) <code>show users</code></td>
<td>Displays the active user sessions.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# show users</code></td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>[no] feature telnet</code></td>
<td>Enables the Telnet server connection. Use the <code>no</code> form of the command to disable the Telnet server connection. The default is disabled.</td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# feature telnet</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>(Optional) show telnet server</code></td>
<td>Displays the Telnet server configuration.</td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# show telnet server</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>(Optional) copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the Device Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Displays the running configuration.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOTD banner text</td>
<td>User Access Verification</td>
</tr>
<tr>
<td>Clock time zone</td>
<td>UTC</td>
</tr>
</tbody>
</table>
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 95
- Working with External Storage Devices, on page 97
- Working with Directories, on page 98
- Working with Files, on page 100
- Working with Archive Files, on page 103
- Examples of Using a File System, on page 105

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

<table>
<thead>
<tr>
<th>File System Name</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash</td>
<td>sup-active</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>sup-local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sup-standby</td>
<td>Internal CompactFlash memory located on a standby supervisor module. Used for storing image files, configuration files, and other miscellaneous files.</td>
</tr>
<tr>
<td></td>
<td>sup-remote</td>
<td></td>
</tr>
<tr>
<td>volatile</td>
<td>—</td>
<td>Volatile random-access memory (VRAM) located on a supervisor module. Used for temporary or pending changes.</td>
</tr>
<tr>
<td>log</td>
<td>—</td>
<td>Memory on an active supervisor module. Used for storing file statistics logs.</td>
</tr>
<tr>
<td>system</td>
<td>—</td>
<td>Memory on a supervisor module. Used for storing the running configuration file.</td>
</tr>
<tr>
<td>debug</td>
<td>—</td>
<td>Memory on a supervisor module. Used for storing the debug logs.</td>
</tr>
</tbody>
</table>

### 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.
<table>
<thead>
<tr>
<th>Platform</th>
<th>PCMCIA</th>
<th>USB¹</th>
<th>USB¹</th>
<th>USB¹</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>slot0</td>
<td>First supported</td>
<td>slot0</td>
<td>usb1</td>
</tr>
<tr>
<td>Cisco MDS 9700 Series Multilayer Director</td>
<td>No hardware port</td>
<td>Cisco MDS NX-OS Release 6.2(1)</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco MDS 9500 Series Multilayer Director</td>
<td>Enabled</td>
<td>Cisco MDS NX-OS Release 6.2(1)</td>
<td>No hardware port</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco MDS 9396S 16G Multilayer Fabric Switch</td>
<td>No hardware port</td>
<td>Cisco MDS NX-OS Release 6.2(13)</td>
<td>No hardware port</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco MDS 9250i Multiservice Fabric Switch</td>
<td>No hardware port</td>
<td>Cisco MDS NX-OS Release 6.2(15)</td>
<td>No hardware port</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco MDS 9222i Multiservice Modular Switch</td>
<td>No hardware port</td>
<td>—</td>
<td>No hardware port</td>
<td>No hardware port</td>
</tr>
<tr>
<td>Cisco MDS 9148S 16G Multilayer Fabric Switch</td>
<td>No hardware port</td>
<td>Cisco MDS NX-OS Release 6.2(15)</td>
<td>No hardware port</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco MDS 9148 Multilayer Fabric Switch</td>
<td>No hardware port</td>
<td>—</td>
<td>No hardware port</td>
<td>No hardware port</td>
</tr>
<tr>
<td>Cisco MDS 8Gb Fabric Switch for HP BladeSystem c-Class</td>
<td>No hardware port</td>
<td>—</td>
<td>No hardware port</td>
<td>No hardware port</td>
</tr>
</tbody>
</table>

¹USB 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:

```bash
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:

```bash
mkdir filesystem://module/][directory]
```

Example:

```
switch# mkdir test
```

Displaying Directory Contents

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

```bash
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.

```
move [filesystem://module/][directory/][source-filename] [filesystem://module/][directory/][target-filename]
```

Example:

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

- **Note**

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

- **Note**

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

  ```
  move [filesystem://module/][directory/][source-filename] [filesystem://module/][directory/][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.

- 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:
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/]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/]filename.gz
  ```

  Example:

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

  **Note** The file that has been 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 beginning 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-sfleek-kickstart-mzg.1.3.0.39a.bin
1864931 Apr 29 12:41:59 2003 dplug2
12288 Apr 18 20:23:11 2003 lost+found/
41574014 Nov 21 16:34:47 2003 m9500-sfleek-kickstart-mzg.6.2.13.FM.0.65.bin
12097024 Nov 21 16:34:18 2003 m9500-sfleek-kickstart-mzg.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
```
Working with Configuration Files

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

- Information About Configuration Files, on page 107
- Managing Configuration Files, on page 108
- Verifying the Device Configuration, on page 117
- Examples of Working with Configuration Files, on page 118

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
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) <code>show running-config</code></td>
<td>Displays the running configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config scheme://server/[url/]filename</code></td>
<td>Copies the running-configuration file to a remote server.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# copy running-config</code></td>
<td></td>
</tr>
<tr>
<td><code>tftp://10.10.1.1/sw1-run-config.bak</code></td>
<td></td>
</tr>
</tbody>
</table>
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 subnet if you do not have a router or a default gateway to route traffic between subnets.

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

SUMMARY STEPS

1. `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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy scheme://server[/url]filename running-config</code></td>
<td>Downloads the running-configuration file from a remote server. For the <code>scheme</code> argument, you can enter <code>tftp:</code>, <code>ftp:</code>, <code>scp:</code>, or <code>sftp:</code>. The <code>server</code> argument is the address or name of the remote server.</td>
</tr>
<tr>
<td><code>switch# copy tftp://10.10.1.1/my-config running-config</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>remote server, and the <em>url</em> argument is the path to the source file on the remote server.</td>
</tr>
<tr>
<td></td>
<td>The <em>server, url, and filename</em> arguments are case sensitive.</td>
</tr>
<tr>
<td>Step 2: (Optional) <strong>show running-config</strong></td>
<td>Displays the running configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 3: (Optional) <strong>copy running-config startup-config</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Step 4: (Optional) <strong>show startup-config</strong></td>
<td>Displays the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>DETAILED STEPS</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>write erase</td>
<td>Erases the startup configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# write erase</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>reload</td>
<td>Reloads the Cisco NX-OS device.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# reload</td>
<td>Do not use the setup utility to configure the device.</td>
</tr>
<tr>
<td></td>
<td>This command will reboot the system. (y/n)? [n] y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter the password for &quot;admin&quot;: &lt;password&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confirm the password for &quot;admin&quot;: &lt;password&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Would you like to enter the basic configuration dialog (yes/no): n</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>copy scheme://server[/url/]filename running-config</td>
<td>Downloads the running configuration file from a remote server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# copy tftp://10.10.1.1/my-config running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>copy running-config startup-config</td>
<td>Saves the running configuration file to the startup configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) show startup-config</td>
<td>Displays the running configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# show startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> (Optional) `dir {slot0:</td>
<td>usb1:</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# dir slot0:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> `copy running-config {slot0:</td>
<td>usb1:</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# copy running-config slot0:dsn-running-config.cfg</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `copy startup-config {slot0:</td>
<td>usb1:</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# copy startup-config slot0:dsn-startup-config.cfg</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>(Optional) `dir {slot0:</td>
<td>usb1:</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# dir slot0:</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>`copy {slot0:</td>
<td>usb1:</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# copy slot0:dsn-config.cfg running-config</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) <code>show running-config</code></td>
<td>Displays the running configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) <code>copy running-config startup-config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) <code>show startup-config</code></td>
<td>Displays the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>switch# show startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Displays the files on the external flash memory device.</td>
</tr>
<tr>
<td>(Optional) dir {slot0:</td>
<td>usb1:</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# dir slot0:</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Copies the startup configuration from an external flash memory device. The filename argument is case sensitive.</td>
</tr>
<tr>
<td>copy {slot0:</td>
<td>usb1:</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# copy slot0:dsn-config.cfg startup-config</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Displays the startup configuration.</td>
</tr>
<tr>
<td>(Optional) show startup-config</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# show startup-config</td>
</tr>
</tbody>
</table>

### 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

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

### Related Topics

Copying Files

---

Note: The code snippets are placeholders and are not meant to be executed as is. They are provided for illustrative purposes only.
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.

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**

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

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

**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:
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Erases the boot variable definitions.</td>
</tr>
<tr>
<td>write erase boot</td>
<td></td>
</tr>
<tr>
<td>switch# write erase boot</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>reload</td>
<td></td>
</tr>
<tr>
<td>switch# reload</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Erases the boot variable definitions.</td>
</tr>
<tr>
<td>write erase</td>
<td></td>
</tr>
<tr>
<td>switch# write erase</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Erases the boot variable definitions and the IPv4 configuration on the management interface.</td>
</tr>
<tr>
<td>write erase boot</td>
<td></td>
</tr>
<tr>
<td>switch# write erase boot</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>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.</td>
</tr>
<tr>
<td>reload</td>
<td></td>
</tr>
<tr>
<td>switch# reload</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the Device Configuration

To verify the configuration after bootstrapping the device using POAP, use one of the following commands:
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Displays the running configuration.</td>
</tr>
<tr>
<td><code>show startup-config</code></td>
<td>Displays the startup configuration.</td>
</tr>
</tbody>
</table>

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:

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

**Backing Up Configuration Files**

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

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

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

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

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

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

**Rolling Back to a Previous Configuration**

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

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

**Note**

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

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

3. Copy the previously saved configuration file to the running configuration with the `copy configuration_file running-configuration` command.
4. Copy the running configuration to the start-up configuration with the `copy running-config startup-config` command.
Rolling Back to a Previous Configuration
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 121
- Configuring CDP, on page 122
- Verifying the CDP Configuration, on page 124
- Clearing CDP Counters and Tables, on page 124
- CDP Example Configuration, on page 125
- Default Settings for CDP, on page 125

Information About CDP

This section includes information about CDP.

CDP Overview

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

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

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

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

The Cisco NX-OS software supports stateless restarts for CDP. After a reboot or a supervisor module switchover, the Cisco NX-OS software applies the running configuration. For more information on high availability, see the.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td>Step 2</td>
<td>cdp enable</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# cdp enable</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config</td>
</tr>
<tr>
<td></td>
<td>startup-config</td>
</tr>
</tbody>
</table>

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**

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

**Configuring Optional CDP Parameters**

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`cdp advertise {v1</td>
<td>v2}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# cdp advertise v1</code></td>
<td></td>
</tr>
</tbody>
</table>
Verifying the CDP Configuration

Use the following commands to verify the CDP configuration:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cdp all</td>
<td>Displays all interfaces that have CDP enabled.</td>
</tr>
<tr>
<td>show cdp entry {all</td>
<td>name entry-name}</td>
</tr>
<tr>
<td>show cdp global</td>
<td>Displays the CDP global parameters.</td>
</tr>
<tr>
<td>show cdp interface interface-type slot/port</td>
<td>Displays the CDP interface status.</td>
</tr>
<tr>
<td>show cdp neighbors {device-id</td>
<td>interface interface-type slot/port} [detail]</td>
</tr>
<tr>
<td>show cdp traffic interface interface-type slot/port</td>
<td>Displays the CDP traffic statistics on an interface.</td>
</tr>
</tbody>
</table>

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).
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:

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

### Default Settings for CDP

This table lists the CDP default settings.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP</td>
<td>Enabled globally and on all interfaces</td>
</tr>
<tr>
<td>CDP version</td>
<td>Version 2</td>
</tr>
<tr>
<td>CDP device ID</td>
<td>Serial number</td>
</tr>
<tr>
<td>CDP timer</td>
<td>60 seconds</td>
</tr>
<tr>
<td>CDP hold timer</td>
<td>180 seconds</td>
</tr>
</tbody>
</table>
CHAPTER 11

Configuring NTP

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

• Information About NTP, on page 127
• Prerequisites for NTP, on page 128
• Guidelines and Limitations for NTP, on page 129
• Configuring NTP, on page 129
• Verifying NTP, on page 138
• Troubleshooting NTP, on page 139
• Example: Configuring NTP, on page 141
• Default Settings for NTP, on page 143

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.

Step 1 Enter configuration mode:
switch# configure terminal

Step 2 Enable NTP:
switch(config)# feature ntp

Disabling NTP

To disable NTP on a switch:

Step 1 Enter configuration mode:
switch# configure terminal
Configuring 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.

---

**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 130.

---

**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:
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 \texttt{ntp server} or \texttt{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:

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 \texttt{ntp server} or \texttt{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.

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:

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:
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:

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:

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:

Step 1
Enter configuration mode:
Enabling NTP Logging

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

**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:

**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:

**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:

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:

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:
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.

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

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 138."

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:

### 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.

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

### Step 1
Enter configuration mode:
```
switch# configure terminal
```

### Step 2
Abort and unlock the existing NTP CFS distribution session on a switch:
```
switch(config)# ntp abort
```

---

Cisco MDS 9000 Series Fundamentals Configuration Guide, Release 8.x
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:

```
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 fewgl2345 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

<table>
<thead>
<tr>
<th>Switch</th>
<th>WWN IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>20:00:8c:60:4f:0d:2b:b0 192.168.12.34</td>
</tr>
<tr>
<td>[switch1]</td>
<td></td>
</tr>
<tr>
<td>Merged</td>
<td>20:00:8c:60:4f:0d:32:d0 192.168.56.78 [switch2.mydomain.com]</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Peer IP Address</th>
<th>Serv/Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.105.194.169</td>
<td>Server (configured)</td>
</tr>
</tbody>
</table>

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.
configure terminal
ntp authenticate
ntp authentication-key 1 md5 aNiceKey
ntp server 192.168.12.34 key 1
ntp authentication-key 2 md5 goodTime
ntp peer 192.168.56.78 key 2
show ntp pending peers
ntp server 192.168.12.34
ntp peer 192.168.56.78
show ntp pending-diff
ntp commit
show ntp pending peers
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:

no ntp peer 192.168.56.78
show ntp pending peers
ntp server 192.168.12.34
show ntp pending-diff
ntp peer 192.168.56.78
ntp commit
show ntp pending peers
show ntp pending-diff
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.

show ntp peer-status
Total peers : 1
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
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
```
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:
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*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>Disabled</td>
</tr>
<tr>
<td>NTP Modes</td>
<td>Disabled</td>
</tr>
<tr>
<td>NTP Source Interface</td>
<td>mgmt0</td>
</tr>
<tr>
<td>NTP Logging</td>
<td>Disabled</td>
</tr>
<tr>
<td>NTP Distribution</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Default Settings for NTP
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 145
- Running CompactFlash Tests, on page 149
- Displaying the Switch Serial Number, on page 149
- Displaying Power Usage Information, on page 150
- Power Supply Modes, on page 151
- About Module Temperature Monitoring, on page 160
- About Fan Modules, on page 162
- Displaying Environment Information, on page 163
- Default Settings, on page 165

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: DTM1646023P

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
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 with 8167860 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

Module6 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 : JAF1647AQT1
  Part Number : 73-14586-02
  Part Revision : 02
  Mfg Deviation : 0
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.

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

<table>
<thead>
<tr>
<th>Power Supply</th>
<th>Model</th>
<th>Actual Output</th>
<th>Total Capacity</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DS-CAC97-3KW</td>
<td>549 W</td>
<td>3000 W</td>
<td>Ok</td>
</tr>
<tr>
<td>2</td>
<td>DS-CAC97-3KW</td>
<td>535 W</td>
<td>3000 W</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>DS-CAC97-3KW</td>
<td>539 W</td>
<td>3000 W</td>
<td>Ok</td>
</tr>
<tr>
<td>4</td>
<td>DS-CAC97-3KW</td>
<td>535 W</td>
<td>3000 W</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>------------</td>
<td>0 W</td>
<td>0 W</td>
<td>Absent</td>
</tr>
<tr>
<td>6</td>
<td>------------</td>
<td>0 W</td>
<td>0 W</td>
<td>Absent</td>
</tr>
<tr>
<td>7</td>
<td>------------</td>
<td>0 W</td>
<td>0 W</td>
<td>Absent</td>
</tr>
<tr>
<td>8</td>
<td>------------</td>
<td>0 W</td>
<td>0 W</td>
<td>Absent</td>
</tr>
</tbody>
</table>

Module | Model      | Actual Draw | Power 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   |
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>
<thead>
<tr>
<th>Cisco MDS Switch</th>
<th>Grid A</th>
<th>Grid B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco MDS 9718</td>
<td>PSU1, PSU2, PSU5, PSU6, PSU9, PSU10, PSU13, PSU14</td>
<td>PSU3, PSU4, PSU7, PSU8, PSU11, PSU12, PSU15, PSU16</td>
</tr>
<tr>
<td>Cisco MDS 9710</td>
<td>PSU1, PSU2, PSU5, PSU6</td>
<td>PSU3, PSU4, PSU7, PSU8</td>
</tr>
<tr>
<td>Cisco MDS 9706</td>
<td>PSU1, PSU2</td>
<td>PSU3, PSU4</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Grid A</th>
<th>Grid B</th>
<th>Available Capacity (Watts)</th>
<th>Power Supply Operational Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>15000 (N+1 redundant mode)</td>
</tr>
<tr>
<td>2</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>12000</td>
</tr>
<tr>
<td>3</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
<td>9000</td>
</tr>
<tr>
<td>4</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
<td>6000</td>
</tr>
</tbody>
</table>

- 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 153 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

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Grid A</th>
<th>Grid B</th>
<th>Available Capacity (Watts)</th>
<th>Power Supply Operational Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Power Supply
Operational Mode
Available Capacity (Watts)
Power Supply Operational Mode

- 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

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Grid A</th>
<th>Grid B</th>
<th>Available Capacity (Watts)</th>
<th>Power Supply Operational Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td>Scenario</td>
<td>Grid A</td>
<td>Grid B</td>
<td>Available Capacity (Watts)</td>
<td>Power Supply Operational Mode</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>--------</td>
<td>-----------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
</tr>
<tr>
<td>3</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
</tr>
<tr>
<td>4</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>
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.

**Note**

- 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>
<thead>
<tr>
<th>Scenario</th>
<th>Grid A</th>
<th>Grid B</th>
<th>Available Capacity (Watts)</th>
<th>Power Supply Operational Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td>2</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td>3</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td>4</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
</tr>
</tbody>
</table>

The following table provides information about moving from combined (nonredundant) mode to other power supply modes:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Grid A</th>
<th>Grid B</th>
<th>Current Usage (Watts)</th>
<th>Current Mode</th>
<th>New Mode</th>
<th>Capacity (Watts)</th>
<th>Power Supply Operational Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>18000</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
<td>15000</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
<td>Off</td>
<td>12000</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Off</td>
<td>Off</td>
<td>9000</td>
<td></td>
</tr>
<tr>
<td>Scenario</td>
<td>Grid A (Watts)</td>
<td>Grid B (Watts)</td>
<td>Current Usage (Watts)</td>
<td>Current Mode</td>
<td>New Mode</td>
<td>Capacity (Watts)</td>
<td>Power Supply Operational Mode</td>
</tr>
<tr>
<td>----------</td>
<td>---------------</td>
<td>---------------</td>
<td>-----------------------</td>
<td>--------------</td>
<td>----------</td>
<td>-----------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Combined</td>
<td>NA</td>
<td>18000</td>
<td>Combined mode.</td>
</tr>
<tr>
<td></td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Combined</td>
<td>NA</td>
<td>9000</td>
<td>Combined mode.</td>
</tr>
<tr>
<td></td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Combined</td>
<td>NA</td>
<td>15000</td>
<td>Combined mode.</td>
</tr>
<tr>
<td></td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Combined</td>
<td>NA</td>
<td>15000</td>
<td>Combined mode.</td>
</tr>
<tr>
<td></td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>Combined</td>
<td>NA</td>
<td>6000</td>
<td>Combined mode.</td>
</tr>
</tbody>
</table>

- The new capacity has changed to redundant mode.  
- Rejected due to insufficient capacity. Power supply mode reverts to the combined (non-redundant) mode, because the power availability in one grid is less than the current usage.
### 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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
|        | Example: 
  `switch# configure terminal`
  `switch(config)#` | |
| Step 2 | `power redundancy-mode {combined | insrc-redundant | ps-redundant | redundant}` | Configures the power supply mode. The default is `redundant`. |
|        | Example: 
  `switch(config)# power redundancy-mode combined` | |
| Step 3 | (Optional) `show environment power` | Displays the power mode configuration. |
|        | Example: 
  `switch(config)# show environment power` | |
| Step 4 | (Optional) `copy running-config startup-config` | Copies the running configuration to the startup configuration. |
|        | Example: 
  `switch(config)# copy running-config startup-config` | |
About Module Temperature Monitoring

Built-in automatic sensors are provided in all switches in the Cisco MDS 9000 Family to monitor your switch at all times.

Each module (switching and supervisor) has four sensors: 1 (outlet sensor), 2 (intake sensor), and 3 (onboard sensor). Each sensor has two thresholds (in degrees Celsius): minor and major.

---

**Note**

A threshold value of –127 indicates that no thresholds are configured or applicable.

- **Minor threshold**—When a minor threshold is exceeded, a minor alarm occurs and the following action is taken for all four sensors:
  - System messages are displayed.
  - Call Home alerts are sent (if configured).
  - SNMP notifications are sent (if configured).

- **Major threshold**—When a major threshold is exceeded, a major alarm occurs and the following action is taken:
  - For sensors 1 and 3 (outlet and onboard sensors):
    - System messages are displayed.
    - Call Home alerts are sent (if configured).
    - SNMP notifications are sent (if configured).
  - For sensor 2 (intake sensor):
    - If the threshold is exceeded in a switching module, only that module is shut down.
    - If the threshold is exceeded in an active supervisor module with HA-standby or standby present, only that supervisor module is shut down and the standby supervisor module takes over.
    - If you do not have a standby supervisor module in your switch, you have an interval of 2 minutes to decrease the temperature. During this interval the software monitors the temperature every five (5) seconds and continuously sends system messages as configured.

---

**Tip**

To realize the benefits of these built-in automatic sensors on any switch in the Cisco MDS 9700 Series, we highly recommend that you install dual supervisor modules. If you are using a Cisco MDS 9000 Series switch without dual supervisor modules, we recommend that you immediately replace the fan module if even one fan is not working.

---

Displaying Module Temperatures

Use the `show environment temperature` command to display temperature sensors for each module.
This example shows the temperature information.

```
switch# show environment temperature
Temperature:
--------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Module</th>
<th>Sensor</th>
<th>MajorThresh (Celsius)</th>
<th>MinorThres (Celsius)</th>
<th>CurTemp (Celsius)</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Crossbar0 (s1)</td>
<td>125</td>
<td>115</td>
<td>46</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>Crossbar1 (s2)</td>
<td>125</td>
<td>115</td>
<td>54</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>Arb-mux (s3)</td>
<td>125</td>
<td>105</td>
<td>48</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>CPU (s4)</td>
<td>125</td>
<td>105</td>
<td>48</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>PCI-SW (s5)</td>
<td>125</td>
<td>105</td>
<td>66</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>IOSSlice0 (s6)</td>
<td>125</td>
<td>115</td>
<td>38</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>IOSSlice1 (s7)</td>
<td>125</td>
<td>115</td>
<td>39</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>IOSSlice2 (s8)</td>
<td>125</td>
<td>115</td>
<td>40</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>Inlet (s1)</td>
<td>60</td>
<td>42</td>
<td>23</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>Crossbar (s2)</td>
<td>125</td>
<td>115</td>
<td>71</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>Arbiter (s3)</td>
<td>125</td>
<td>105</td>
<td>51</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>L2L3Dev1 (s4)</td>
<td>125</td>
<td>110</td>
<td>41</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>CPU1CORE1 (s5)</td>
<td>85</td>
<td>75</td>
<td>35</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>CPU1CORE2 (s6)</td>
<td>85</td>
<td>75</td>
<td>29</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>CPU1CORE3 (s7)</td>
<td>85</td>
<td>75</td>
<td>35</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>CPU1CORE4 (s8)</td>
<td>85</td>
<td>75</td>
<td>31</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>DDR3DIMM1 (s9)</td>
<td>95</td>
<td>85</td>
<td>31</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>Inlet (s1)</td>
<td>60</td>
<td>42</td>
<td>25</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>Crossbar (s2)</td>
<td>125</td>
<td>115</td>
<td>70</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>Arbiter (s3)</td>
<td>125</td>
<td>105</td>
<td>52</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>L2L3Dev1 (s4)</td>
<td>125</td>
<td>110</td>
<td>41</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>CPU1CORE1 (s5)</td>
<td>85</td>
<td>70</td>
<td>36</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>CPU1CORE2 (s6)</td>
<td>85</td>
<td>70</td>
<td>34</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>CPU1CORE3 (s7)</td>
<td>85</td>
<td>70</td>
<td>36</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>CPU1CORE4 (s8)</td>
<td>85</td>
<td>70</td>
<td>33</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>DDR3DIMM1 (s9)</td>
<td>95</td>
<td>85</td>
<td>31</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>Crossbar0 (s1)</td>
<td>125</td>
<td>115</td>
<td>83</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>Crossbar1 (s2)</td>
<td>125</td>
<td>115</td>
<td>82</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>Arb-mux (s3)</td>
<td>125</td>
<td>115</td>
<td>52</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>CPU (s4)</td>
<td>125</td>
<td>115</td>
<td>53</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>L2L3Dev0 (s5)</td>
<td>125</td>
<td>115</td>
<td>66</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>IOSSlice0 (s6)</td>
<td>125</td>
<td>115</td>
<td>56</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>IOSSlice1 (s7)</td>
<td>125</td>
<td>115</td>
<td>56</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>IOSSlice2 (s8)</td>
<td>125</td>
<td>115</td>
<td>57</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>FC-IP 0 (s9)</td>
<td>95</td>
<td>85</td>
<td>55</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>FC-IP 1 (s10)</td>
<td>95</td>
<td>85</td>
<td>56</td>
<td>Ok</td>
</tr>
<tr>
<td>8</td>
<td>Crossbar0 (s1)</td>
<td>125</td>
<td>115</td>
<td>52</td>
<td>Ok</td>
</tr>
<tr>
<td>8</td>
<td>Crossbar1 (s2)</td>
<td>125</td>
<td>115</td>
<td>52</td>
<td>Ok</td>
</tr>
<tr>
<td>8</td>
<td>Arb-mux (s3)</td>
<td>125</td>
<td>105</td>
<td>50</td>
<td>Ok</td>
</tr>
<tr>
<td>8</td>
<td>CPU (s4)</td>
<td>125</td>
<td>105</td>
<td>47</td>
<td>Ok</td>
</tr>
<tr>
<td>8</td>
<td>PCI-SW (s5)</td>
<td>125</td>
<td>105</td>
<td>56</td>
<td>Ok</td>
</tr>
<tr>
<td>8</td>
<td>IOSSlice0 (s6)</td>
<td>125</td>
<td>115</td>
<td>40</td>
<td>Ok</td>
</tr>
<tr>
<td>8</td>
<td>IOSSlice1 (s7)</td>
<td>125</td>
<td>115</td>
<td>41</td>
<td>Ok</td>
</tr>
<tr>
<td>8</td>
<td>IOSSlice2 (s8)</td>
<td>125</td>
<td>115</td>
<td>42</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>Crossbar (s1)</td>
<td>125</td>
<td>115</td>
<td>79</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>Crossbar2 (s2)</td>
<td>125</td>
<td>115</td>
<td>78</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>Arb-mux (s3)</td>
<td>125</td>
<td>105</td>
<td>79</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>L2L3Dev1 (s5)</td>
<td>125</td>
<td>110</td>
<td>61</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>L2L3Dev2 (s6)</td>
<td>125</td>
<td>110</td>
<td>61</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>L2L3Dev3 (s7)</td>
<td>125</td>
<td>110</td>
<td>57</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>L2L3Dev4 (s8)</td>
<td>125</td>
<td>110</td>
<td>56</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>L2L3Dev5 (s9)</td>
<td>125</td>
<td>110</td>
<td>61</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>L2L3Dev6 (s10)</td>
<td>125</td>
<td>110</td>
<td>52</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>L2L3Dev7 (s11)</td>
<td>125</td>
<td>110</td>
<td>58</td>
<td>Ok</td>
</tr>
<tr>
<td>10</td>
<td>L2L3Dev8 (s12)</td>
<td>125</td>
<td>110</td>
<td>66</td>
<td>Ok</td>
</tr>
</tbody>
</table>
```
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.

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.

```bash
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
```
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

<table>
<thead>
<tr>
<th>Power Supply</th>
<th>Model</th>
<th>Actual Output</th>
<th>Total Capacity</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DS-CAC97-3KW</td>
<td>548 W</td>
<td>3000 W</td>
<td>Ok</td>
</tr>
<tr>
<td>2</td>
<td>DS-CAC97-3KW</td>
<td>535 W</td>
<td>3000 W</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>DS-CAC97-3KW</td>
<td>535 W</td>
<td>3000 W</td>
<td>Ok</td>
</tr>
<tr>
<td>4</td>
<td>--------------</td>
<td>0 W</td>
<td>0 W</td>
<td>Absent</td>
</tr>
<tr>
<td>5</td>
<td>--------------</td>
<td>0 W</td>
<td>0 W</td>
<td>Absent</td>
</tr>
<tr>
<td>6</td>
<td>--------------</td>
<td>0 W</td>
<td>0 W</td>
<td>Absent</td>
</tr>
<tr>
<td>7</td>
<td>--------------</td>
<td>0 W</td>
<td>0 W</td>
<td>Absent</td>
</tr>
<tr>
<td>8</td>
<td>DS-CAC97-3KW</td>
<td>535 W</td>
<td>3000 W</td>
<td>Ok</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module</th>
<th>Model</th>
<th>Actual Draw</th>
<th>Power Allocated</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>DS-X9448-768K9</td>
<td>N/A</td>
<td>0 W</td>
<td>Powered-Dn</td>
</tr>
<tr>
<td>3</td>
<td>DS-X9648-1536K9</td>
<td>265 W</td>
<td>350 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>5</td>
<td>DS-X97-SF1-K9</td>
<td>107 W</td>
<td>190 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>6</td>
<td>DS-X97-SF1-K9</td>
<td>106 W</td>
<td>190 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>7</td>
<td>DS-X9334-K9</td>
<td>441 W</td>
<td>480 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>8</td>
<td>DS-X9648-1536K9</td>
<td>252 W</td>
<td>750 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>10</td>
<td>DS-X9848-480K9</td>
<td>363 W</td>
<td>500 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>Xb1</td>
<td>DS-X9710-FAB1</td>
<td>95 W</td>
<td>150 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>Xb2</td>
<td>DS-X9710-FAB1</td>
<td>94 W</td>
<td>150 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>Xb3</td>
<td>DS-X9710-FAB1</td>
<td>91 W</td>
<td>150 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>Xb</td>
<td>DS-X9710-FAB1</td>
<td>N/A</td>
<td>150 W</td>
<td>Powered-Dn</td>
</tr>
<tr>
<td>fan1</td>
<td>DS-C9710-FAN</td>
<td>45 W</td>
<td>600 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>fan2</td>
<td>DS-C9710-FAN</td>
<td>45 W</td>
<td>600 W</td>
<td>Powered-Up</td>
</tr>
<tr>
<td>fan3</td>
<td>DS-C9710-FAN</td>
<td>50 W</td>
<td>600 W</td>
<td>Powered-Up</td>
</tr>
</tbody>
</table>

N/A - Per module power not available
Power Usage Summary:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply redundancy mode (configured)</td>
<td>Redundant</td>
</tr>
<tr>
<td>Power Supply redundancy mode (operational)</td>
<td>Redundant</td>
</tr>
<tr>
<td>Total Power Capacity (based on configured mode)</td>
<td>6000 W</td>
</tr>
<tr>
<td>Total Power of all Inputs (cumulative)</td>
<td>12000 W</td>
</tr>
<tr>
<td>Total Power Output (actual draw)</td>
<td>2153 W</td>
</tr>
<tr>
<td>Total Power Allocated (budget)</td>
<td>5560 W</td>
</tr>
<tr>
<td>Total Power Available for additional modules</td>
<td>440 W</td>
</tr>
</tbody>
</table>

Clock:

<table>
<thead>
<tr>
<th>Clock Model</th>
<th>Hw Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Clock Module</td>
<td>NotSupported/None</td>
</tr>
<tr>
<td>B Clock Module</td>
<td>NotSupported/None</td>
</tr>
</tbody>
</table>

Fan:

<table>
<thead>
<tr>
<th>Fan Model</th>
<th>Hw Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan1(sys_fan1)</td>
<td>DS-C9710-FAN 0.2 Ok</td>
</tr>
<tr>
<td>Fan2(sys_fan2)</td>
<td>DS-C9710-FAN 0.2 Ok</td>
</tr>
<tr>
<td>Fan3(sys_fan3)</td>
<td>DS-C9710-FAN 0.2 Ok</td>
</tr>
<tr>
<td>Fan_in_PS1</td>
<td>-- Ok</td>
</tr>
<tr>
<td>Fan_in_PS2</td>
<td>-- Ok</td>
</tr>
<tr>
<td>Fan_in_PS3</td>
<td>-- Ok</td>
</tr>
<tr>
<td>Fan_in_PS4</td>
<td>-- Absent</td>
</tr>
<tr>
<td>Fan_in_PS5</td>
<td>-- Absent</td>
</tr>
<tr>
<td>Fan_in_PS6</td>
<td>-- Absent</td>
</tr>
<tr>
<td>Fan_in_PS7</td>
<td>-- Absent</td>
</tr>
<tr>
<td>Fan_in_PS8</td>
<td>-- Ok</td>
</tr>
</tbody>
</table>

Fan Zone Speed % (Hex): Zone 1: 40.78 (0x68)

Temperature:

<table>
<thead>
<tr>
<th>Module</th>
<th>Sensor</th>
<th>MajorThresh</th>
<th>MinorThresh</th>
<th>CurTemp</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Crossbar0 (s1)</td>
<td>125</td>
<td>115</td>
<td>46</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>Crossbar1 (s2)</td>
<td>125</td>
<td>115</td>
<td>54</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>Arb-mux (s3)</td>
<td>125</td>
<td>105</td>
<td>49</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>CPU (s4)</td>
<td>125</td>
<td>105</td>
<td>48</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>PCISW (s5)</td>
<td>125</td>
<td>105</td>
<td>66</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>IOSlice0 (s6)</td>
<td>125</td>
<td>115</td>
<td>38</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>IOSlice1 (s7)</td>
<td>125</td>
<td>115</td>
<td>39</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>IOSlice2 (s8)</td>
<td>125</td>
<td>115</td>
<td>40</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>Inlet (s1)</td>
<td>60</td>
<td>42</td>
<td>24</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>Crossbar (s2)</td>
<td>125</td>
<td>115</td>
<td>71</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>Arbiter (s3)</td>
<td>125</td>
<td>105</td>
<td>51</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>L2L3Dev1 (s4)</td>
<td>125</td>
<td>110</td>
<td>42</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>CPU1CORE1 (s5)</td>
<td>85</td>
<td>75</td>
<td>35</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>CPU1CORE2 (s6)</td>
<td>85</td>
<td>75</td>
<td>29</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>CPU1CORE3 (s7)</td>
<td>85</td>
<td>75</td>
<td>35</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>CPU1CORE4 (s8)</td>
<td>85</td>
<td>75</td>
<td>30</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>DDR3DIMM1 (s9)</td>
<td>95</td>
<td>85</td>
<td>31</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>Inlet (s1)</td>
<td>60</td>
<td>42</td>
<td>26</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>Crossbar (s2)</td>
<td>125</td>
<td>115</td>
<td>70</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>Arbiter (s3)</td>
<td>125</td>
<td>105</td>
<td>52</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>L2L3Dev1 (s4)</td>
<td>125</td>
<td>110</td>
<td>41</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>CPU1CORE1 (s5)</td>
<td>85</td>
<td>70</td>
<td>36</td>
<td>Ok</td>
</tr>
</tbody>
</table>
Default Settings

This table lists the default hardware settings.

**Table 25: Default Hardware Parameter Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply mode</td>
<td>PS redundant mode.</td>
</tr>
</tbody>
</table>
CHAPTER 13

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 167
- Maintaining Supervisor Modules, on page 170
- Verifying the Status of a Module, on page 171
- Checking the State of a Module, on page 172
- Connecting to a Module, on page 172
- Reloading Modules, on page 173
- Saving the Module Configuration, on page 174
- Purging Module Configurations, on page 175
- Powering Off Switching Modules, on page 176
- Identifying Module LEDs, on page 177
- EPLD Images, on page 182
- SSI Boot Images, on page 188
- Managing SSMs and Supervisor Modules, on page 188
- Default Settings, on page 192

About Modules

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

Table 26: Supervisor Module Options

<table>
<thead>
<tr>
<th>Product</th>
<th>Number of Supervisor Modules</th>
<th>Supervisor Module Slot Number</th>
<th>Switching and Services Module Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco MDS 9513</td>
<td>Two modules</td>
<td>7 and 8</td>
<td>13-slot chassis allows any switching or services module in the other eleven slots.</td>
</tr>
<tr>
<td>Cisco MDS 9509</td>
<td>Two modules</td>
<td>5 and 6</td>
<td>9-slot chassis allows any switching or services module in the other seven slots.</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Module Terms</th>
<th>Fixed or Relative</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>module-7 and module-8</td>
<td>Fixed usage for the Cisco MDS 9513 Director</td>
<td>module-7 always refers to the supervisor module in slot 7 and module-8 always refers to the supervisor module in slot 8.</td>
</tr>
<tr>
<td>Module Terms</td>
<td>Fixed or Relative</td>
<td>Usage</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>module-5 and module-6</td>
<td>Fixed usage for the Cisco MDS 9509 and Cisco MDS 9506 Directors</td>
<td>module-5 always refers to the supervisor module in slot 5 and module-6 always refers to the supervisor module in slot 6.</td>
</tr>
<tr>
<td>module-1</td>
<td>Fixed usage for the Cisco MDS 9200 Series switches</td>
<td>module-1 always refers to the supervisor module in slot 1.</td>
</tr>
<tr>
<td>sup-1 and sup-2</td>
<td>Fixed usage</td>
<td>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.</td>
</tr>
<tr>
<td>sup-active and sup-standby</td>
<td>Relative usage</td>
<td>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.</td>
</tr>
<tr>
<td>sup-local and sup-remote</td>
<td>Relative usage</td>
<td>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).</td>
</tr>
</tbody>
</table>

**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 \texttt{out-of-service} command before removing the supervisor module.

\begin{verbatim}
out-of-service module slot
\end{verbatim}

Where \texttt{slot} indicates the chassis slot number in which the supervisor module resides.

\begin{itemize}
  \item \textbf{Note} You must remove and reinsert or replace the supervisor module to bring it into service.
\end{itemize}

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 \texttt{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
--- ----- ------------------------------- ------------------ ------------
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
3 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 JAB06350B1R
6 00-05-30-01-37-7a to 00-05-30-01-37-fe JAB072705ja
8 00-05-30-00-2d-e2 to 00-05-30-00-2d-e6 JAB06280ae9

* this terminal session
```

The Status column in the output should display an ok status for switching modules and an active or standby (or HA-standby) status for supervisor modules. If the status is either ok or active, you can continue with your configuration.

### Note

A standby supervisor module reflects the HA-standby status if the HA switchover mechanism is enabled. If the warm switchover mechanism is enabled, the standby supervisor module reflects the standby status.
Checking the State of a Module

If your chassis has more than one switching module (also known as line card), you can check the progress by issuing the `show module` command several times and viewing the Status column each time. The switching module goes through a testing and an initializing stage before displaying an ok status.

This table describes the module states listed in the `show module` command output.

<table>
<thead>
<tr>
<th>Module Status Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>powered up</td>
<td>The hardware has electrical power. When the hardware is powered up, the software begins booting.</td>
</tr>
<tr>
<td>testing</td>
<td>The switching module has established connection with the supervisor module and the switching module is performing bootup diagnostics.</td>
</tr>
<tr>
<td>initializing</td>
<td>The diagnostics have completed successfully and the configuration is being downloaded.</td>
</tr>
<tr>
<td>failure</td>
<td>The switch detects a switching module failure upon initialization and automatically attempts to power-cycle the module three times. After the third attempt it continues to display a failed state.</td>
</tr>
<tr>
<td>ok</td>
<td>The switch is ready to be configured.</td>
</tr>
<tr>
<td>power-denied</td>
<td>The switch detects insufficient power for a switching module to power up.</td>
</tr>
<tr>
<td>active</td>
<td>This module is the active supervisor module and the switch is ready to be configured.</td>
</tr>
<tr>
<td>HA-standby</td>
<td>The HA switchover mechanism is enabled on the standby supervisor module.</td>
</tr>
<tr>
<td>standby</td>
<td>The warm switchover mechanism is enabled on the standby supervisor module.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Provides direct access to the module in the specified slot.</td>
</tr>
<tr>
<td><code>attach module slot</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# attach module 4</code></td>
<td></td>
</tr>
<tr>
<td><code>Attaching to module 4 ...</code></td>
<td></td>
</tr>
<tr>
<td><code>To exit type 'exit', to abort type '$.'</code></td>
<td></td>
</tr>
<tr>
<td><code>module-4#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Exits module access configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>module-4# exit</code></td>
<td></td>
</tr>
<tr>
<td><code>rlogin: connection closed.</code></td>
<td></td>
</tr>
<tr>
<td><code>switch#</code></td>
<td></td>
</tr>
</tbody>
</table>

**Reloading Modules**

You can reload the entire switch, reset specific modules in the switch, or reload the image on specific modules in the switch.

**Reloading a Switch**

To reload the switch, issue the `reload` command without any options. When you issue this command, you reboot the switch (see the *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*).

**Power Cycling Modules**

You can power cycle any module in a chassis. Power cycling reinitializes the module.

**SUMMARY STEPS**

1. Identify the module that needs to be reset.
2. Issue the `reload module` command to reset the identified module. This command power cycles the selected module.
**DETAILED STEPS**

**Step 1** Identify the module that needs to be reset.

**Step 2** Issue the `reload module` command to reset the identified module. This command power cycles the selected module.

```
reload module number
```

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

```
switch# reload module 2
```

**Caution** Reloading a module disrupts traffic through the module.

---

**Reloading Switching Modules**

Switching modules automatically download their images from the supervisor module and do not need a forced download. This procedure is provided for reference if a new image is required.

**SUMMARY STEPS**

1. Identify the switching module that requires the new image.
2. Issue the `reload module` command to update the image on the switching module.

---

**DETAILED STEPS**

**Step 1** Identify the switching module that requires the new image.

**Step 2** Issue the `reload module` command to update the image on the switching module.

```
reload module number force-dnld
```

`number` indicates the slot in which the identified module resides. In this example, the identified module resides in slot 9:

```
switch# reload module 9 force-dnld
```

Jan 1 00:00:46 switch %LC-2-MSG:SLOT9 LOG_LC-2-IMG_DNLD_COMPLETE: COMPLETED
downloading of linecard image. Download successful...

---

**Saving the Module Configuration**

Issue the `copy running-config startup-config` command to save the new configuration into nonvolatile storage. Once this command is issued, the running and the startup copies of the configuration are identical.
This table displays various scenarios when module configurations are preserved or lost.

**Table 28: Switching Module Configuration Status**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>You remove a switching module and issue the <code>copy running-config startup-config</code> command.</td>
<td>The configured module information is lost.</td>
</tr>
<tr>
<td>You remove a switching module and reininsert the same switching module before issuing the <code>copy running-config startup-config</code> command.</td>
<td>The configured module information is saved.</td>
</tr>
<tr>
<td>You remove a switching module, insert the same type switching module in the same slot, and issue a <code>reload module number</code> command.</td>
<td>The configured module information is saved.</td>
</tr>
<tr>
<td>You enter a <code>reload module number</code> command to reload a switching module.</td>
<td>The configured module information is preserved.</td>
</tr>
<tr>
<td>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.</td>
<td>The configured module information is lost from the running configuration. The default configuration is applied.</td>
</tr>
<tr>
<td>Sample scenario:</td>
<td></td>
</tr>
<tr>
<td>1. The switch currently has a 16-port switching module and the startup and running configuration files are the same.</td>
<td></td>
</tr>
<tr>
<td>2. You replace the 16-port switching module in the switch with a 32-port switching module.</td>
<td></td>
</tr>
<tr>
<td>3. Next, you remove the 32-port switching module and replace it with the same 16-port switching module referred to in Step 1.</td>
<td></td>
</tr>
<tr>
<td>4. You enter the <code>reload</code> command to reload the switch.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Purging Module Configurations**

Enter the `purge module slot running-config` command to delete the configuration in a specific module. Once you enter this command, the Cisco NX-OS software clears the running configuration for the specified slot. This command does not work on supervisor modules or on any slot that currently has a module. This command only works on an empty slot (where the specified module once resided).

The `purge module` command clears the configuration for any module that previously existed in a slot and has since been removed. While the module was in that slot, some parts of the configuration may have been stored in the running configuration and cannot be reused (for example, IP addresses), unless you clear it from the running configuration.
For example, suppose you create an IP storage configuration with an IPS module in slot 3 in Switch A. This module uses IP address 10.1.5.500. You decide to remove this IPS module and move it to Switch B, and you no longer need the IP address 10.1.5.500. If you try to configure this unused IP address, you will receive an error message that prevents you from proceeding with the configuration. In this case, you must enter the `purge module 3 running-config` command to clear the old configuration on Switch A before proceeding with using this IP address.

**Powering Off Switching Modules**

You can power off a switching module from the command-line interface (CLI). By default, all switching modules are in the power up state when the chassis loads or you insert the module into the chassis.

**SUMMARY STEPS**

1. `configure terminal`
2. `[no] poweroff module slot`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>[no] poweroff module slot</code></td>
<td>Powers off the specified module. Use the <code>no</code> form of the command to power on a module.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# poweroff module 2</td>
<td></td>
</tr>
</tbody>
</table>
# Identifying Module LEDs

This table describes the LEDs for the Cisco MDS 9200 Series integrated supervisor modules.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Green</td>
<td>All diagnostics pass. The module is operational (normal initialization sequence).</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>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.</td>
</tr>
<tr>
<td>Speed</td>
<td>On</td>
<td>2-Gbps mode and beacon mode disabled.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>1-Gbps mode and beacon mode disabled.</td>
</tr>
<tr>
<td></td>
<td>Flashing</td>
<td>Beacon mode enabled.</td>
</tr>
<tr>
<td>LED</td>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Link</td>
<td>Solid green</td>
<td>Link is up.</td>
</tr>
<tr>
<td></td>
<td>Solid yellow</td>
<td>Link is disabled by software.</td>
</tr>
<tr>
<td></td>
<td>Flashing yellow</td>
<td>A fault condition exists.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No link.</td>
</tr>
</tbody>
</table>

This table describes the LEDs for the Cisco MDS 9200 Series interface module.

Table 30: LEDs on the Cisco MDS 9200 Series Interface Module

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Green</td>
<td>All diagnostics pass. The module is operational (normal initialization sequence).</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>The module is booting or running diagnostics (normal initialization sequence).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or The inlet air temperature of the system has exceeded the maximum system operating temperature limit (a minor environmental warning).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To ensure maximum product life, you should immediately correct the environmental temperature and restore the system to normal operation.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>The diagnostic test failed. The module is not operational because a fault occurred during the initialization sequence.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>LED</td>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System</td>
<td>Green</td>
<td>All chassis environmental monitors are reporting OK.</td>
</tr>
<tr>
<td>Orange</td>
<td></td>
<td>The power supply failed or the power supply fan failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incompatible power supplies are installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The redundant clock failed.</td>
</tr>
<tr>
<td>Red</td>
<td></td>
<td>The temperature of the supervisor module exceeded the major threshold.</td>
</tr>
<tr>
<td>MGMT 10/100 Ethernet Link LED</td>
<td>Green</td>
<td>Link is up.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No link.</td>
</tr>
<tr>
<td>MGMT 10/100 Ethernet Activity LED</td>
<td>Green</td>
<td>Traffic is flowing through port.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No link or no traffic.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Green</td>
<td>All diagnostics pass. The module is operational (normal initialization sequence).</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>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.</td>
</tr>
<tr>
<td>Speed</td>
<td>On</td>
<td>2-Gbps mode.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>1-Gbps mode.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>Solid green</td>
<td>Link is up.</td>
</tr>
<tr>
<td></td>
<td>Steady flashing green</td>
<td>Link is up (beacon used to identify port).</td>
</tr>
<tr>
<td></td>
<td>Intermittent flashing green</td>
<td>Link is up (traffic on port).</td>
</tr>
<tr>
<td></td>
<td>Solid yellow</td>
<td>Link is disabled by software.</td>
</tr>
<tr>
<td></td>
<td>Flashing yellow</td>
<td>A fault condition exists.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No link.</td>
</tr>
</tbody>
</table>

Table 32: LEDs for the Cisco MDS 9500 Series Supervisor Modules

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>All diagnostics pass. The module is operational (normal initialization sequence).</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>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).</td>
</tr>
</tbody>
</table>
**EPLD Images**

Switches and directors in the Cisco MDS 9000 Family contain several electrical programmable logical devices (EPLDs) that provide hardware functionalities in all modules. EPLD image upgrades are periodically provided to include enhanced hardware functionality or to resolve known issues.
Tip
Refer to the Cisco MDS NX-OS Release Notes to verify if the EPLD has changed for the Cisco NX-OS image version being used.

Upgrading EPLD Images

You can upgrade the EPLD images on the modules.

Note
The same procedure used to upgrade the EPLD images on a module can be used to downgrade the EPLD images.

SUMMARY STEPS

1. Log into the switch through the console port, an SSH session, or a Telnet session.
2. Enter the `show version` command to verify the Cisco MDS NX-OS software release running on the MDS switch.
3. If necessary, upgrade the Cisco MDS NX-OS software running on your switch (see the Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide).
4. Issue the `dir bootflash:` or `dir slot0:` command to verify that the EPLD software image file corresponding to your Cisco MDS NX-OS release is present on the active supervisor module. For example, if your switch is running Cisco MDS SAN-OS Release 2.1(2), you must have `m9000-epld-2.1.2.img` in bootflash: or slot0: on the active supervisor module.
5. If you need to obtain the appropriate EPLD software image file, follow these steps:
6. Use the `install module number epld url` command on the active supervisor module to upgrade EPLD images for a module.

DETAILED STEPS

**Step 1**
Log into the switch through the console port, an SSH session, or a Telnet session.

**Step 2**
Enter the `show version` command to verify the Cisco MDS NX-OS software release running on the MDS switch.

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public License or the GNU Lesser General Public License. A copy of each such license is available at http://www.gnu.org/licenses/gpl.html and http://www.gnu.org/licenses/lgpl.html

Software
BIOS: version 1.0.8
loader: version unavailable [last: 1.0(0.267c)]
kickstart: version 2.1(2) [build 2.1(2.47)] [gdb]
system: version 2.1(2) [build 2.1(2.47)] [gdb]
```
... 

Step 3  If necessary, upgrade the Cisco MDS NX-OS software running on your switch (see the Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide).

Step 4  Issue the `dir bootflash:` or `dir slot0:` command to verify that the EPLD software image file corresponding to your Cisco MDS NX-OS release is present on the active supervisor module. For example, if your switch is running Cisco MDS SAN-OS Release 2.1(2), you must have m9000-epld-2.1.2.img in bootflash: or slot0: on the active supervisor module.

```
switch# dir bootflash:
    12288 Jan 01 00:01:07 1980 lost+found/
    2337571 May 31 13:43:02 2005 m9000-epld-2.1.2.img
...
```

You can find the EPLD images at the following URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/mds-epld

Step 5  If you need to obtain the appropriate EPLD software image file, follow these steps:

1. Download the EPLD software image file from Cisco.com to your FTP server.

2. Verify that you have enough free space available on the active and standby supervisor memory devices that you plan to use, either bootflash: or slot0:. The download site on Cisco.com shows the size of the EPLD image file in bytes.

The following example shows how to display the available memory for the bootflash: devices on the active and standby supervisors:

```
switch# dir bootflash:
    12288 Jan 01 00:01:06 1980 lost+found/
    14765056 Mar 21 15:35:06 2005 m9500-sfie9-kickstart-mz.2.1.1.bin
    15944704 Apr 06 16:46:04 2005 m9500-sfie9-kickstart-mz.2.1.1a.bin
    48063243 Mar 21 15:34:46 2005 m9500-sfie9-mz.2.1.1.bin
    48036239 Apr 06 16:45:41 2005 m9500-sfie9-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/
    14766506 Mar 21 15:35:06 2005 m9500-sfie9-kickstart-mz.2.1.1.bin
    15944704 Apr 06 16:46:04 2005 m9500-sfie9-kickstart-mz.2.1.1a.bin
```
Managing Modules

Upgrading EPLD Images

Usage for bootflash://sup-local
141066240 bytes used
43493376 bytes free
184559616 bytes total

switch(standby)# exit
switch#

The following example shows how to display the available memory for the slot0: devices on the active and standby supervisors:

switch# dir slot0:
  12288 Jan 01 00:01:06 1980 lost+found/
  14765056 Mar 21 15:35:06 2005 m9500-sf1ek9-kickstart-mz.2.1.1.bin
  15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
  48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
  48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-mz.2.1.1a.bin

Usage for slot:
141066240 bytes used
43493376 bytes free
184559616 bytes total

switch# show module
Mod Ports Module-Type Model Status
--- ----- -------------------------------- ------------------ ------------
 2  32 Storage Services Module DS-X9032-SSM ok
 5  0 Supervisor/Fabric-1 DS-X9530-SF1-K9 active *
 6  0 Supervisor/Fabric-1 DS-X9530-SF1-K9 ha-standby
...

The show module command output shows that the standby supervisor is in slot 6. Use the attach command to access the supervisor module.

switch# attach module 6
...
switch(standby)# dir slot0:
  12288 Jan 01 00:01:06 1980 lost+found/
  14765056 Mar 21 15:35:06 2005 m9500-sf1ek9-kickstart-mz.2.1.1.bin
  15944704 Apr 06 16:46:04 2005 m9500-sf1ek9-kickstart-mz.2.1.1a.bin
  48063243 Mar 21 15:34:46 2005 m9500-sf1ek9-mz.2.1.1.bin
  48036239 Apr 06 16:45:41 2005 m9500-sf1ek9-mz.2.1.1a.bin

Usage for slot0:
141066240 bytes used
43493376 bytes free
184559616 bytes total

switch(standby)# exit
switch#

3. If there is not enough space, delete unneeded files.

switch# delete bootflash:m9500-sf1ek9-kickstart-mz.2.1.1.bin
The `show module` command output shows that the standby supervisor is in slot 6. Use the `attach` command to access the supervisor module.

```
switch# attach module 6
switch(standby)# delete bootflash:m9500-sfle9-kickstart-mz.2.1.1.bin
switch(standby)# exit
switch#
```

4. Copy the EPLD image file from the FTP server to the bootflash: or slot0: device in the active supervisor module. The following example shows how to copy to bootflash:

```
switch# copy ftp://10.1.7.2/m9000-epld-2.1.2.img bootflash:m9000-epld-2.1.2.img
```

**Note**

The system will automatically synchronize the 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

<table>
<thead>
<tr>
<th>EPLD</th>
<th>Curr Ver</th>
<th>New Ver</th>
</tr>
</thead>
<tbody>
<tr>
<td>XBUS IO</td>
<td>0x07</td>
<td>0x07</td>
</tr>
<tr>
<td>UD Flow Control</td>
<td>0x05</td>
<td>0x05</td>
</tr>
<tr>
<td>PCI ASIC I/F</td>
<td>0x05</td>
<td>0x05</td>
</tr>
<tr>
<td>PCI Bridge</td>
<td>0x05</td>
<td>0x07</td>
</tr>
</tbody>
</table>

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
```
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
```
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

*Example:*

```
switch# configure terminal
switch(config)#
```
### Command or Action

| Step 2 | `[no]` `ssm upgrade delay seconds`  
Example:  
```
switch(config)# ssm upgrade delay 30
``` |

**Purpose**  
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
``` |

**Purpose**  
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

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.
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:

<table>
<thead>
<tr>
<th>Module</th>
<th>Image</th>
<th>Running-Version</th>
<th>New-Version</th>
<th>Upg-Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>slc</td>
<td>2.0(3)</td>
<td>2.1(1a)</td>
<td>yes</td>
</tr>
<tr>
<td>2</td>
<td>bios</td>
<td>v1.1.0(10/24/03)</td>
<td>v1.1.0(10/24/03)</td>
<td>no</td>
</tr>
<tr>
<td>3</td>
<td>slc</td>
<td>2.0(3)</td>
<td>2.1(1a)</td>
<td>yes</td>
</tr>
<tr>
<td>3</td>
<td>SSI</td>
<td>2.0(3)</td>
<td>2.1(1a)</td>
<td>yes</td>
</tr>
<tr>
<td>3</td>
<td>bios</td>
<td>v1.0.8(08/07/03)</td>
<td>v1.1.0(10/24/03)</td>
<td>yes</td>
</tr>
<tr>
<td>4</td>
<td>ips4</td>
<td>2.0(3)</td>
<td>2.1(1a)</td>
<td>yes</td>
</tr>
<tr>
<td>4</td>
<td>bios</td>
<td>v1.1.0(10/24/03)</td>
<td>v1.1.0(10/24/03)</td>
<td>no</td>
</tr>
<tr>
<td>5</td>
<td>system</td>
<td>2.0(3)</td>
<td>2.1(1a)</td>
<td>yes</td>
</tr>
<tr>
<td>5</td>
<td>kickstart</td>
<td>2.0(3)</td>
<td>2.1(1a)</td>
<td>yes</td>
</tr>
<tr>
<td>5</td>
<td>bios</td>
<td>v1.1.0(10/24/03)</td>
<td>v1.1.0(10/24/03)</td>
<td>no</td>
</tr>
<tr>
<td>5</td>
<td>loader</td>
<td>1.2(2)</td>
<td>1.2(2)</td>
<td>no</td>
</tr>
</tbody>
</table>

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 33: Default Supervisor Module Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative connection</td>
<td>Serial connection.</td>
</tr>
<tr>
<td>Global switch information</td>
<td>• No value for system name.</td>
</tr>
<tr>
<td></td>
<td>• No value for system contact.</td>
</tr>
<tr>
<td></td>
<td>• No value for location.</td>
</tr>
<tr>
<td>System clock</td>
<td>No value for system clock time.</td>
</tr>
<tr>
<td>In-band (VSAN 1) interface</td>
<td>IP address, subnet mask, and broadcast address assigned to the VSAN are set to 0.0.0.0.</td>
</tr>
</tbody>
</table>
This table lists the default settings for the SSM.

**Table 34: Default Supervisor Module Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial state when installed</td>
<td>• Power-down state on switches with Cisco MDS SAN-OS Release 2.1(1a) and earlier installed.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
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 195
- Guidelines and Limitations, on page 195
- Information about Tcl, on page 197

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#
```
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
```

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
```

**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 initial 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 iterations.

**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 tel 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>tclsh [bootflash:filename [argument ... ]]</code></td>
<td>Starts a tcl shell.</td>
</tr>
</tbody>
</table>

**Example:**

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:

```
```
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>tclsh</td>
<td>Starts an interactive tcl shell.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# tclsh</td>
<td>switch-tcl#</td>
</tr>
</tbody>
</table>

| **Step 2** | | |
| configure terminal | Runs a Cisco NX-OS command in the tcl shell, changing modes. |
| **Example:** | The tcl prompt changes to indicate the Cisco NX-OS command mode. |
| switch-tcl# configure terminal | |
| switch(config-tcl)# | |

| **Step 3** | | |
| tclquit | Terminates the tcl shell and returns to the starting mode. |
| **Example:** | |
| switch-tcl# tclquit | switch# |

**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:

INDEX

--More-- prompt 59
  filtering output 59
  searching output 59

A

aliases, See command aliases
archive files 103, 104, 105
  appending files 104
  creating 103
  displaying the contents to the screen 105
  extracting files 105
  listing archived filenames 105

B

banners, See MOTD banners
BIOS 64
  loader> prompt 64
boot variables 116
  erasing configuration 116

C

Call Home 4
  description 4
CDP 121, 123, 124, 125
  clearing cache 124
  clearing counters 124
  clearing statistics 124
  clearing tables 124
  configuring timers, example 125
  default settings 125
  description 121
  optional parameters 123
  verifying configuration 124
characters 41
  special 41
Cisco Embedded Event Manager, . See EEM
Cisco MDS 9200 Series interfaces modules 177
  LED description 177
Cisco MDS 9200 Series supervisor modules 177
  LED description 177

Cisco MDS 9200 Series switching modules 177
  LED description 177
CLI 37, 38, 44, 60, 61, 62, 64
  command history 60
  command modes 38
  command name completion 44
  command prompt 37
  configuring the edit mode 61
  disabling confirmation prompts 62
  enabling confirmation prompts 62
  examples 64
  setting display colors 62
CLI history 61
  controlling command recall 61
CLI prompt 37
  description 37
CLI variables 46, 47, 64, 65
  characteristics 46
  description 46
  examples 64
  persistent 47
  referencing 46
  session-only 47
  system-defined variables 65
clock modules 28, 33
  description 28, 33
  displaying information 28, 33
clocks 84, 91, 94
  default settings 94
  description 84
  setting manually 91
COM1 port 68
  settings 68
COM1 ports 71, 75, 80
  configuring settings 71
  default settings 80
  enabling modem connections 75
command aliases 48, 49, 64
  characteristics 48
  defining 49
  description 48
  examples 64
  user session only 49
command history 60, 61
  description 60
INDEX

command history (continued)
  displaying  61
command modes  38, 39, 40
  description  38
EXEC  38
  global configuration  38
interface  39
restoring  40
saving  40
subinterface  39
summary (table)  40
command scripts  50, 51, 65
  delaying command actions  51
  description  50
  echoing text to terminals  50
  examples  65
commands  43, 45, 60
  abbreviations  43
  no form  45
  recalling  60
commands scripts  50
  running  50
CompactFlash  149
  running tests  149
compatibility  3
  software  3
configuration  35, 93, 117
  displaying  35, 93, 117
configuration files  107, 108, 111, 114, 115, 116, 118
  copying from remote servers  108
  copying to external memory  111
  copying to internal file systems  114
  description  107
  erasing  116
  example backup  118
  example copy  118
  example roll back  118
  rolling back to previous configurations  115
  types  107
configuration prompts  62
  disabling  62
  enabling  62
configuring devices  31, 32, 33, 34, 35
  POAP process  31, 32, 33, 34
    DHCP phase  33
    post-installation reload phase  34
    power up phase  32
    script execution phase  34
    using POAP  35
console ports  67, 69, 75, 80
  configuring settings  69
  default settings  80
  enabling modem connections  75
  settings  67
context-sensitive help
  syntax checking  52

D

daylight savings time, See summer time
default gateway  84
  description  84
default settings  80, 94, 125, 143, 165
  CDP  125
  clocks  94
  COM1 ports  80
  console ports  80
  modems  80
  MOTD banners  94
  NTP  143
  system hardware  165
  Telnet servers  94
  terminals  80
  virtual terminals  80
diagnostics, See online diagnostics
diff utility  57
  description  57
directories  96, 98, 99
  changing current directories  99
  creating  99
  description  96
  displaying contents  99
  displaying current directory  98
  working with  98
downgrading  190
  guidelines  190

E

EDLD images  183
  downgrading  183
EEM  4
  description  4
egrep utility  57
  filtering show command output  57
  searching show command output  57
EPLD images  182, 183, 187
  description  182
  displaying versions  187
  upgrading  183
examples  106, 118
  accessing directories on standby supervisor modules  106
  backing up configuration files  118
  copying configuration files  118
  rolling back to a previous configuration  118
EXEC command mode  38
  description  38

F

fan modules  162
  description  162
files 95, 99, 100
   accessing standby supervisor modules 100
   changing current directories 99
   description 95
   specifying 95
files 96, 100, 101, 102, 103
   compressing 102
   copying 101
   deleting 101
   description 96
   displaying checksums 102
   displaying contents 101
   displaying last lines 103
   finding 103
   moving 100
   redirecting command output 103
   renaming 100
   tar files 103
   uncompressing 102
files systems 98
   displaying current directory 98
filtering 55, 57, 58, 59
   --More-- prompt 59
   diff utility 57
   egrep utility 57
   grep utility 57
   keywords 55
   less utility 58
   sed utility 58
   show command output 55
G
   global configuration command mode 38
      description 38
   global configuration mode 40
      summary 40
   grep utility 57
   searching show command output 57
   grep utility filtering show command output 57
   guidelines and limitations 28
      POAP 28
H
   hardware 145
      displaying inventory 145
   high availability 122
      CDP 122
      NTP 122
   hostname 83, 85
      configuring 85
      description 83
I
   Interface configuration command mode 39
      description 39
   interface configuration mode 40
      summary 40
K
   keystrokes 41
      shortcuts 41
L
   LEDs 177
      descriptions 177
   less utility 58
      filtering show command output 58
      searching show command output 58
   licensing 8
   support 8
   loader> prompt 64
      description 64
M
   manageability 6
      description 6
   management 19
      configuring in-band management 19
      management interface 86
      configuring 86
   message-of-the-day banners, See MOTD banners
   modems 68, 75, 76, 77, 78, 80
      configuring connections 75
      configuring user-specific initialization strings 77
      default settings 80
      downloading initialization string 76
      enabling connections 75
      initializing connection 78
      settings 68
   modes, See command modes
   module temperature monitoring 160
      description 160
      checking states 172
      connecting to with CLI 172
      description 167
      monitoring temperatures 160
      power cycling 173
      purging configurations 175
      reloading 173
      removing configuration after removal 116
      saving configurations 174
      sending commands from the supervisor module session 63
modules (continued)
  services modules 170
  supervisor modules 168
  switching modules 169
  verifying status 171
MOTD banner 88
  configuring 88
MOTD banners 84,94
  default settings 94
  description 84
MSMs 188
  configuring global delay timers 188

N
NTP 7,122,127,128,129,135,141,143
  clearing a session 138
  clearing statistics 135,138
  configuring a server, example 141
  default settings 143
  description 7,127
  displaying statistics 135
  guidelines 129
  high availability 122
  limitations 129
  prerequisites 128
  verifying configuration 138
NTP configuration distribution 136
  enabling 136
NTP configuration distribution 137,138
  committing changes 137
  discarding changes 137
  releasing the fabric session lock 138

O
online diagnostics 4
  description 4

P
POAP 28,31,33,34,35
  DHCP discovery phase 33
  guidelines and limitations 28
  post-installation reload phase 34
  process 31
  using to configure a switch 35
  power 150
  displaying usage information 150
  power cycling 173
  modules 173
Power On Auto Provisioning 32
  power up phase 32
Power On Auto Provisioning (continued)
  provisioning devices 32
    POAP process 32
      power up phase 32
  power supply mode 151
    description 151
  power supply modes 152,159
    configuration guidelines 152
    configuring 159
PowerOn Auto Provisioning 33,34
  script execution phase 34
  privileged EXEC mode 40
  summary 40
prompts. See confirmation prompts
provisioning devices 31,33,34
  POAP process 31,33,34
    DHCP phase 33
    post-installation reload phase 34
    script execution phase 34

Q
QoS 9
  description 9
  Quality of Service. See QoS

R
RBAC 6
  description 6
  regular expressions 53,54
    anchoring 54
    filtering CLI output 53
    multiple-character patterns 54
    special characters 53
  role-based access control. See RBAC
running configuration 35,93,117
  displaying 35,93,117
  running configurations 108,109,112,114,115,116,118
    copying from external memory devices 112
    copying to internal file systems 114
    downloading from remote servers 109
    example backup 118
    example copy 118
    example roll back 118
    removing configuration for missing modules 116
    rolling back to previous configurations 115
    saving to startup configurations 108

S
scripts. See command scripts
searching 55,57,58,59
  --More-- prompt 59
  diff utility 57
searching (continued)
  egrep utility 57
  grep utility 57
  keywords 55
  less utility 58
  sed utility 58
  show command output 55
sed utility 58
  filtering show command output 58
  searching show command output 58
serial number 149
  displaying 149
serviceability 3
  description 3
services modules 170
  description 170
setup utility 11, 13
  description 11
  prerequisites 13
shortcuts 41
  keystrokes 41
show commands 55
  filtering output 55
  searching output 55
Simple Network Management Protocol. See SNMP
SNMP 6
  description 6
software compatibility 3
  description 3
sort utility 58
  description 58
SPAN 4
  description 4
special characters 41
  description 41
sscp 55, 59, 66
  example 66
  redirecting show command output 55, 59
SSI boot images 188
  description 188
SSMs 188, 189, 192
  configuring global delay timers 188
  default settings 192
  downgrading software, guidelines 188
  recovering after replacing corrupted Compact Flash 189
  replacing, guidelines 189
  upgrading software, guidelines 188
standby supervisor modules 100, 106
  accessing directories, examples 106
  accessing file systems 100
startup configuration 35, 93, 116, 117
  displaying 35, 93, 117
  erasing 116
startup configurations (continued)
  copying from external memory devices 113
  copying from running configurations 108
  copying to internal file systems 114
  downloading from remote servers 110
  example backup 118
  example copy 118
  example rollback 118
  rolling back to previous configurations 115
storage 97
  device operation 97
streaming secure copy. See sscp
subinterface configuration command mode 39
  description 39
subinterface configuration mode 40
  summary 40
summer time 85, 90
  configuring 90
  description 85
supervisor modules 168, 188, 189, 192
  default settings 192
  description 168
  downgrading, guidelines 188
  replacing, guidelines 188, 189
  upgrading, guidelines 188
Switched Port Analyzer. See SPAN
switches 173
  reloading 173
  switching module 174
  reloading 174
  switching modules 169, 176
  description 169
  powering off 176
switchname 83, 85
  configuring 85
syntax checking. See context-sensitive help
system hardware 165
  default settings 165
T
tcl 195, 196, 197, 200
  cli commands 196
  command separation 196
  history 196
  no interactive help 195
  options 197
  references 200
  sandbox 197
  security 197
  tab completion 196
  telquit command 197
  variables 197
Telnet servers 85, 93, 94
  connections 85
  default settings 94
  disabling connection 93
Telnet servers (continued)
   enabling connection 93
terminal sessions 67, 79
   clearing 79
   displaying information 79
   settings 67
terminals 80
   default settings 80
time zones 85, 89
   configuring 89
   description 85
Tool Command Language, See tcl

U
   upgrading 190
   guidelines 190

user sessions 85, 92
   description 85
   sending messages 92
users 92
   managing 92
users sessions 92
   displaying information 92

V
variables, See CLI variables
virtual terminals 68, 72, 74, 80
   configuring 72
   configuring session limits 74
   default settings 80
   settings 68