



System Management Configuration Guide, Cisco IOS XE Amsterdam 17.1.x (Catalyst 9600 Switches)

First Published: 2019-11-26

Americas Headquarters

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

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

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

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

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

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

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

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

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

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

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Administering the Device 1

Information About Administering the Device 1

System Time and Date Management 1

System Clock 1

Network Time Protocol 2

NTP Stratum 3

NTP Associations 3

NTP Security 5

NTP Services on a Specific Interface 6

Source IP Address for NTP Packets 6

NTP Implementation 6

System Name and Prompt 7

Stack System Name and Prompt 8

Default System Name and Prompt Configuration 8

DNS 8

Default DNS Settings 8

Login Banners 8

Default Banner Configuration 9

MAC Address Table 9

MAC Address Table Creation 9

MAC Addresses and VLANs 9

MAC Addresses and Device Stacks 9

Default MAC Address Table Settings 10

ARP Table Management 10

How to Administer the Device 10

Configuring the Time and Date Manually 10

| | |
|---|----|
| Setting the System Clock | 11 |
| Configuring the Time Zone | 11 |
| Configuring Summer Time (Daylight Saving Time) | 12 |
| Configuring NTP | 14 |
| Default NTP Configuration | 14 |
| Configuring NTP Authentication | 15 |
| Configuring Poll-Based NTP Associations | 16 |
| Configuring Broadcast-Based NTP Associations | 18 |
| Configuring NTP Access Restrictions | 19 |
| Configuring a System Name | 21 |
| Setting Up DNS | 22 |
| Configuring a Message-of-the-Day Login Banner | 24 |
| Configuring a Login Banner | 25 |
| Managing the MAC Address Table | 26 |
| Changing the Address Aging Time | 26 |
| Configuring MAC Address Change Notification Traps | 27 |
| Configuring MAC Address Move Notification Traps | 29 |
| Configuring MAC Threshold Notification Traps | 31 |
| Disabling MAC Address Learning on VLAN | 33 |
| Adding and Removing Static Address Entries | 34 |
| Configuring Unicast MAC Address Filtering | 36 |
| Monitoring and Maintaining Administration of the Device | 36 |
| Configuration Examples for Device Administration | 37 |
| Example: Setting the System Clock | 37 |
| Examples: Configuring Summer Time | 38 |
| Example: Configuring a MOTD Banner | 38 |
| Example: Configuring a Login Banner | 38 |
| Example: Configuring MAC Address Change Notification Traps | 39 |
| Example: Configuring MAC Threshold Notification Traps | 39 |
| Example: Adding the Static Address to the MAC Address Table | 39 |
| Example: Configuring Unicast MAC Address Filtering | 40 |
| Additional References for Device Administration | 40 |
| Feature History for Device Administration | 40 |

CHAPTER 2**Boot Integrity Visibility 41**

- Information About Boot Integrity Visibility 41
- Verifying the Software Image and Hardware 41
- Verifying Platform Identity and Software Integrity 42
- Additional References for Boot Integrity Visibility 45
- Feature History for Boot Integrity Visibility 45

CHAPTER 3**Performing Device Setup Configuration 47**

- Information About Performing Device Setup Configuration 47
 - Device Boot Process 47
 - Devices Information Assignment 48
 - Default Switch Information 48
 - DHCP-Based Autoconfiguration Overview 49
 - DHCP Client Request Process 49
 - DHCP-based Autoconfiguration and Image Update 50
 - Restrictions for DHCP-based Autoconfiguration 50
 - DHCP Autoconfiguration 51
 - DHCP Auto-Image Update 51
 - DHCP Server Configuration Guidelines 51
 - Purpose of the TFTP Server 52
 - Purpose of the DNS Server 52
 - How to Obtain Configuration Files 53
 - How to Control Environment Variables 53
 - Common Environment Variables 54
 - Environment Variables for TFTP 56
 - Scheduled Reload of the Software Image 56
- How to Perform Device Setup Configuration 57
 - Configuring DHCP Autoconfiguration (Only Configuration File) 57
 - Configuring DHCP Auto-Image Update (Configuration File and Image) 59
 - Configuring the Client to Download Files from DHCP Server 61
 - Manually Assigning IP Information to Multiple SVIs 62
 - Modifying the Device Startup Configuration 64
 - Specifying the Filename to Read and Write the System Configuration 64

| | |
|---|----|
| Manually Booting the Switch | 65 |
| Configuring a Scheduled Software Image Reload | 66 |
| Monitoring Device Setup Configuration | 67 |
| Configuration Examples for Performing Device Setup | 67 |
| Example: Configuring a Device as a DHCP Server | 67 |
| Example: Configuring DHCP Auto-Image Update | 68 |
| Example: Configuring a Device to Download Configurations from a DHCP Server | 68 |
| Examples: Scheduling Software Image Reload | 68 |
| Additional References For Performing Device Setup | 69 |
| Feature History for Performing Device Setup Configuration | 69 |

CHAPTER 4

Configuring Smart Licensing 71

| | |
|---|----|
| Prerequisites for Configuring Smart Licensing | 71 |
| Introduction to Smart Licensing | 71 |
| Overview of CSSM | 72 |
| Connecting to CSSM | 72 |
| Configuring a Connection to CSSM and Setting Up the License Level | 74 |
| Setting Up a Connection to CSSM | 74 |
| Configuring the Call Home Service for Direct Cloud Access | 76 |
| Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server | 78 |
| Configuring the Call Home Service for Cisco Smart Software Manager On-Prem | 80 |
| Configuring the License Level | 83 |
| Registering a Device on CSSM | 84 |
| Generating a New Token from CSSM | 84 |
| Registering a Device with the New Token | 86 |
| Verifying the License Status After Registration | 87 |
| Canceling a Device's Registration in CSSM | 87 |
| Monitoring Smart Licensing Configuration | 88 |
| Configuration Examples for Smart Licensing | 89 |
| Example: Viewing the Call Home Profile | 89 |
| Example: Registering a Device | 89 |
| Additional References | 90 |
| Feature History for Smart Licensing | 90 |

| | | |
|------------------|---|------------|
| CHAPTER 5 | Environmental Monitoring and Power Management | 91 |
| | About Environmental Monitoring | 91 |
| | Using CLI Commands to Monitor your Environment | 91 |
| | Displaying Environment Conditions | 92 |
| | Displaying On Board Failure Logging (OBFL) information | 94 |
| | Emergency Actions | 95 |
| | System Alarms | 96 |
| | Power Management | 97 |
| | Restrictions for Power Management | 97 |
| | Power Supply Modes | 97 |
| | Operating States | 98 |
| | Power Management Considerations | 98 |
| | Selecting a Power Supply Mode | 99 |
| | Configuring the Redundant Mode | 99 |
| | Configuring the Combined Mode | 100 |
| | Power Budgeting for Supervisor Modules | 101 |
| | Configuring the Power Budget Mode for a Single Supervisor | 102 |
| | Moving from a Single to a Dual Supervisor Setup | 102 |
| | Powering Down a Line Card | 103 |
| | Configuration Examples for Operating States | 104 |
| | show power | 104 |
| | show power detail | 104 |
| | Feature History for Environmental Monitoring and Power Management | 105 |
| CHAPTER 6 | Configuring SDM Templates | 107 |
| | Information About SDM Templates | 107 |
| | SDM Templates and Switch Stacks | 107 |
| | How to Configure SDM Templates | 108 |
| | Setting the SDM Template | 108 |
| | Monitoring and Maintaining SDM Templates | 109 |
| | Configuration Examples for SDM Templates | 109 |
| | Examples: Displaying SDM Templates | 109 |
| | Examples: Configuring SDM Templates | 112 |

Additional References for SDM Templates 112

Feature History for SDM Templates 113

CHAPTER 7

Configuring System Message Logs 115

Information About Configuring System Message Logs 115

System Message Logging 115

System Log Message Format 116

Default System Message Logging Settings 117

Syslog Message Limits 117

How to Configure System Message Logs 118

Setting the Message Display Destination Device 118

Synchronizing Log Messages 119

Disabling Message Logging 120

Enabling and Disabling Time Stamps on Log Messages 121

Enabling and Disabling Sequence Numbers in Log Messages 122

Defining the Message Severity Level 122

Limiting Syslog Messages Sent to the History Table and to SNMP 123

Logging Messages to a UNIX Syslog Daemon 124

Monitoring and Maintaining System Message Logs 125

Monitoring Configuration Archive Logs 125

Configuration Examples for System Message Logs 125

Example: Switch System Message 125

Additional References for System Message Logs 126

Feature History for System Message Logs 126

CHAPTER 8

Configuring Online Diagnostics 127

Information About Configuring Online Diagnostics 127

Generic Online Diagnostics (GOLD) 128

TestPortTxMonitoring 128

TestUnusedPortLoopback 128

How to Configure Online Diagnostics 129

Starting Online Diagnostic Tests 129

Configuring Online Diagnostics 130

Monitoring and Maintaining Online Diagnostics 130

| | |
|--|-----|
| Configuration Examples for Online Diagnostic Tests | 130 |
| Examples: Start Diagnostic Tests | 130 |
| Examples: Displaying Online Diagnostics | 130 |
| Additional References for Online Diagnostics | 131 |
| Feature Information for Configuring Online Diagnostics | 131 |

CHAPTER 9

Managing Configuration Files 133

| | |
|--|-----|
| Prerequisites for Managing Configuration Files | 133 |
| Restrictions for Managing Configuration Files | 133 |
| Information About Managing Configuration Files | 133 |
| Types of Configuration Files | 133 |
| Configuration Mode and Selecting a Configuration Source | 134 |
| Configuration File Changes Using the CLI | 134 |
| Location of Configuration Files | 134 |
| Copy Configuration Files from a Network Server to the Device | 135 |
| Copying a Configuration File from the Device to a TFTP Server | 135 |
| Copying a Configuration File from the Device to an RCP Server | 136 |
| Copying a Configuration File from the Device to an FTP Server | 137 |
| Copying files through a VRF | 138 |
| Copy Configuration Files from a Switch to Another Switch | 138 |
| Configuration Files Larger than NVRAM | 139 |
| Configuring the Device to Download Configuration Files | 139 |
| How to Manage Configuration File Information | 140 |
| Displaying Configuration File Information | 140 |
| Modifying the Configuration File | 141 |
| Copying a Configuration File from the Device to a TFTP Server | 142 |
| What to Do Next | 143 |
| Copying a Configuration File from the Device to an RCP Server | 143 |
| Examples | 144 |
| What to Do Next | 145 |
| Copying a Configuration File from the Device to the FTP Server | 145 |
| Examples | 146 |
| What to Do Next | 147 |
| Copying a Configuration File from a TFTP Server to the Device | 147 |

| | |
|---|------------------------|
| What to Do Next | 148 |
| Copying a Configuration File from the rcp Server to the Device | 148 |
| Examples | 149 |
| What to Do Next | 149 |
| Copying a Configuration File from an FTP Server to the Device | 149 |
| Examples | 150 |
| What to Do Next | 151 |
| Maintaining Configuration Files Larger than NVRAM | 151 |
| Compressing the Configuration File | 151 |
| Storing the Configuration in Flash Memory on Class A Flash File Systems | 153 |
| Loading the Configuration Commands from the Network | 154 |
| Copying Configuration Files from Flash Memory to the Startup or Running Configuration | 155 |
| Copying Configuration Files Between Flash Memory File Systems | 156 |
| Copying a Configuration File from an FTP Server to Flash Memory Devices | 157 |
| What to Do Next | 158 |
| Copying a Configuration File from an RCP Server to Flash Memory Devices | 158 |
| Copying a Configuration File from a TFTP Server to Flash Memory Devices | 159 |
| Re-executing the Configuration Commands in the Startup Configuration File | 160 |
| Clearing the Startup Configuration | 160 |
| Deleting a Specified Configuration File | 161 |
| Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems | 162 |
| What to Do Next | 163 |
| Configuring the Device to Download Configuration Files | 164 |
| Configuring the Device to Download the Network Configuration File | 164 |
| Configuring the Device to Download the Host Configuration File | 165 |
| Feature History for Managing Configuration Files | 167 |
| | |
| CHAPTER 10 | Secure Copy 169 |
| Prerequisites for Secure Copy | 169 |
| Information About Secure Copy | 169 |
| How to Configure Secure Copy | 170 |
| Configuring Secure Copy | 170 |
| Enabling Secure Copy Protocol on the SSH Server | 171 |
| How to Configure Secure Copy | 173 |

| | |
|---|-----|
| Example: Secure Copy Configuration Using Local Authentication | 173 |
| Example: SCP Server-Side Configuration Using Network-Based Authentication | 173 |
| Additional References for Secure Copy | 173 |
| Feature History for Secure Copy | 174 |

CHAPTER 11

Configuration Replace and Configuration Rollback 175

| | |
|---|-----|
| Prerequisites for Configuration Replace and Configuration Rollback | 175 |
| Restrictions for Configuration Replace and Configuration Rollback | 176 |
| Information About Configuration Replace and Configuration Rollback | 176 |
| Configuration Archive | 176 |
| Configuration Replace | 177 |
| Configuration Rollback | 178 |
| Configuration Rollback Confirmed Change | 178 |
| Benefits of Configuration Replace and Configuration Rollback | 178 |
| How to Use Configuration Replace and Configuration Rollback | 179 |
| Creating a Configuration Archive | 179 |
| Performing a Configuration Replace or Configuration Rollback Operation | 180 |
| Monitoring and Troubleshooting the Feature | 183 |
| Configuration Examples for Configuration Replace and Configuration Rollback | 185 |
| Creating a Configuration Archive | 185 |
| Replacing the Current Running Configuration with a Saved Cisco IOS Configuration File | 185 |
| Reverting to the Startup Configuration File | 186 |
| Performing a Configuration Replace Operation with the configure confirm Command | 186 |
| Performing a Configuration Rollback Operation | 186 |
| Additional References for Configuration Replace and Configuration Rollback | 187 |
| Feature History for Configuration Replace and Configuration Rollback | 188 |

CHAPTER 12

BIOS Protection 189

| | |
|-------------------------------------|-----|
| Introduction to BIOS Protection | 189 |
| ROMMON Upgrade | 189 |
| Capsule Upgrade | 190 |
| Feature History for BIOS Protection | 190 |

CHAPTER 13

Software Maintenance Upgrade 193

| | |
|---|-----|
| Restrictions for Software Maintenance Upgrade | 193 |
| Information About Software Maintenance Upgrade | 193 |
| SMU Overview | 193 |
| SMU Workflow | 194 |
| SMU Package | 194 |
| SMU Reload | 194 |
| How to Manage Software Maintenance Updates | 194 |
| Installing an SMU Package | 194 |
| Managing an SMU Package | 195 |
| Configuration Examples for Software Maintenance Upgrade | 196 |
| Example: Managing an SMU | 197 |
| Additional References for Software Maintenance Upgrade | 201 |
| Feature History for Software Maintenance Upgrade | 202 |

CHAPTER 14

| | |
|---|------------|
| Working with the Flash File System | 203 |
| Information About the Flash File System | 203 |
| Displaying Available File Systems | 203 |
| Setting the Default File System | 205 |
| Displaying Information About Files on a File System | 205 |
| Changing Directories and Displaying the Working Directory | 206 |
| Creating Directories | 207 |
| Removing Directories | 207 |
| Copying Files | 207 |
| Deleting Files | 208 |
| Creating, Displaying and Extracting Files | 209 |
| Additional References for Flash File System | 210 |
| Feature History for Flash File System | 211 |

CHAPTER 15

| | |
|--|------------|
| Performing Factory Reset | 213 |
| Prerequisites for Performing a Factory Reset | 213 |
| Restrictions for Performing a Factory Reset | 213 |
| Information About Factory Reset | 213 |
| How to Perform a Factory Reset | 214 |
| Configuration Example for Performing a Factory Reset | 215 |

| | |
|--|-----|
| Additional References for Factory Reset | 216 |
| Feature History for Performing a Factory Reset | 216 |

CHAPTER 16

| | |
|--|------------|
| Configuring Secure Storage | 217 |
| Information About Secure Storage | 217 |
| Enabling Secure Storage | 217 |
| Disabling Secure Storage | 218 |
| Verifying the Status of Encryption | 218 |
| Feature Information for Secure Storage | 219 |

CHAPTER 17

| | |
|---|------------|
| Conditional Debug and Radioactive Tracing | 221 |
| Introduction to Conditional Debugging | 221 |
| Introduction to Radioactive Tracing | 222 |
| How to Configure Conditional Debug and Radioactive Tracing | 222 |
| Conditional Debugging and Radioactive Tracing | 222 |
| Location of Tracefiles | 222 |
| Configuring Conditional Debugging | 223 |
| Radioactive Tracing for L2 Multicast | 224 |
| Recommended Workflow for Trace files | 224 |
| Copying tracefiles off the box | 225 |
| Monitoring Conditional Debugging | 226 |
| Configuration Examples for Conditional Debugging | 226 |
| Additional References for Conditional Debugging and Radioactive Tracing | 227 |
| Feature History for Conditional Debugging and Radioactive Tracing | 227 |

CHAPTER 18

| | |
|---|------------|
| Consent Token | 229 |
| Restrictions for Consent Token | 229 |
| Information About Consent Token | 229 |
| Consent Token Authorization Process for System Shell Access | 230 |
| Feature History for Consent Token | 231 |

CHAPTER 19

| | |
|--|------------|
| Troubleshooting the Software Configuration | 233 |
| Information About Troubleshooting the Software Configuration | 233 |
| Software Failure on a Switch | 233 |

| | |
|---|-----|
| Lost or Forgotten Password on a Device | 233 |
| Ping | 234 |
| Layer 2 Traceroute | 234 |
| Layer 2 Traceroute Guidelines | 234 |
| IP Traceroute | 235 |
| Debug Commands | 236 |
| System Report | 236 |
| Onboard Failure Logging on the Switch | 238 |
| Fan Failures | 238 |
| Possible Symptoms of High CPU Utilization | 239 |
| How to Troubleshoot the Software Configuration | 239 |
| Recovering from a Lost or Forgotten Password | 239 |
| Procedure with Password Recovery Enabled | 240 |
| Procedure with Password Recovery Disabled | 241 |
| Preventing Switch Stack Problems | 243 |
| Preventing Autonegotiation Mismatches | 244 |
| Troubleshooting SFP Module Security and Identification | 244 |
| Executing Ping | 245 |
| Monitoring Temperature | 245 |
| Monitoring the Physical Path | 245 |
| Executing IP Traceroute | 246 |
| Redirecting Debug and Error Message Output | 246 |
| Using the show platform Command | 246 |
| Using the show debug command | 246 |
| Verifying Troubleshooting of the Software Configuration | 247 |
| Displaying OBFL Information | 247 |
| Example: Verifying the Problem and Cause for High CPU Utilization | 248 |
| Configuration Examples for Troubleshooting Software | 249 |
| Example: Pinging an IP Host | 249 |
| Example: Performing a Traceroute to an IP Host | 249 |
| Additional References for Troubleshooting Software Configuration | 250 |
| Feature History for Troubleshooting Software Configuration | 250 |



CHAPTER 1

Administering the Device

- [Information About Administering the Device, on page 1](#)
- [How to Administer the Device, on page 10](#)
- [Configuration Examples for Device Administration, on page 37](#)
- [Additional References for Device Administration, on page 40](#)
- [Feature History for Device Administration, on page 40](#)

Information About Administering the Device

System Time and Date Management

You can manage the system time and date on your device using automatic configuration methods (RTC and NTP), or manual configuration methods.



Note For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference* on Cisco.com.

System Clock

The basis of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- RTC
- NTP
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time appears correctly for the local time zone.

The system clock keeps track of whether the time is *authoritative* or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed.

Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

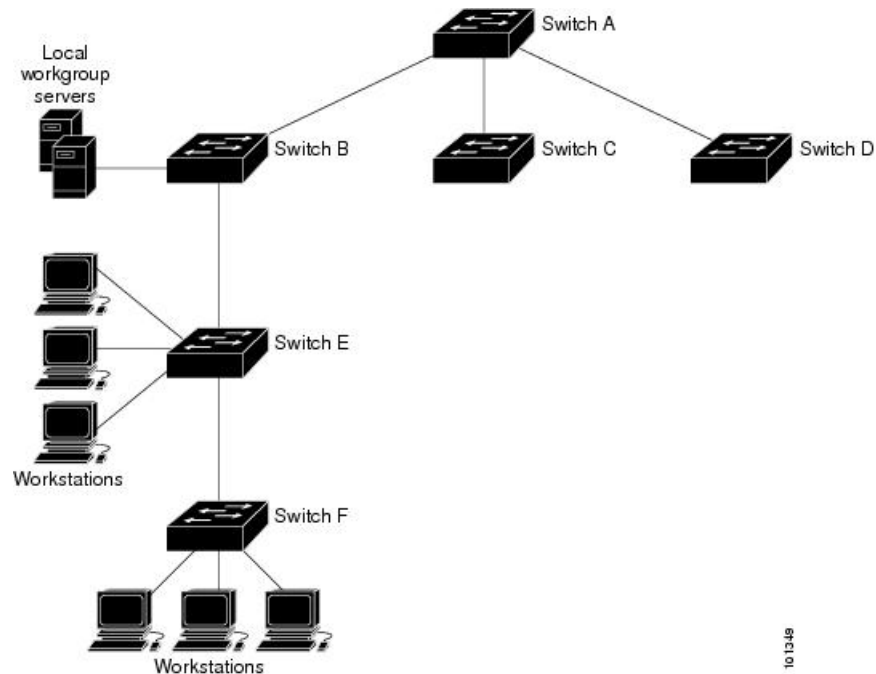
The communications between devices running NTP (known as associations) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

The Figure shows a typical network example using NTP. Device A is the primary NTP, with the **Device B**, **C**, and **D** configured in NTP server mode, in server association with Device A. Device E is configured as an NTP peer to the upstream and downstream device, Device B and Device F, respectively.

Figure 1: Typical NTP Network Configuration



If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

NTP Stratum

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

NTP Associations

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces

configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

Poll-Based NTP Associations

Networking devices running NTP can be configured to operate in variety of association modes when synchronizing time with reference time sources. A networking device can obtain time information on a network in two ways—by polling host servers and by listening to NTP broadcasts. This section focuses on the poll-based association modes. Broadcast-based NTP associations are discussed in the *Broadcast-Based NTP Associations* section.

The following are the two most commonly used poll-based association modes:

- Client mode
- Symmetric active mode

The client and the symmetric active modes should be used when NTP is required to provide a high level of time accuracy and reliability.

When a networking device is operating in the client mode, it polls its assigned time-serving hosts for the current time. The networking device will then pick a host from among all the polled time servers to synchronize with. Because the relationship that is established in this case is a client-host relationship, the host will not capture or use any time information sent by the local client device. This mode is most suited for file-server and workstation clients that are not required to provide any form of time synchronization to other local clients. Use the **ntp server** command to individually specify the time server that you want your networking device to consider synchronizing with and to set your networking device to operate in the client mode.

When a networking device is operating in the symmetric active mode, it polls its assigned time-serving hosts for the current time and it responds to polls by its hosts. Because this is a peer-to-peer relationship, the host will also retain time-related information of the local networking device that it is communicating with. This mode should be used when a number of mutually redundant servers are interconnected via diverse network paths. Most stratum 1 and stratum 2 servers on the Internet adopt this form of network setup. Use the **ntp peer** command to individually specify the time serving hosts that you want your networking device to consider synchronizing with and to set your networking device to operate in the symmetric active mode.

The specific mode that you should set for each of your networking devices depends primarily on the role that you want them to assume as a timekeeping device (server or client) and the device's proximity to a stratum 1 timekeeping server.

A networking device engages in polling when it is operating as a client or a host in the client mode or when it is acting as a peer in the symmetric active mode. Although polling does not usually place a burden on memory and CPU resources such as bandwidth, an exceedingly large number of ongoing and simultaneous polls on a system can seriously impact the performance of a system or slow the performance of a given network. To avoid having an excessive number of ongoing polls on a network, you should limit the number of direct, peer-to-peer or client-to-server associations. Instead, you should consider using NTP broadcasts to propagate time information within a localized network.

Broadcast-Based NTP Associations

Broadcast-based NTP associations should be used when time accuracy and reliability requirements are modest and if your network is localized and has more than 20 clients. Broadcast-based NTP associations are also recommended for use on networks that have limited bandwidth, system memory, or CPU resources.

A networking device operating in the broadcast client mode does not engage in any polling. Instead, it listens for NTP broadcast packets that are transmitted by broadcast time servers. Consequently, time accuracy can be marginally reduced because time information flows only one way.

Use the **ntp broadcast client** command to set your networking device to listen for NTP broadcast packets propagated through a network. For broadcast client mode to work, the broadcast server and its clients must be located on the same subnet. You must enable the time server that transmits NTP broadcast packets on the interface of the given device by using the **ntp broadcast** command.

NTP Security

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.



Note We do not recommend configuring Message Direct 5 (MD5) authentication. You can use other supported authentication methods for stronger encryption.

NTP Access Group

The access list-based restriction scheme allows you to grant or deny certain access privileges to an entire network, a subnet within a network, or a host within a subnet. To define an NTP access group, use the **ntp access-group** command in global configuration mode.

The access group options are scanned in the following order, from least restrictive to the most restrictive:

1. **ipv4** —Configures IPv4 access lists.
2. **ipv6** —Configures IPv6 access lists.
3. **peer** —Allows time requests and NTP control queries, and allows the system to synchronize itself to a system whose address passes the access list criteria.
4. **serve** —Allows time requests and NTP control queries, but does not allow the system to synchronize itself to a system whose address passes the access list criteria.
5. **serve-only** —Allows only time requests from a system whose address passes the access list criteria.
6. **query-only** —Allows only NTP control queries from a system whose address passes the access list criteria.

If the source IP address matches the access lists for more than one access type, the first type is granted access. If no access groups are specified, all access types are granted access to all systems. If any access groups are specified, only the specified access types will be granted access.

For details on NTP control queries, see RFC 1305 (NTP Version 3).

The encrypted NTP authentication scheme should be used when a reliable form of access control is required. Unlike the access list-based restriction scheme that is based on IP addresses, the encrypted authentication scheme uses authentication keys and an authentication process to determine if NTP synchronization packets sent by designated peers or servers on a local network are deemed as trusted before the time information that they carry along with them is accepted.

The authentication process begins from the moment an NTP packet is created. Cryptographic checksum keys are generated using the message digest algorithm 5 (MD5) and are embedded into the NTP synchronization

packet that is sent to a receiving client. Once a packet is received by a client, its cryptographic checksum key is decrypted and checked against a list of trusted keys. If the packet contains a matching authentication key, the time-stamp information that is contained within the packet is accepted by the receiving client. NTP synchronization packets that do not contain a matching authenticator key are ignored.



Note In large networks, where many trusted keys must be configured, the Range of Trusted Key Configuration feature enables configuring multiple keys simultaneously.

It is important to note that the encryption and decryption processes used in NTP authentication can be very CPU-intensive and can seriously degrade the accuracy of the time that is propagated within a network. If your network setup permits a more comprehensive model of access control, you should consider the use of the access list-based form of control.

After NTP authentication is properly configured, your networking device will synchronize with and provide synchronization only to trusted time sources.

NTP Services on a Specific Interface

Network Time Protocol (NTP) services are disabled on all interfaces by default. NTP is enabled globally when any NTP commands are entered. You can selectively prevent NTP packets from being received through a specific interface by using the **ntp disable** command in interface configuration mode.

Source IP Address for NTP Packets

When the system sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the **ntp source interface** command in global configuration mode to configure a specific interface from which the IP source address will be taken.

This interface will be used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **ntp peer** or **ntp server** command.

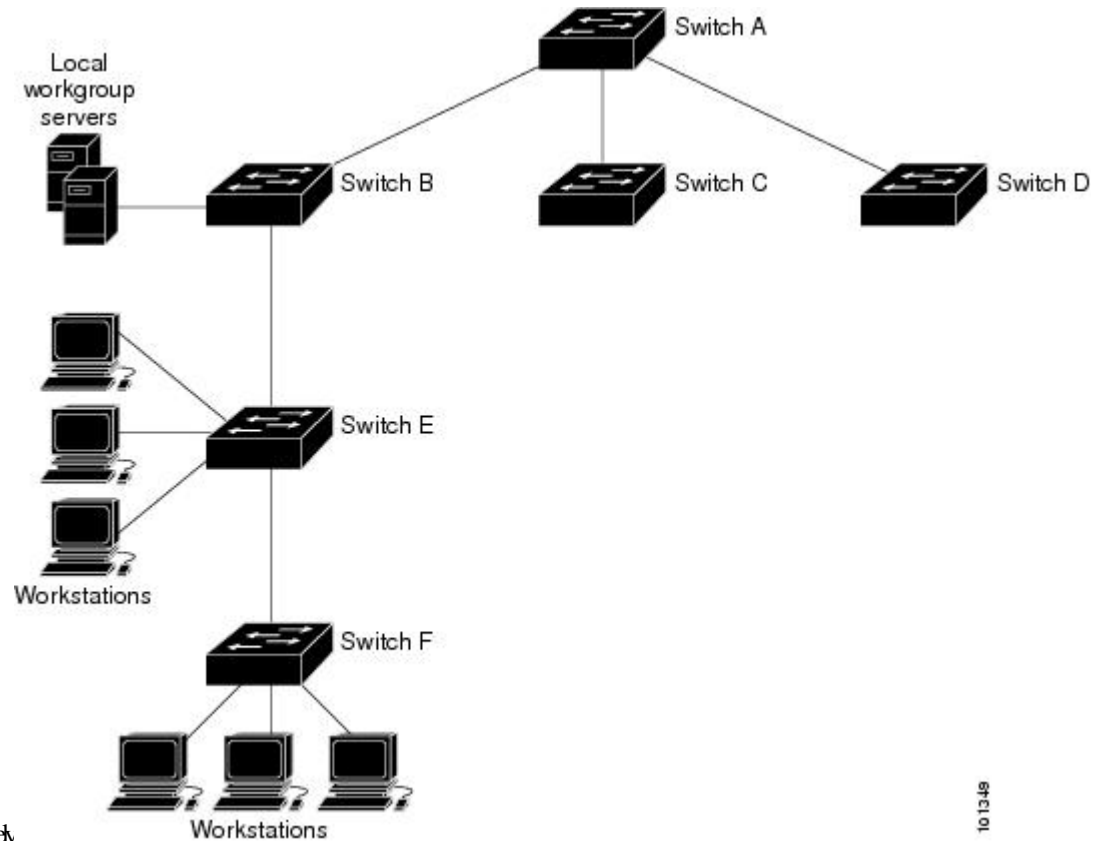
NTP Implementation

Implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

Figure 2: Typical NTP Network Configuration

The following figure shows a typical network example using NTP. Switch A is the primary NTP, with the Switch B, C, and D configured in NTP server mode, in server association with Switch A. Switch E is configured

as an NTP peer to the upstream and downstream switches, Switch B and Switch F,



respectively.

If the network is isolated from the Internet, NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

System Name and Prompt

You configure the system name on the device to identify it. By default, the system name and prompt are *Switch*.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol [*>*] is appended. The prompt is updated whenever the system name changes.

For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4* and the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*.

Stack System Name and Prompt

If you are accessing a stack member through the active switch, you must use the **session** *stack-member-number* privileged EXEC command. The stack member number range is . When you use this command, the stack member number is appended to the system prompt. For example, Switch-2# is the prompt in privileged EXEC mode for stack member 2, and the system prompt for the switch stack is Switch.

Default System Name and Prompt Configuration

The default switch system name and prompt is *Switch*.

DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your device, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, for example, the File Transfer Protocol (FTP) system is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

Default DNS Settings

Table 1: Default DNS Settings

| Feature | Default Setting |
|-------------------------|--|
| DNS enable state | Enabled. |
| DNS default domain name | None configured. |
| DNS servers | No name server addresses are configured. |

Login Banners

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner is displayed on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner is also displayed on all connected terminals. It appears after the MOTD banner and before the login prompts.



Note For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*.

Default Banner Configuration

The MOTD and login banners are not configured.

MAC Address Table

The MAC address table contains address information that the device uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address—A source MAC address that the device learns and then ages when it is not in use.
- Static address—A manually entered unicast address that does not age and that is not lost when the device resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).



Note For complete syntax and usage information for the commands used in this section, see the command reference for this release.

MAC Address Table Creation

With multiple MAC addresses supported on all ports, you can connect any port on the device to other network devices. The device provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As devices are added or removed from the network, the device updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the device maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The device sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the device forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The device always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Unicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 1 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

MAC Addresses and Device Stacks

The MAC address tables on all stack members are synchronized. At any given time, each stack member has the same copy of the address tables for each VLAN. When an address ages out, the address is removed from

the address tables on all stack members. When a device joins a switch stack, that device receives the addresses for each VLAN learned on the other stack members. When a stack member leaves the switch stack, the remaining stack members age out or remove all addresses learned by the former stack member.

Default MAC Address Table Settings

The following table shows the default settings for the MAC address table.

Table 2: Default Settings for the MAC Address

| Feature | Default Setting |
|-------------------|-----------------------|
| Aging time | 300 seconds |
| Dynamic addresses | Automatically learned |
| Static addresses | None configured |

ARP Table Management

To communicate with a device (over Ethernet, for example), the software first must learn the 48-bit MAC address or the local data link address of that device. The process of learning the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Using an IP address, ARP finds the associated MAC address. When a MAC address is found, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

ARP entries added manually to the table do not age and must be manually removed.

For CLI procedures, see the Cisco IOS Release 12.4 documentation on *Cisco.com*.

How to Administer the Device

Configuring the Time and Date Manually

System time remains accurate through restarts and reboot, however, you can manually configure the time and date after the system is restarted.

We recommend that you use manual configuration only when necessary. If you have an outside source to which the device can synchronize, you do not need to manually set the system clock.



Note You must reconfigure this setting if you have manually configured the system clock before the device fails and a different stack member assumes the role of the device.

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Follow these steps to set the system clock:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | Use one of the following: <ul style="list-style-type: none"> • clock set <i>hh:mm:ss day month year</i> • clock set <i>hh:mm:ss month day year</i> Example: <pre>Device# clock set 13:32:00 23 March 2013</pre> | Manually set the system clock using one of these formats: <ul style="list-style-type: none"> • <i>hh:mm:ss</i>—Specifies the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. • <i>day</i>—Specifies the day by date in the month. • <i>month</i>—Specifies the month by name. • <i>year</i>—Specifies the year (no abbreviation). |

Configuring the Time Zone

Follow these steps to manually configure the time zone:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 3 | clock timezone <i>zone hours-offset</i> <i>[minutes-offset]</i> Example: <pre>Device(config)# clock timezone AST -3 30</pre> | <p>Sets the time zone.</p> <p>Internal time is kept in Coordinated Universal Time (UTC), so this command is used only for display purposes and when the time is manually set.</p> <ul style="list-style-type: none"> • <i>zone</i>—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC. • <i>hours-offset</i>—Enters the hours offset from UTC. • (Optional) <i>minutes-offset</i>—Enters the minutes offset from UTC. This is available where the local time zone is a percentage of an hour different from UTC. |
| Step 4 | end Example: <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 5 | show running-config Example: <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 6 | copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Configuring Summer Time (Daylight Saving Time)

To configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year, perform this task:

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------------|---|
| Step 1 | enable Example: | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Device> enable | |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | clock summer-time zone date date month year hh:mm date month year hh:mm [offset] Example: Device(config)# clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00 | Configures summer time to start and end on specified days every year. |
| Step 4 | clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]] Example: Device(config)# clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00 | <p>Configures summer time to start and end on the specified days every year. All times are relative to the local time zone. The start time is relative to standard time.</p> <p>The end time is relative to summer time. Summer time is disabled by default. If you specify clock summer-time zone recurring without parameters, the summer time rules default to the United States rules.</p> <p>If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.</p> <ul style="list-style-type: none"> • <i>zone</i>—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) <i>week</i>— Specifies the week of the month (1 to 4, first, or last). • (Optional) <i>day</i>—Specifies the day of the week (Sunday, Monday...). • (Optional) <i>month</i>—Specifies the month (January, February...). • (Optional) <i>hh:mm</i>—Specifies the time (24-hour format) in hours and minutes. • (Optional) <i>offset</i>—Specifies the number of minutes to add during summer time. The default is 60. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 5 | end Example: Device (config) # end | Returns to privileged EXEC mode. |
| Step 6 | show running-config Example: Device # show running-config | Verifies your entries. |
| Step 7 | copy running-config startup-config Example: Device # copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring NTP

The device does not have a hardware-supported clock and cannot function as an NTP primary clock to which peers synchronize themselves when an external NTP source is not available. The device also has no hardware support for a calendar. As a result, the **ntp update-calendar** and the **ntp master** commands in global configuration mode are not available.

These following sections provide configuration information on NTP:

Default NTP Configuration

shows the default NTP configuration.

Table 3: Default NTP Configuration

| Feature | Default Setting |
|---------------------------------|---|
| NTP authentication | Disabled. No authentication key is specified. |
| NTP peer or server associations | None configured. |
| NTP broadcast service | Disabled; no interface sends or receives NTP broadcast packets. |
| NTP access restrictions | No access control is specified. |
| NTP packet source IP address | The source address is set by the outgoing interface. |

NTP is enabled on all interfaces by default. All interfaces receive NTP packets.

Configuring NTP Authentication

To configure NTP authentication, perform this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | [no] ntp authenticate Example: <pre>Device(config)# ntp authenticate</pre> | Enables NTP authentication. Use the no form of this command to disable NTP authentication |
| Step 4 | [no] ntp authentication-key <i>number</i> {md5 cmac-aes-128 hmac-sha1 hmac-sha2-256} <i>value</i> Example: <pre>Device(config)# ntp authentication-key 42 md5 aNiceKey</pre> | Defines the authentication keys. <ul style="list-style-type: none"> Each key has a key number, a type, and a value. Keys can be one of the following types: <ul style="list-style-type: none"> md5: Authentication using the MD5 algorithm. cmac-aes-128: Authentication using Cipher-based message authentication codes (CMAC) with the AES-128 algorithm. The digest length is 128 bits and the key length is 16 or 32 bytes. hmac-sha1: Authentication using Hash-based Message Authentication Code (HMAC) using the SHA1 hash function. The digest length is 128 bits and the key length is 1 to 32 bytes. hmac-sha2-256: Authentication using HMAC using the SHA2 hash function. The digest length is 256 bits and the key length is 1 to 32 bytes |

| | Command or Action | Purpose |
|---------------|---|--|
| | | Use the no form of this command to remove authentication key. |
| Step 5 | <p>[no] ntp trusted-key <i>key-number</i></p> <p>Example:</p> <pre>Device(config)# ntp trusted-key 42</pre> | <p>Defines trusted authentication keys that a peer NTP device must provide in its NTP packets for this device to synchronize to it.</p> <p>Use the no form of this command to disable trusted authentication.</p> |
| Step 6 | <p>[no] ntp server <i>ip-address</i> key <i>key-id</i> [prefer]</p> <p>Example:</p> <pre>Device(config)# ntp server 172.16.22.44 key 42</pre> | <p>Allows the software clock to be synchronized by an NTP time server.</p> <ul style="list-style-type: none"> • <i>ip-address</i>: The IP address of the time server providing the clock synchronization. • <i>key-id</i>: Authentication key defined with the ntp authentication-key command. • prefer: Sets this peer as the preferred one that provides synchronization. This keyword reduces clock hop among peers. <p>Use the no form of this command to remove a server association.</p> |
| Step 7 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |

Configuring Poll-Based NTP Associations

To configure poll-based NTP associations, perform this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Device> enable</pre> | <p>Enables privileged EXEC mode.</p> <p>Enter your password if prompted.</p> |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre> | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | <p>[no] ntp peer <i>ip-address</i> [version <i>number</i>] [key <i>key-id</i>] [source <i>interface</i>] [prefer]</p> <p>Example:</p> <pre>Device(config)# ntp peer 172.16.22.44 version 2</pre> | <p>Configures the device system clock to synchronize a peer or to be synchronized by a peer (peer association).</p> <ul style="list-style-type: none"> • <i>ip-address</i>: The IP address of the peer providing or being provided, the clock synchronization. • <i>number</i>: NTP version number. The range is 1 to 3. By default, version 3 is selected. • <i>key-id</i>: Authentication key defined with the ntp authentication-key command. • <i>interface</i>: The interface from which to pick the IP source address. By default, the source IP address is taken from the outgoing interface. • prefer: Sets this peer as the preferred one that provides synchronization. This keyword reduces switching back and forth between peers. <p>Use the no form of this command to remove a peer association.</p> |
| Step 4 | <p>[no] ntp server <i>ip-address</i> [version <i>number</i>] [key <i>key-id</i>] [source <i>interface</i>] [prefer]</p> <p>Example:</p> <pre>Device(config)# ntp server 172.16.22.44 version 2</pre> | <p>Configures the device's system clock to be synchronized by a time server (server association).</p> <ul style="list-style-type: none"> • <i>ip-address</i>: The IP address of the time server providing the clock synchronization. • <i>number</i>: NTP version number. The range is 1 to 3. By default, version 3 is selected. • <i>key-id</i>: Authentication key defined with the ntp authentication-key command. • <i>interface</i>: The interface from which to pick the IP source address. By default, the source IP address is taken from the outgoing interface. • prefer: Sets this peer as the preferred one that provides synchronization. This keyword reduces clock hop among peers. <p>Use the no form of this command to remove a server association.</p> |

| | Command or Action | Purpose |
|---------------|---|----------------------------------|
| Step 5 | end Example: Device(config)# end | Returns to privileged EXEC mode. |

Configuring Broadcast-Based NTP Associations

To configure broadcast-based NTP associations, perform this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet1/0/1 | Configures an interface and enters interface configuration mode. |
| Step 4 | [no] ntp broadcast [version <i>number</i>] [key <i>key-id</i>] [<i>destination-address</i>] Example: Device(config-if)# ntp broadcast version 2 | Enables the interface to send NTP broadcast packets to a peer. <ul style="list-style-type: none"> • <i>number</i>: NTP version number. The range is 1 to 3. By default, version 3 is used. • <i>key-id</i>: Authentication key. • <i>destination-address</i>: IP address of the peer that is synchronizing its clock to this switch. Use the no form of this command to disable the interface from sending NTP broadcast packets. |
| Step 5 | [no] ntp broadcast client Example: | Enables the interface to receive NTP broadcast packets. |

| | Command or Action | Purpose |
|---------------|---|---|
| | <code>Device(config-if) # ntp broadcast client</code> | Use the no form of this command to disable the interface from receiving NTP broadcast packets. |
| Step 6 | exit Example: <code>Device(config-if) # exit</code> | Returns to privileged EXEC mode. |
| Step 7 | <code>[no] ntp broadcastdelay <i>microseconds</i></code> Example: <code>Device(config) # ntp broadcastdelay 100</code> | (Optional) Change the estimated round-trip delay between the device and the NTP broadcast server The default is 3000 microseconds. The range is from 1 to 999999. Use the no form of this command to disable the interface from receiving NTP broadcast packets. |
| Step 8 | end Example: <code>Device(config) # end</code> | Returns to privileged EXEC mode. |

Configuring NTP Access Restrictions

You can control NTP access on two levels as described in these sections:

Creating an Access Group and Assigning a Basic IP Access List

To create an access group and assign a basic IP access list, perform this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <code>Device> enable</code> | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: <code>Device# configure terminal</code> | Enters global configuration mode. |
| Step 3 | <code>[no] ntp access-group {query-only serve-only serve peer} <i>access-list-number</i></code> | Create an access group, and apply a basic IP access list.. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Example: Device(config)# ntp access-group peer 99 | <ul style="list-style-type: none"> • query-only: NTP control queries. • serve-only: Time requests. • serve: Allows time requests and NTP control queries, but does not allow the device to synchronize to the remote device. • peer: Allows time requests and NTP control queries and allows the device to synchronize to the remote device. • access-list-number: IP access list number. The range is from 1 to 99. <p>Use the no form of this command to remove access control to the switch NTP services.</p> |
| Step 4 | access-list access-list-number permit source [source-wildcard] Example: Device(config)# access-list 99 permit 172.20.130.5 | <p>Create the access list.</p> <ul style="list-style-type: none"> • access-list-number: IP access list number. The range is from 1 to 99. • permit: Permits access if the conditions are matched. • source: IP address of the device that is permitted access to the device. • source-wildcard: Wildcard bits to be applied to the source. <p>Note When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.</p> <p>Use the no form of this command to remove authentication key.</p> |
| Step 5 | end Example: Device(config)# end | <p>Returns to privileged EXEC mode.</p> |

Disabling NTP Services on a Specific Interface

To disable NTP packets from being received on an interface, perform this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet1/0/1</pre> | Enters global configuration mode. |
| Step 4 | [no] ntp disable Example: <pre>Device(config-if)# ntp disable</pre> | Disables NTP packets from being received on the interface. Use the no form of this command to re-enable receipt of NTP packets on an interface. |
| Step 5 | end Example: <pre>Device(config-if)# end</pre> | Returns to privileged EXEC mode. |

Configuring a System Name

Follow these steps to manually configure a system name:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | hostname <i>name</i> Example: <pre>Device(config)# hostname remote-users</pre> | <p>Configures a system name. When you set the system name, it is also used as the system prompt.</p> <p>The default setting is Switch.</p> <p>The name must follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.</p> |
| Step 4 | end Example: <pre>remote-users(config)#end remote-users#</pre> | Returns to privileged EXEC mode. |
| Step 5 | show running-config Example: <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 6 | copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Setting Up DNS

If you use the device IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain name** command in global configuration mode. If there is a period (.) in the hostname, the Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

Follow these steps to set up your switch to use the DNS:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | ip domain name <i>name</i> Example: <pre>Device(config)# ip domain name Cisco.com</pre> | Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the device configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information). |
| Step 4 | ip name-server <i>server-address1</i> [<i>server-address2</i> ... <i>server-address6</i>] Example: <pre>Device(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300</pre> | Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried. |
| Step 5 | ip domain lookup [<i>nsap</i> <i>source-interface interface</i>] Example: <pre>Device(config)# ip domain-lookup</pre> | (Optional) Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS). |
| Step 6 | end Example: | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Device(config)# end | |
| Step 7 | show running-config Example: Device# show running-config | Verifies your entries. |
| Step 8 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs in to the device.

Follow these steps to configure a MOTD login banner:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | banner motd c message c Example: Device(config)# banner motd # This is a secure site. Only authorized users are allowed. For access, contact technical support. # | Specifies the message of the day. <i>c</i> —Enters the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. |

| | Command or Action | Purpose |
|---------------|---|---|
| | | <i>message</i> —Enters a banner message up to 255 characters. You cannot use the delimiting character in the message. |
| Step 4 | end Example: Device(config) # end | Returns to privileged EXEC mode. |
| Step 5 | show running-config Example: Device# show running-config | Verifies your entries. |
| Step 6 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring a Login Banner

You can configure a login banner to be displayed on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Follow these steps to configure a login banner:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | banner login c message c Example: | Specifies the login message. <i>c</i> — Enters the delimiting character of your choice, for example, a pound sign (#), and press |

| | Command or Action | Purpose |
|---------------|---|--|
| | <pre>Device(config)# banner login \$ Access for authorized users only. Please enter your username and password. \$</pre> | <p>the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.</p> <p><i>message</i>—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.</p> |
| Step 4 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 5 | <p>show running-config</p> <p>Example:</p> <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 6 | <p>copy running-config startup-config</p> <p>Example:</p> <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Managing the MAC Address Table

Changing the Address Aging Time

Follow these steps to configure the dynamic address table aging time:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Device> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre> | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | mac address-table aging-time [<i>0</i> <i>10-1000000</i>] [routed-mac vlan <i>vlan-id</i>] Example: <pre>Device(config)# mac address-table aging-time 500 vlan 2</pre> | Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table. <i>vlan-id</i> —Valid IDs are 1 to 4094. |
| Step 4 | end Example: <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 5 | show running-config Example: <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 6 | copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Configuring MAC Address Change Notification Traps

Follow these steps to configure the switch to send MAC address change notification traps to an NMS host:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | <p>snmp-server host <i>host-addr</i> <i>community-string</i> <i>notification-type</i> { informs traps } { version { 1 2c 3 } } { vrf <i>vrf instance name</i> }</p> <p>Example:</p> <pre>Device(config)# snmp-server host 172.20.10.10 traps private mac-notification</pre> | <p>Specifies the recipient of the trap message.</p> <ul style="list-style-type: none"> • <i>host-addr</i>—Specifies the name or address of the NMS. • traps (the default)—Sends SNMP traps to the host. • informs—Sends SNMP informs to the host. • version—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • <i>community-string</i>—Specifies the string to send with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define this string by using the snmp-server community command before using the snmp-server host command. • <i>notification-type</i>—Uses the mac-notification keyword. • vrf <i>vrf instance name</i>—Specifies the VPN routing/forwarding instance for this host. |
| Step 4 | <p>snmp-server enable traps mac-notification change</p> <p>Example:</p> <pre>Device(config)# snmp-server enable traps mac-notification change</pre> | Enables the device to send MAC address change notification traps to the NMS. |
| Step 5 | <p>mac address-table notification change</p> <p>Example:</p> <pre>Device(config)# mac address-table notification change</pre> | Enables the MAC address change notification feature. |
| Step 6 | <p>mac address-table notification change [<i>interval value</i>] [<i>history-size value</i>]</p> <p>Example:</p> <pre>Device(config)# mac address-table notification change interval 123 Device(config)# mac address-table</pre> | <p>Enters the trap interval time and the history table size.</p> <ul style="list-style-type: none"> • (Optional) interval value—Specifies the notification trap interval in seconds between each set of traps that are generated to the NMS. The range is 0 to |

| | Command or Action | Purpose |
|----------------|--|--|
| | <code>notification change history-size 100</code> | 2147483647 seconds; the default is 1 second. • (Optional) history-size value —Specifies the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1. |
| Step 7 | interface <i>interface-id</i> Example: Device(config)# interface fortygigabitethernet1/0/2 | Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap. |
| Step 8 | snmp trap mac-notification change { added removed } Example: Device(config-if)# snmp trap mac-notification change added | Enables the MAC address change notification trap on the interface. • Enables the trap when a MAC address is added on this interface. • Enables the trap when a MAC address is removed from this interface. |
| Step 9 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 10 | show running-config Example: Device# show running-config | Verifies your entries. |
| Step 11 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring MAC Address Move Notification Traps

When you configure MAC-move notification, an SNMP notification is generated and sent to the network management system whenever a MAC address moves from one port to another within the same VLAN.

Follow these steps to configure the device to send MAC address-move notification traps to an NMS host:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | snmp-server host <i>host-addr</i> {traps informs} {version {1 2c 3}} <i>community-string</i> <i>notification-type</i> Example: <pre>Device(config)# snmp-server host 172.20.10.10 traps private mac-notification</pre> | Specifies the recipient of the trap message. <ul style="list-style-type: none"> • <i>host-addr</i>—Specifies the name or address of the NMS. • traps (the default)—Sends SNMP traps to the host. • informs—Sends SNMP informs to the host. • version—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • <i>community-string</i>—Specifies the string to send with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define this string by using the snmp-server community command before using the snmp-server host command. • <i>notification-type</i>—Uses the mac-notification keyword. |
| Step 4 | snmp-server enable traps mac-notification move Example: <pre>Device(config)# snmp-server enable traps mac-notification move</pre> | Enables the device to send MAC address move notification traps to the NMS. |
| Step 5 | mac address-table notification mac-move Example: | Enables the MAC address move notification feature. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Device(config)# mac address-table notification mac-move | |
| Step 6 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 7 | show running-config Example: Device# show running-config | Verifies your entries. |
| Step 8 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

What to do next

To disable MAC address-move notification traps, use the **no snmp-server enable traps mac-notification move** global configuration command. To disable the MAC address-move notification feature, use the **no mac address-table notification mac-move** global configuration command.

You can verify your settings by entering the **show mac address-table notification mac-move** privileged EXEC commands.

Configuring MAC Threshold Notification Traps

When you configure MAC threshold notification, an SNMP notification is generated and sent to the network management system when a MAC address table threshold limit is reached or exceeded.

Follow these steps to configure the switch to send MAC address table threshold notification traps to an NMS host:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | snmp-server host <i>host-addr</i> {traps informs} {version {1 2c 3}} <i>community-string</i> <i>notification-type</i> Example: <pre>Device(config)# snmp-server host 172.20.10.10 traps private mac-notification</pre> | Specifies the recipient of the trap message. <ul style="list-style-type: none"> • <i>host-addr</i>—Specifies the name or address of the NMS. • traps (the default)—Sends SNMP traps to the host. • informs—Sends SNMP informs to the host. • version—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • <i>community-string</i>—Specifies the string to send with the notification operation. You can set this string by using the snmp-server host command, but we recommend that you define this string by using the snmp-server community command before using the snmp-server host command. • <i>notification-type</i>—Uses the mac-notification keyword. |
| Step 4 | snmp-server enable traps mac-notification threshold Example: <pre>Device(config)# snmp-server enable traps mac-notification threshold</pre> | Enables MAC threshold notification traps to the NMS. |
| Step 5 | mac address-table notification threshold Example: <pre>Device(config)# mac address-table notification threshold</pre> | Enables the MAC address threshold notification feature. |
| Step 6 | mac address-table notification threshold [limit <i>percentage</i>] [interval <i>time</i>] | Enters the threshold value for the MAC address threshold usage monitoring. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Example: <pre>Device(config)# mac address-table notification threshold interval 123 Device(config)# mac address-table notification threshold limit 78</pre> | <ul style="list-style-type: none"> • (Optional) limit percentage—Specifies the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent. • (Optional) interval time—Specifies the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds. |
| Step 7 | end Example: <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 8 | show running-config Example: <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 9 | copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Disabling MAC Address Learning on VLAN

You can control MAC address learning on a VLAN to manage the available MAC address table space by controlling which VLANs can learn MAC addresses. Before you disable MAC address learning, be sure that you are familiar with the network topology. Disabling MAC address learning on VLAN could cause flooding in the network.

Beginning in privileged EXEC mode, follow these steps to disable MAC address learning on a VLAN:

Before you begin

Follow these guidelines when disabling MAC address learning on a VLAN:

- Use caution before disabling MAC address learning on a VLAN with a configured switch virtual interface (SVI). The switch then floods all IP packets in the Layer 2 domain.
- You can disable MAC address learning on a single VLAN ID from 2 - 4093 (for example, no mac address-table learning vlan 223) or a range of VLAN IDs, separated by a hyphen or comma (for example, no mac address-table learning vlan 1-10, 15).

- It is recommended that you disable MAC address learning only in VLANs with two ports. If you disable MAC address learning on a VLAN with more than two ports, every packet entering the switch is flooded in that VLAN domain.
- If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on that port.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters the global configuration mode. |
| Step 2 | no mac-address-table learning vlan [vlan-id [,vlan-id -vlan-id,] Example: Device(config)# no mac-address-table learning {vlan vlan-id [,vlan-id -vlan-id]} | Disable MAC address learning on a specified VLAN or VLANs. You can specify a single VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs range from 2 - 4093. It cannot be an internal VLAN. |
| Step 3 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 4 | show mac-address-table learning vlan [vlan-id] Example: Device# show mac-address-table learning [vlan vlan-id] | Verify the configuration. You can display the MAC address learning status of all VLANs or a specified VLAN by entering the show mac-address-table learning [vlan vlan-id] privileged EXEC command. |
| Step 5 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Save your entries in the configuration file. |
| Step 6 | default mac address-table learning Example: Device# default mac address-table | (Optional) Reenable MAC address learning on VLAN in a global configuration mode. |

Adding and Removing Static Address Entries

Follow these steps to add a static address:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | mac address-table static <i>mac-addr</i> vlan <i>vlan-id</i> interface <i>interface-id</i> Example: <pre>Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface fortygigabitethernet 1/0/1</pre> | Adds a static address to the MAC address table. <ul style="list-style-type: none"> • <i>mac-addr</i>—Specifies the destination MAC unicast address to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface. • <i>vlan-id</i>—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. • <i>interface-id</i>—Specifies the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels. For static multicast addresses, you can enter multiple interface IDs. For static unicast addresses, you can enter only one interface at a time, but you can enter the command multiple times with the same MAC address and VLAN ID. |
| Step 4 | show running-config Example: <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 5 | copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Configuring Unicast MAC Address Filtering

Follow these steps to configure the device to drop a source or destination unicast static address:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | mac address-table static <i>mac-addr</i> vlan <i>vlan-id</i> drop Example: Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop | Enables unicast MAC address filtering and configure the device to drop a packet with the specified source or destination unicast static address. <ul style="list-style-type: none">• <i>mac-addr</i>—Specifies a source or destination unicast MAC address (48-bit). Packets with this MAC address are dropped.• <i>vlan-id</i>—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. |
| Step 4 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 5 | show running-config Example: Device# show running-config | Verifies your entries. |
| Step 6 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Monitoring and Maintaining Administration of the Device

| Command | Purpose |
|--|------------------------------|
| clear mac address-table dynamic | Removes all dynamic entries. |

| Command | Purpose |
|---|--|
| clear mac address-table dynamic address <i>mac-address</i> | Removes a specific MAC address. |
| clear mac address-table dynamic interface <i>interface-id</i> | Removes all addresses on the specified physical port or port channel. |
| clear mac address-table dynamic vlan <i>vlan-id</i> | Removes all addresses on a specified VLAN. |
| show clock [<i>detail</i>] | Displays the time and date configuration. |
| show ip igmp snooping groups | Displays the Layer 2 multicast entries for all VLANs or the specified VLAN. |
| show mac address-table address <i>mac-address</i> | Displays MAC address table information for the specified MAC address. |
| show mac address-table aging-time | Displays the aging time in all VLANs or the specified VLAN. |
| show mac address-table count | Displays the number of addresses present in all VLANs or the specified VLAN. |
| show mac address-table dynamic | Displays only dynamic MAC address table entries. |
| show mac address-table interface <i>interface-name</i> | Displays the MAC address table information for the specified interface. |
| show mac address-table move update | Displays the MAC address table move update information. |
| show mac address-table multicast | Displays a list of multicast MAC addresses. |
| show mac address-table notification { <i>change</i> <i>mac-move</i> <i>threshold</i> } | Displays the MAC notification parameters and history table. |
| show mac address-table secure | Displays the secure MAC addresses. |
| show mac address-table static | Displays only static MAC address table entries. |
| show mac address-table vlan <i>vlan-id</i> | Displays the MAC address table information for the specified VLAN. |

Configuration Examples for Device Administration

Example: Setting the System Clock

This example shows how to manually set the system clock:

```
Device# clock set 13:32:00 23 July 2013
```

Examples: Configuring Summer Time

This example (for daylight savings time) shows how to specify that summer time starts on March 10 at 02:00 and ends on November 3 at 02:00:

```
Device(config)# clock summer-time PDT recurring PST date  
10 March 2013 2:00 3 November 2013 2:00
```

This example shows how to set summer time start and end dates:

```
Device(config)#clock summer-time PST date  
20 March 2013 2:00 20 November 2013 2:00
```

Example: Configuring a MOTD Banner

This example shows how to configure a MOTD banner by using the pound sign (#) symbol as the beginning and ending delimiter:

```
Device(config)# banner motd #  
  
This is a secure site. Only authorized users are allowed.  
For access, contact technical support.  
  
#  
  
Device(config)#
```

This example shows the banner that appears from the previous configuration:

```
Unix> telnet 192.0.2.15  
  
Trying 192.0.2.15...  
  
Connected to 192.0.2.15.  
  
Escape character is '^]'.  
  
This is a secure site. Only authorized users are allowed.  
  
For access, contact technical support.  
  
User Access Verification  
  
Password:
```

Example: Configuring a Login Banner

This example shows how to configure a login banner by using the dollar sign (\$) symbol as the beginning and ending delimiter:

```
Device(config)# banner login $
```

Access for authorized users only. Please enter your username and password.

\$

Device(config)#

Example: Configuring MAC Address Change Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable MAC address notification traps to the NMS, enable the MAC address-change notification feature, set the interval time to 123 seconds, set the history-size to 100 entries, and enable traps whenever a MAC address is added on the specified port:

```
Device(config)# snmp-server host 172.20.10.10 traps private mac-notification
Device(config)# snmp-server enable traps mac-notification change
Device(config)# mac address-table notification change
Device(config)# mac address-table notification change interval 123
Device(config)# mac address-table notification change history-size 100
Device(config)# interface fortygigabitethernet1/0/1
Device(config-if)# snmp trap mac-notification change added
```

Example: Configuring MAC Threshold Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable the MAC address threshold notification feature, set the interval time to 123 seconds, and set the limit to 78 per cent:

```
Device(config)# snmp-server host 172.20.10.10 traps private mac-notification
Device(config)# snmp-server enable traps mac-notification threshold
Device(config)# mac address-table notification threshold
Device(config)# mac address-table notification threshold interval 123
Device(config)# mac address-table notification threshold limit 78
```

Example: Adding the Static Address to the MAC Address Table

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination address, the packet is forwarded to the specified port:



Note You cannot associate the same static MAC address to multiple interfaces. If the command is executed again with a different interface, the static MAC address is overwritten on the new interface.

```
Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
fortygigabitethernet1/0/1
```

Example: Configuring Unicast MAC Address Filtering

This example shows how to enable unicast MAC address filtering and how to configure drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

Additional References for Device Administration

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

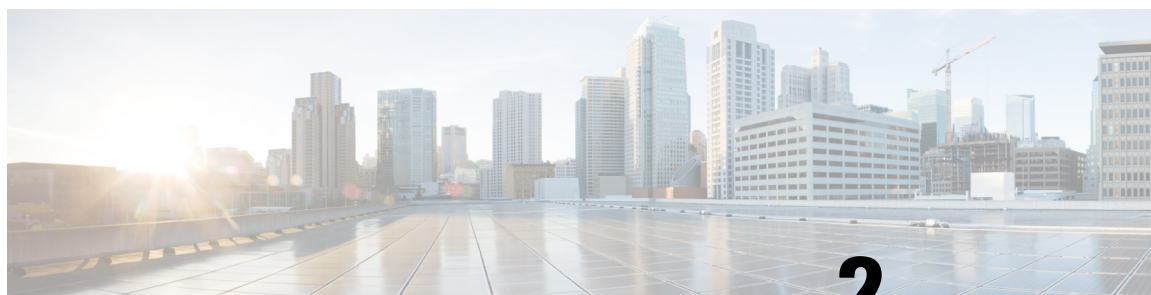
Feature History for Device Administration

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|-----------------------|--|
| Cisco IOS XE Gibraltar 16.11.1 | Device Administration | The device administration allows to configure the system time and date, system name, a login banner, and set up the DNS. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 2

Boot Integrity Visibility

- [Information About Boot Integrity Visibility, on page 41](#)
- [Verifying the Software Image and Hardware, on page 41](#)
- [Verifying Platform Identity and Software Integrity, on page 42](#)
- [Additional References for Boot Integrity Visibility, on page 45](#)
- [Feature History for Boot Integrity Visibility, on page 45](#)

Information About Boot Integrity Visibility

Boot Integrity Visibility allows Cisco's platform identity and software integrity information to be visible and actionable. Platform identity provides the platform's manufacturing installed identity. Software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted trusted code.

During the boot process, the software creates a checksum record of each stage of the bootloader activities.

You can retrieve this record and compare it with a Cisco-certified record to verify if your software image is genuine. If the checksum values do not match, you may be running a software image that is either not certified by Cisco or has been altered by an unauthorized party.

Verifying the Software Image and Hardware

This task describes how to retrieve the checksum record that was created during a switch bootup. Enter the following commands in privileged EXEC mode.



Note On executing the following commands, you might see the message **% Please Try After Few Seconds** displayed on the CLI. This does not indicate a CLI failure, but indicates setting up of underlying infrastructure required to get the required output. We recommend waiting for a few minutes and then try the command again.

The messages **% Error retrieving SUDI certificate** and **% Error retrieving integrity data** signify a real CLI failure.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | show platform sudi certificate [sign [nonce]] Example: Device# show platform sudi certificate sign nonce 123 | Displays checksum record for the specific SUDI. <ul style="list-style-type: none"> • (Optional) sign - Show signature • (Optional) nonce - Enter a nonce value |
| Step 2 | show platform integrity [sign [nonce]] Example: Device# show platform integrity sign nonce 123 | Displays checksum record for boot stages. <ul style="list-style-type: none"> • (Optional) sign - Show signature • (Optional) nonce - Enter a nonce value |

Verifying Platform Identity and Software Integrity

Verifying Platform Identity

The following example displays the Secure Unique Device Identity (SUDI) chain in PEM format. Encoded into the SUDI is the Product ID and Serial Number of each individual device such that the device can be uniquely identified on a network of thousands of devices. The first certificate is the Cisco Root CA 2048 and the second is the Cisco subordinate CA (ACT2 SUDI CA). Both certificates can be verified to match those published on <https://www.cisco.com/security/pki/>. The third is the SUDI certificate.



Important All the CLI outputs provided here are intended only for reference. The output differs based the configuration of the device.

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaxNjbyBSb290IENB
IDIwNDgwHhcnMDQwNTEOMjAxNzEyWhcNMjkwNTEOMjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaxNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEayv8CrLqUccda8bnuoqrpu0hWISewdovyD0My5jOamaHBKen8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJsZr2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUL4FlpyXOWWqCZe+36ufijXWlbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmrxrU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
olEwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXH0jgxkhLtv5M0hmBvrbW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyC8lWhJDtSd9i7rp77rMKSSh0T8lasz
Bvt9YaretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
```



```

kxpUnwVwwEpxYB5DC2Ae/qP0gRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAYsGawIBAgIKYQLufQAAAAAADBANBgqhkiG9w0BAQUFADA1MRYwFAYD
VQKKEw1DaXNjbyBTeXN0ZWlzMRSwGQYDVQQDEwJDaXNjbyBSb290IENBIDwNDGw
HhcNMTEwNjMwMTC1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDAxNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIEENBMB4XDTE0MjAyNTQyWjAnMQ4wDAYDV
MIIBCgKCAQEAm5l3THixA9tN/hS5qr/6UZRpdd+9aE2JbFkNjht6gfHKd477Aks
5XAtUs5oxDYVt/zEbs1Zq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMgmgm+
xghHiooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj130VeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVhM6aAgkWrSugiWbF2nsqvjBDBgNVHR8EPDA6MDIqNQA0hJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW50cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVROgBFUwUzBRBgorBgEEAQKv
AQwAMEMwQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3VyYXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIHvcNAQEFBQADggEBAGhlqclr9tx4hzWgDERm37lyeuEmqCIfi9b9+GbMSJbi
ZHc/CcC10lJu0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51lklT8NbcKY
/4dw1ex+7amATUQ04QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhoWryAK4dVo8hCjkjEkzu3ufBTJapnv89g90E+H3VKM4L+/KdkUO+52djFKN
hy147d7cZR4DY4LIuFM2PlAs8YyjoNpK/urSRI14WdIlplRlnH7KND15618yFVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIEAwQD7zANBgqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbyBVMBMGA1UEAxMMQUNUMiBTVURJIEENBMB4XDTE0MjAyNTQyWjAnMQ4w
MDUxNDIwMjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0
MzZMMFE5MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0MjU0
MRQwEgYDVQQDEwVDAxNjbyBTeXN0ZWlzMRSwGQYDVQQDEwJDaXNjbyBSb290I
AQoCggEBANsh0jcvghlpdOjP9KnffDnDc/zEHDzbCTWpJi2FZcsaSE5jvq6CUqc4
MYpNAZU2Jym7NSD8iQbMXwnCtoL64QtXQeFhRYmc4d5o933M7GwpEH0I7HUSbo/
Fxy7J7BmGPPgAkY7rKsYENiNK2hiR7Q207X2BidOKknEuofWdJMNyMaZgLYLOHbJ
5oXaORxhUy3VRaxN16qI7kYxuugg2LcAbZ539sRXe8JtHyK811URNsGMIQ0S17pS
idGmrJJ0pEHA0EUVTZqEny3z+NW9uxLVSzu6+hEJYlqfI+Yef0DbVZlY1cy5r/jF
yNdGuGKvd5agvgCly8aYMZa3P+D5S8sCAwEAANvMG0wDgYDVR0PAAQhBAQDAgXg
MAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEEAQKvAgOgNRMzQ2hpcE1E
PVUxUk5TVE13TVRjd05qSTFBQwFwZndBQwFwZndBQwFwZndBQwFwZndBQwFwZndB
CSqGSIB3DQEBcWUAA4IBAQCpHo/CUyk5Hs/asIcYW0ep8KocSknNh8qamyd4oWD
e/MGJW9Bs5f0IEbILWpdytCCS2lSyJbxz2HvVdZdxQdxjDwUNiWuu3dWMXN/i67
yucGM+1A1AAG5dT6lNgWYHh+YzsZm9eoq1+4NM+JuMXWsnzAK8rSy+dSpBxqFsBq
E00lPsaK7y2h8gs+XrV9x+D48OZQkTRXpxhJfiWvs+EbdgsAM/vBxTAoTJFPvMXWN
Cmcj9X52X13i4MdOUXocZLO2kh6JSgOYGkFeZifJ0iDvMfAf0cJ6+cEF6bSxAqBL
veel+8LmeiE/209h6qGHPPDacCaXA2oJCDHveAt8iPTG
-----END CERTIFICATE-----

```

Signature version: 1

Signature:

-----BEGIN CERTIFICATE-----

The optional RSA 2048 signature is across the three certificates, the signature version and the user-provided nonce.

```

RSA PKCS#1v1.5 Sign {<Nonce (UINT64)> || <Signature Version (UINT32)> || <Cisco Root CA
2048 cert (DER)> ||
<Cisco subordinate CA (DER)> || <SUDI certificate (DER)> }

```

```
[linux-host:~]openssl x509 -in sudi_id.pem -subject -noout
subject= /serialNumber=PID:C9600-SUP-1 SN:CAT2239L06B/CN=C9600-SUP-1-70b3171ea00
```

The following example displays the checksum record for the boot stages. The hash measurements are displayed for each of the three stages of software successively booted. These hashes can be compared against Cisco-provided reference values. An option to sign the output gives a verifier the ability to ensure the output is genuine and is not altered. A nonce can be provided to protect against replay attacks.



The following is a sample output of the **show platform integrity sign nonce 123** command. This output includes measurements of each installed package file.

```
Device#show platform integrity sign nonce 123
Platform: C9606R
Boot 0 Version: MA0083R06.1810032017
Boot 0 Hash: 535AD9DC3D2A26C030D7DF6D4342FD52AB4DC6B1395DB18E7CA33F678A874B9E
Boot Loader Version: System Bootstrap, Version 16.11.1r[FC2], RELEASE SOFTWARE (P)
Boot Loader Hash:
C66199E7F6324245FAA0AFBCB5C17432FA13AF82FB1596D5CFEE1FF1080F2107FEFFB48AC5DF88B41894AEC7AF87052717012BFF6185D34F579D9BF1784597
OS Version: BLD_V1611_THROTTLE_LATEST_20190203_030036
OS Hashes:
cat9k_iosxe.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.bin:
3F4A10066FAAA30417D7D17395ADD71FFCCED6BA122ABA439D12A03C78EF38E8D281DEFAD27CC15AA7FE63AA1344FEABF68AC6A09D408F89277F35DB8EE55
cat9k-wlc.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
2F0894E3F3A1323FDE2733EB456AE5B7E1A417BF46B53AD1323D1B02BA7688667C84AC7BD274B6B3A5DD3D19EB7EFA5DAB13E9941A37C73256C7577F3A3A1
cat9k-webui.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
ADE978FA0AC1C2694BEA93C96F77DC0E96D7D36134795A1197AF60B9E2E9EE5820C535E9CE11A5FED50542C6A94B55742E916185E333D3EF9E716D16AD0FDD
cat9k-guestshell.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
174AE72DF46F86D5ADDA73344295A91C809CD42E6C12FBE9204215DAC89140511EFE2DEF8E85CAD731B4276C85B3F7D5BF9386083CCEB3E4C504E1E0400E1
cat9k-sdrdriver.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
64884593C281B687374E283E14BFCF89F6D37EB4C238E7D71FA280B940FD0D11F57BAFF16788AA054FEE6B898BC689D623DDE25C743069538A7E83F146240
cat9k-sipbase.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
0AFF960435A97C9FA3522AC93E5CE1A683003C93CED4288AA8AE481E3D9D880451A23022A5E810A010B6196B802CFA5D1354DDCC6B7A7120FF4A915B9ECF9
cat9k-espbases.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
6D5324CD00E578EFFE5C874620900AEEFC38CD05B01E43B4E579E267D581145FE5EFC5E5DD09EE12338FDB2A162A389FED6C951AF8C394AE5FAF4FAE4D7E9
cat9k-cc_sdrdriver.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
59362HDD62AB1E94297891D8ECEB467FE28261B6D75F6442610DD41AE54D69609C94D081D32142412CC69C5C88036F26BE5F356B848ACBEB5692A423D92F
cat9k-sipsps.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
708BD0869E841CD9220C9165C6646D07CE206FAD29449E81A915E69F3063B9FAFCBBE5B048F250150E07EA37160AA8E5AA4CD491E4020C836A6322631175
cat9k-rpbase.BLD_V1611_THROTTLE_LATEST_20190203_030036.SSA.pkg:
F24FB837047A3D0930F8B353E2494EFCB0FB60E2A1BFE5F9C322EBC675A0A5D94CC36195B41971F5B47383FB095BC731FB45407D42E57BA14E3E6DEFFHE
PCR0: 7803FB049E7B111131B2FDACAF9B1918C28448E250054FE0C65D0317427A5EB1
PCR8: 0B65A1D00AA4AC815552170D11E5B4405C6D4B80453925E54F866D5BDF2B718A
Signature version: 1
Signature:
```

Additional References for Boot Integrity Visibility

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

Feature History for Boot Integrity Visibility

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|---------------------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Boot Integrity Visibility | Boot Integrity Visibility allows Cisco's platform identity and software integrity information to be visible and actionable. Platform identity provides the platform's manufacturing installed identity. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 3

Performing Device Setup Configuration

- [Information About Performing Device Setup Configuration, on page 47](#)
- [How to Perform Device Setup Configuration, on page 57](#)
- [Monitoring Device Setup Configuration, on page 67](#)
- [Configuration Examples for Performing Device Setup, on page 67](#)
- [Additional References For Performing Device Setup, on page 69](#)
- [Feature History for Performing Device Setup Configuration, on page 69](#)

Information About Performing Device Setup Configuration

Review the sections in this module before performing your initial device configuration tasks that include IP address assignments and DHCP autoconfiguration.

Device Boot Process

To start your device, you need to follow the procedures in the hardware installation guide for installing and powering on the device and setting up the initial device configuration.

The normal boot process involves the operation of the boot loader software and includes these activities:

- Performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, its quantity, its speed, and so forth.
- Performs power-on self-test (POST) for the CPU subsystem and tests the system DRAM.
- Initializes the file systems on the system board.
- Loads a default operating system software image into memory and boots up the device.

The boot loader provides access to the file systems before the operating system is loaded. Normally, the boot loader is used only to load, decompress, and start the operating system. After the boot loader gives the operating system control of the CPU, the boot loader is not active until the next system reset or power-on.

Before you can assign device information, make sure you have connected a PC or terminal to the console port or a PC to the Ethernet management port, and make sure you have configured the PC or terminal-emulation software baud rate and character format to match these of the device console port:

- Baud rate default is 9600.

- Data bits default is 8.



Note If the data bits option is set to 8, set the parity option to none.

- Stop bits default is 2 (minor).
- Parity settings default is none.

Devices Information Assignment

You can assign IP information through the device setup program, through a DHCP server, or manually.

Use the device setup program if you want to be prompted for specific IP information. With this program, you can also configure a hostname and an enable secret password.

It gives you the option of assigning a Telnet password (to provide security during remote management) and configuring your switch as a command or member switch of a cluster or as a standalone switch.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.



Note If you are using DHCP, do not respond to any of the questions in the setup program until the device receives the dynamically assigned IP address and reads the configuration file.

If you are an experienced user familiar with the device configuration steps, manually configure the device. Otherwise, use the setup program described in the [Device Boot Process, on page 47](#) section.

Default Switch Information

Table 4: Default Switch Information

| Feature | Default Setting |
|--------------------------------------|--|
| IP address and subnet mask | No IP address or subnet mask are defined. |
| Default gateway | No default gateway is defined. |
| Enable secret password | No password is defined. |
| Hostname | The factory-assigned default hostname is device. |
| Telnet password | No password is defined. |
| Cluster command switch functionality | Disabled. |
| Cluster name | No cluster name is defined. |

DHCP-Based Autoconfiguration Overview

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and an operation for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The device can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your device (DHCP client) is automatically configured at startup with IP address information and a configuration file.

With DHCP-based autoconfiguration, no DHCP client-side configuration is needed on your device. However, you need to configure the DHCP server for various lease options associated with IP addresses.

If you want to use DHCP to relay the configuration file location on the network, you might also need to configure a Trivial File Transfer Protocol (TFTP) server and a Domain Name System (DNS) server.



Note We recommend a redundant connection between a switch stack and the DHCP, DNS, and TFTP servers. This is to help ensure that these servers remain accessible in case one of the connected stack members is removed from the switch stack.

The DHCP server for your device can be on the same LAN or on a different LAN than the device. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your device and the DHCP server. A relay device forwards broadcast traffic between two directly connected LANs. A router does not forward broadcast packets, but it forwards packets based on the destination IP address in the received packet.

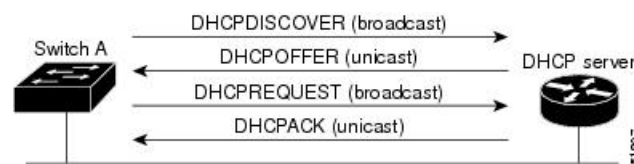
DHCP-based autoconfiguration replaces the BOOTP client functionality on your device.

DHCP Client Request Process

When you boot up your device, the DHCP client is invoked and requests configuration information from a DHCP server when the configuration file is not present on the device. If the configuration file is present and the configuration includes the **ip address dhcp** interface configuration command on specific routed interfaces, the DHCP client is invoked and requests the IP address information for those interfaces.

This is the sequence of messages that are exchanged between the DHCP client and the DHCP server.

Figure 3: DHCP Client and Server Message Exchange



The client, Device A, broadcasts a DHCPDISCOVER message to locate a DHCP server. The DHCP server offers configuration parameters (such as an IP address, subnet mask, gateway IP address, DNS IP address, a lease for the IP address, and so forth) to the client in a DHCPOFFER unicast message.

In a DHCPREQUEST broadcast message, the client returns a formal request for the offered configuration information to the DHCP server. The formal request is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the device receives depends on how you configure the DHCP server.

If the configuration parameters sent to the client in the DHCP OFFER unicast message are invalid (a configuration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCPNAK denial broadcast message, which means that the offered configuration parameters have not been assigned, that an error has occurred during the negotiation of the parameters, or that the client has been slow in responding to the DHCP OFFER message (the DHCP server assigned the parameters to another client).

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee that the IP address is allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the device accepts replies from a BOOTP server and configures itself, the device broadcasts, instead of unicasts, TFTP requests to obtain the device configuration file.

The DHCP hostname option allows a group of devices to obtain hostnames and a standard configuration from the central management DHCP server. A client (device) includes in its DHCPDISCOVER message an option 12 field used to request a hostname and other configuration parameters from the DHCP server. The configuration files on all clients are identical except for their DHCP-obtained hostnames.

DHCP-based Autoconfiguration and Image Update

You can use the DHCP image upgrade features to configure a DHCP server to download both a new image and a new configuration file to one or more devices in a network. Simultaneous image and configuration upgrade for all switches in the network helps ensure that each new device added to a network receives the same image and configuration.

There are two types of DHCP image upgrades: DHCP autoconfiguration and DHCP auto-image update.

Restrictions for DHCP-based Autoconfiguration

- The DHCP-based autoconfiguration with a saved configuration process stops if there is not at least one Layer 3 interface in an up state without an assigned IP address in the network.
- Unless you configure a timeout, the DHCP-based autoconfiguration with a saved configuration feature tries indefinitely to download an IP address.
- The auto-install process stops if a configuration file cannot be downloaded or if the configuration file is corrupted.
- The configuration file that is downloaded from TFTP is merged with the existing configuration in the running configuration but is not saved in the NVRAM unless you enter the **write memory** or **copy running-configuration startup-configuration** privileged EXEC command. If the downloaded configuration is saved to the startup configuration, the feature is not triggered during subsequent system restarts.

DHCP Autoconfiguration

DHCP autoconfiguration downloads a configuration file to one or more devices in your network from a DHCP server. The downloaded configuration file becomes the running configuration of the device. It does not overwrite the bootup configuration saved in the flash, until you reload the device.

DHCP Auto-Image Update

You can use DHCP auto-image upgrade with DHCP autoconfiguration to download both a configuration and a new image to one or more devices in your network. The devices (or devices) downloading the new configuration and the new image can be blank (or only have a default factory configuration loaded).

If the new configuration is downloaded to a switch that already has a configuration, the downloaded configuration is appended to the configuration file stored on the switch. (Any existing configuration is not overwritten by the downloaded one.)

To enable a DHCP auto-image update on the device, the TFTP server where the image and configuration files are located must be configured with the correct option 67 (the configuration filename), option 66 (the DHCP server hostname) option 150 (the TFTP server address), and option 125 (description of the Cisco IOS image file) settings.

After you install the device in your network, the auto-image update feature starts. The downloaded configuration file is saved in the running configuration of the device, and the new image is downloaded and installed on the device. When you reboot the device, the configuration is stored in the saved configuration on the device.

DHCP Server Configuration Guidelines

Follow these guidelines if you are configuring a device as a DHCP server:

- You should configure the DHCP server with reserved leases that are bound to each device by the device hardware address.
- If you want the device to receive IP address information, you must configure the DHCP server with these lease options:
 - IP address of the client (required)
 - Subnet mask of the client (required)
 - DNS server IP address (optional)
 - Router IP address (default gateway address to be used by the device) (required)
- If you want the device to receive the configuration file from a TFTP server, you must configure the DHCP server with these lease options:
 - TFTP server name (required)
 - Boot filename (the name of the configuration file that the client needs) (recommended)
 - Hostname (optional)
- Depending on the settings of the DHCP server, the device can receive IP address information, the configuration file, or both.

- If you do not configure the DHCP server with the lease options described previously, it replies to client requests with only those parameters that are configured. If the IP address and the subnet mask are not in the reply, the device is not configured. If the router IP address or the TFTP server name are not found, the device might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.
- The device can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your device but are not configured. (These features are not operational.)

Purpose of the TFTP Server

Based on the DHCP server configuration, the device attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the device with all the options required for IP connectivity to the TFTP server, and if you configured the DHCP server with a TFTP server name, address, and configuration filename, the device attempts to download the specified configuration file from the specified TFTP server.

If you did not specify the configuration filename, the TFTP server, or if the configuration file could not be downloaded, the device attempts to download a configuration file by using various combinations of filenames and TFTP server addresses. The files include the specified configuration filename (if any) and these files: `network-config`, `cisconet.cfg`, `hostname.config`, or `hostname.cfg`, where *hostname* is the device's current hostname. The TFTP server addresses used include the specified TFTP server address (if any) and the broadcast address (255.255.255.255).

For the device to successfully download a configuration file, the TFTP server must contain one or more configuration files in its base directory. The files can include these files:

- The configuration file named in the DHCP reply (the actual device configuration file).
- The `network-config` or the `cisconet.cfg` file (known as the default configuration files).
- The `router-config` or the `ciscotr.cfg` file (These files contain commands common to all device. Normally, if the DHCP and TFTP servers are properly configured, these files are not accessed.)

If you specify the TFTP server name in the DHCP server-lease database, you must also configure the TFTP server name-to-IP-address mapping in the DNS-server database.

If the TFTP server to be used is on a different LAN from the device, or if it is to be accessed by the device through the broadcast address (which occurs if the DHCP server response does not contain all the required information described previously), a relay must be configured to forward the TFTP packets to the TFTP server. The preferred solution is to configure the DHCP server with all the required information.

Purpose of the DNS Server

The DHCP server uses the DNS server to resolve the TFTP server name to an IP address. You must configure the TFTP server name-to-IP address map on the DNS server. The TFTP server contains the configuration files for the device.

You can configure the IP addresses of the DNS servers in the lease database of the DHCP server from where the DHCP replies will retrieve them. You can enter up to two DNS server IP addresses in the lease database.

The DNS server can be on the same LAN or on a different LAN from the device. If it is on a different LAN, the device must be able to access it through a router.

How to Obtain Configuration Files

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the device obtains its configuration information in these ways:

- The IP address and the configuration filename is reserved for the device and provided in the DHCP reply (one-file read method).

The device receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. The device sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server and upon receipt, it completes its boot up process.

- The IP address and the configuration filename is reserved for the device, but the TFTP server address is not provided in the DHCP reply (one-file read method).

The device receives its IP address, subnet mask, and the configuration filename from the DHCP server. The device sends a broadcast message to a TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, it completes its boot-up process.

- Only the IP address is reserved for the device and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

The device receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The device sends a unicast message to the TFTP server to retrieve the network-config or cisco.net.cfg default configuration file. (If the network-config file cannot be read, the device reads the cisco.net.cfg file.)

The default configuration file contains the hostnames-to-IP-address mapping for the device. The device fills its host table with the information in the file and obtains its hostname. If the hostname is not found in the file, the device uses the hostname in the DHCP reply. If the hostname is not specified in the DHCP reply, the device uses the default *Switch* as its hostname.

After obtaining its hostname from the default configuration file or the DHCP reply, the device reads the configuration file that has the same name as its hostname (*hostname-config* or *hostname.cfg*, depending on whether network-config or cisco.net.cfg was read earlier) from the TFTP server. If the cisco.net.cfg file is read, the filename of the host is truncated to eight characters.

If the device cannot read the network-config, cisco.net.cfg, or the hostname file, it reads the router-config file. If the device cannot read the router-config file, it reads the ciscotr.cfg file.

**Note**

The device broadcasts TFTP server requests if the TFTP server is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

How to Control Environment Variables

With a normally operating device, you enter the boot loader mode only through the console connection configured for 9600 bps. Unplug the device power cord, and press the **Mode** button while reconnecting the power cord. The boot loader device prompt then appears.

The device boot loader software provides support for nonvolatile environment variables, which can be used to control how the boot loader, or any other software running on the system, operates. Boot loader environment variables are similar to environment variables that can be set on UNIX or DOS systems.

Environment variables that have values are stored in flash memory outside of the flash file system.

Each line in these files contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not present; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, "") is a variable with a value. Many environment variables are predefined and have default values.

You can change the settings of the environment variables by accessing the boot loader or by using Cisco IOS commands. Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Common Environment Variables

This table describes the function of the most common environment variables.

Table 5: Common Environment Variables

| Variable | Boot Loader Command | Cisco IOS Global Configuration Command |
|----------|---|---|
| BOOT | <p>set BOOT <i>filesystem</i> <i>:/file-url ...</i></p> <p>A semicolon-separated list of executable files to try to load and execute when automatically booting.</p> | <p>boot system <i>{filesystem : /file-url ... switch {number all}}</i></p> <p>Specifies the Cisco IOS image to load during the next boot cycle and the stack members on which the image is loaded. This command changes the setting of the BOOT environment variable.</p> <p>The package provisioning file, also referred to as the <i>packages.conf</i> file, is used by the system to determine which software packages to activate during boot up.</p> <ul style="list-style-type: none"> When booting in installed mode, the package provisioning file specified in the boot command is used to determine which packages to activate. For example boot flash:packages.conf. When booting in bundle mode, the package provisioning file contained in the booted bundle is used to activate the packages included in the bundle. For example, boot flash:image.bin. |

| Variable | Boot Loader Command | Cisco IOS Global Configuration Command |
|-----------------|--|--|
| MANUAL_BOOT | set MANUAL_BOOT yes Decides whether the switch automatically or manually boots. Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the boot loader mode. | boot manual Enables manually booting the switch during the next boot cycle and changes the setting of the MANUAL_BOOT environment variable. The next time you reboot the system, the switch is in boot loader mode. To boot up the system, use the boot flash: filesystem :/ file-url boot loader command, and specify the name of the bootable image. |
| CONFIG_FILE | set CONFIG_FILE flash:/ file-url Changes the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. | boot config-file flash:/ file-url Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. This command changes the CONFIG_FILE environment variable. |
| SWITCH_NUMBER | set SWITCH_NUMBER stack-member-number Changes the member number of a stack member. | switch current-stack-member-number renumber new-stack-member-number Changes the member number of a stack member. |
| SWITCH_PRIORITY | set SWITCH_PRIORITY stack-member-number Changes the priority value of a stack member. | switch stack-member-number priority priority-number Changes the priority value of a stack member. |
| BAUD | set BAUD baud-rate | line console 0 speed speed-value Configures the baud rate. |
| ENABLE_BREAK | set ENABLE_BREAK yes/no | boot enable-break switch yes/no Enables a break to the auto-boot cycle. You have 5 seconds to enter the break command. |

Environment Variables for TFTP

When the switch is connected to a PC through the Ethernet management port, you can download or upload a configuration file to the boot loader by using TFTP. Make sure the environment variables in this table are configured.

Table 6: Environment Variables for TFTP

| Variable | Description |
|-----------------|--|
| MAC_ADDR | Specifies the MAC address of the switch. Note We recommend that you do not modify this variable. However, if you modify this variable after the boot loader is up or the value is different from the saved value, enter this command before using TFTP. A reset is required for the new value to take effect. |
| IP_ADDRESS | Specifies the IP address and the subnet mask for the associated IP subnet of the switch. |
| DEFAULT_GATEWAY | Specifies the IP address and subnet mask of the default gateway. |

Scheduled Reload of the Software Image

You can schedule a reload of the software image to occur on the device at a later time (for example, late at night or during the weekend when the device is used less), or you can synchronize a reload network-wide (for example, to perform a software upgrade on all device in the network).



Note A scheduled reload must take place within approximately 24 days.

You have these reload options:

- Reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 hours. You can specify the reason for the reload in a string up to 255 characters in length.
- Reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight.

The **reload** command halts the system. If the system is not set to manually boot up, it reboots itself.

If your device is configured for manual booting, do not reload it from a virtual terminal. This restriction prevents the device from entering the boot loader mode and then taking it from the remote user's control.

If you modify your configuration file, the device prompts you to save the configuration before reloading. During the save operation, the system requests whether you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you proceed in this situation, the system enters setup mode upon reload.

To cancel a previously scheduled reload, use the **reload cancel** privileged EXEC command.

How to Perform Device Setup Configuration

Using DHCP to download a new image and a new configuration to a device requires that you configure at least two devices. One device acts as a DHCP and TFTP server and the second device (client) is configured to download either a new configuration file or a new configuration file and a new image file.

Configuring DHCP Autoconfiguration (Only Configuration File)

This task describes how to configure DHCP autoconfiguration of the TFTP and DHCP settings on an existing device in the network so that it can support the autoconfiguration of a new device.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | ip dhcp pool <i>poolname</i> Example: Device(config)# ip dhcp pool pool | Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode. |
| Step 3 | boot <i>filename</i> Example: Device(dhcp-config)# boot config-boot.text | Specifies the name of the configuration file that is used as a boot image. |
| Step 4 | network <i>network-number mask prefix-length</i> Example: Device(dhcp-config)# network 10.10.10.0 255.255.255.0 | Specifies the subnet network number and mask of the DHCP address pool. Note The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/). |
| Step 5 | default-router <i>address</i> Example: | Specifies the IP address of the default router for a DHCP client. |

| | Command or Action | Purpose |
|----------------|--|---|
| | Device (dhcp-config) # default-router 10.10.10.1 | |
| Step 6 | option 150 <i>address</i> Example: Device (dhcp-config) # option 150 10.10.10.1 | Specifies the IP address of the TFTP server. |
| Step 7 | exit Example: Device (dhcp-config) # exit | Returns to global configuration mode. |
| Step 8 | tftp-server flash: <i>filename.text</i> Example: Device (config) # tftp-server flash:config-boot.text | Specifies the configuration file on the TFTP server. |
| Step 9 | interface <i>interface-id</i> Example: | Specifies the address of the client that will receive the configuration file. |
| Step 10 | no switchport Example: Device (config-if) # no switchport | Puts the interface into Layer 3 mode. |
| Step 11 | ip address <i>address mask</i> Example: Device (config-if) # ip address 10.10.10.1 255.255.255.0 | Specifies the IP address and mask for the interface. |
| Step 12 | end Example: Device (config-if) # end | Returns to privileged EXEC mode. |

Configuring DHCP Auto-Image Update (Configuration File and Image)

This task describes DHCP autoconfiguration to configure TFTP and DHCP settings on an existing device to support the installation of a new switch.

Before you begin

You must first create a text file (for example, `autoinstall_dhcp`) that will be uploaded to the device. In the text file, put the name of the image that you want to download (for example, `cat9k_iosxe.16.xx.xx.SPA.bin`).

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | ip dhcp pool <i>poolname</i> Example: Device(config)# ip dhcp pool pool1 | Creates a name for the DHCP server address pool and enter DHCP pool configuration mode. |
| Step 3 | boot <i>filename</i> Example: Device(dhcp-config)# boot config-boot.text | Specifies the name of the file that is used as a boot image. |
| Step 4 | network <i>network-number mask prefix-length</i> Example: Device(dhcp-config)# network 10.10.10.0 255.255.255.0 | Specifies the subnet network number and mask of the DHCP address pool. Note The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/). |
| Step 5 | default-router <i>address</i> Example: Device(dhcp-config)# default-router 10.10.10.1 | Specifies the IP address of the default router for a DHCP client. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 6 | option 150 <i>address</i> Example: <pre>Device(dhcp-config)# option 150 10.10.10.1</pre> | Specifies the IP address of the TFTP server. |
| Step 7 | option 125 <i>hex</i> Example: <pre>Device(dhcp-config)# option 125 hex 0000.0009.0a05.0866.1.7574.6f69.6e73.7461.6c6c.5f64.696370</pre> | Specifies the path to the text file that describes the path to the image file. |
| Step 8 | copy tftp flash <i>filename.txt</i> Example: <pre>Device(config)# copy tftp flash image.bin</pre> | Uploads the text file to the device. |
| Step 9 | copy tftp flash <i>imagename.bin</i> Example: <pre>Device(config)# copy tftp flash image.bin</pre> | Uploads the tar file for the new image to the device. |
| Step 10 | exit Example: <pre>Device(dhcp-config)# exit</pre> | Returns to global configuration mode. |
| Step 11 | tftp-server flash: <i>config.text</i> Example: <pre>Device(config)# tftp-server flash:config-boot.text</pre> | Specifies the Cisco IOS configuration file on the TFTP server. |
| Step 12 | tftp-server flash: <i>imagename.bin</i> Example: <pre>Device(config)# tftp-server flash:image.bin</pre> | Specifies the image name on the TFTP server. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 13 | tftp-server flash: <i>filename.txt</i> Example: <pre>Device(config)# tftp-server flash:boot-config.text</pre> | Specifies the text file that contains the name of the image file to download |
| Step 14 | interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitEthernet1/0/4</pre> | Specifies the address of the client that will receive the configuration file. |
| Step 15 | no switchport Example: <pre>Device(config-if)# no switchport</pre> | Puts the interface into Layer 3 mode. |
| Step 16 | ip address <i>address mask</i> Example: <pre>Device(config-if)# ip address 10.10.10.1 255.255.255.0</pre> | Specifies the IP address and mask for the interface. |
| Step 17 | end Example: <pre>Device(config-if)# end</pre> | Returns to privileged EXEC mode. |
| Step 18 | copy running-config startup-config Example: <pre>Device(config-if)# end</pre> | (Optional) Saves your entries in the configuration file. |

Configuring the Client to Download Files from DHCP Server



Note You should only configure and enable the Layer 3 interface. Do not assign an IP address or DHCP-based autoconfiguration with a saved configuration.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | boot host dhcp Example: Device(conf)# boot host dhcp | Enables autoconfiguration with a saved configuration. |
| Step 3 | boot host retry timeout timeout-value Example: Device(conf)# boot host retry timeout 300 | (Optional) Sets the amount of time the system tries to download a configuration file. Note If you do not set a timeout, the system will try indefinitely to obtain an IP address from the DHCP server. |
| Step 4 | banner config-save ^C warning-message ^C Example: Device(conf)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot^C | (Optional) Creates warning messages to be displayed when you try to save the configuration file to NVRAM. |
| Step 5 | end Example: Device(config-if)# end | Returns to privileged EXEC mode. |
| Step 6 | show boot Example: Device# show boot | Verifies the configuration. |

Manually Assigning IP Information to Multiple SVIs

This task describes how to manually assign IP information to multiple switched virtual interfaces (SVIs):

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | interface vlan <i>vlan-id</i> Example: Device(config)# interface vlan 99 | Enters interface configuration mode, and enters the VLAN to which the IP information is assigned. The range is 1 to 4094. |
| Step 3 | ip address <i>ip-address subnet-mask</i> Example: Device(config-vlan)# ip address 10.10.10.2 255.255.255.0 | Enters the IP address and subnet mask. |
| Step 4 | exit Example: Device(config-vlan)# exit | Returns to global configuration mode. |
| Step 5 | ip default-gateway <i>ip-address</i> Example: Device(config)# ip default-gateway 10.10.10.1 | <p>Enters the IP address of the next-hop router interface that is directly connected to the device where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the device.</p> <p>Once the default gateway is configured, the device has connectivity to the remote networks with which a host needs to communicate.</p> <p>Note When your device is configured to route with IP, it does not need to have a default gateway set.</p> <p>Note The device capwap relays on default-gateway configuration to support routed access point join the device.</p> |
| Step 6 | end Example: | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Device(config)# end | |
| Step 7 | show interfaces vlan <i>vlan-id</i> Example: Device# show interfaces vlan 99 | Verifies the configured IP address. |
| Step 8 | show ip redirects Example: Device# show ip redirects | Verifies the configured default gateway. |

Modifying the Device Startup Configuration

Specifying the Filename to Read and Write the System Configuration

By default, the Cisco IOS software uses the config.text file to read and write a nonvolatile copy of the system configuration. However, you can specify a different filename, which will be loaded during the next boot cycle.

Before you begin

Use a standalone device for this task.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Switch# configure terminal | Enters global configuration mode. |
| Step 2 | boot flash: <i>file-url</i> Example: Switch(config)# boot flash:config.text | Specifies the configuration file to load during the next boot cycle. <i>file-url</i> —The path (directory) and the configuration filename. Filenames and directory names are case-sensitive. |
| Step 3 | end Example: | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Switch(config)# end | |
| Step 4 | show boot Example: Switch# show boot | Verifies your entries. The boot global configuration command changes the setting of the CONFIG_FILE environment variable. |
| Step 5 | copy running-config startup-config Example: Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Manually Booting the Switch

By default, the switch automatically boots up; however, you can configure it to manually boot up.

Before you begin

Use a standalone switch for this task.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | boot manual Example: Device(config)# boot manual | Enables the switch to manually boot up during the next boot cycle. |
| Step 3 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 4 | show boot Example: | Verifies your entries. The boot manual global command changes the setting of the MANUAL_BOOT environment variable. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Device# show boot | <p>The next time you reboot the system, the switch is in boot loader mode, shown by the <i>switch:</i> prompt. To boot up the system, use the boot filesystem:/file-url boot loader command.</p> <ul style="list-style-type: none"> • <i>filesystem:</i>—Uses flash: for the system board flash device. <p>Switch: boot flash:</p> <ul style="list-style-type: none"> • For <i>file-url</i>—Specifies the path (directory) and the name of the bootable image. <p>Filenames and directory names are case-sensitive.</p> |
| Step 5 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring a Scheduled Software Image Reload

This task describes how to configure your device to reload the software image at a later time.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | copy running-config startup-config Example: Device# copy running-config startup-config | Saves your device configuration information to the startup configuration before you use the reload command. |
| Step 3 | reload in [hh:]mm [text] Example: Device# reload in 12 System configuration has been modified. Save? [yes/no]: y | Schedules a reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days. You can specify the reason for the reload in a string up to 255 characters in length. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 4 | reload at <i>hh:mm</i> [<i>month day</i> <i>day month</i>] [<i>text</i>] Example: Device(config)# reload at 14:00 | Specifies the time in hours and minutes for the reload to occur. Note Use the at keyword only if the device system clock has been set (through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the device. To schedule reloads across several devices to occur simultaneously, the time on each device must be synchronized with NTP. |
| Step 5 | reload cancel Example: Device(config)# reload cancel | Cancels a previously scheduled reload. |
| Step 6 | show reload Example: show reload | Displays information about a previously scheduled reload or identifies if a reload has been scheduled on the device. |

Monitoring Device Setup Configuration

Configuration Examples for Performing Device Setup

Example: Configuring a Device as a DHCP Server

```

Device# configure terminal
Device(config)# ip dhcp pool pool1
Device(dhcp-config)# network 10.10.10.0 255.255.255.0
Device(dhcp-config)# boot config-boot.text
Device(dhcp-config)# default-router 10.10.10.1
Device(dhcp-config)# option 150 10.10.10.1
Device(dhcp-config)# exit
Device(config)# tftp-server flash:config-boot.text
Device(config)# interface gigabitethernet1/0/4
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.10.1 255.255.255.0
Device(config-if)# end

```

Example: Configuring DHCP Auto-Image Update

```

Device# configure terminal
Device(config)# ip dhcp pool pool1
Device(dhcp-config)# network 10.10.10.0 255.255.255.0
Device(dhcp-config)# boot config-boot.text
Device(dhcp-config)# default-router 10.10.10.1
Device(dhcp-config)# option 150 10.10.10.1
Device(dhcp-config)# option 125 hex 0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370

Device(dhcp-config)# exit
Device(config)# tftp-server flash:config-boot.text
Device(config)# tftp-server flash:image_name
Device(config)# tftp-server flash:boot-config.text
Device(config)# tftp-server flash:autoinstall_dhcp
Device(config)# interface gigabitethernet1/0/4
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.10.1 255.255.255.0
Device(config-if)# end

```

Example: Configuring a Device to Download Configurations from a DHCP Server

This example uses a Layer 3 SVI interface on VLAN 99 to enable DHCP-based autoconfiguration with a saved configuration:

```

Device# configure terminal
Device(config)# boot host dhcp
Device(config)# boot host retry timeout 300
Device(config)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause
  You to No longer Automatically Download Configuration Files at Reboot^C
Device(config)# vlan 99
Device(config-vlan)# interface vlan 99
Device(config-if)# no shutdown
Device(config-if)# end
Device# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:         no
Manual Boot:          no
HELPER path-list:
NVRAM/Config file
  buffer size:        32768
Timeout for Config
  Download:           300 seconds
Config Download
  via DHCP:           enabled (next boot: enabled)
Device#

```

Examples: Scheduling Software Image Reload

This example shows how to reload the software on the device on the current day at 7:30 p.m:

```
Device# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 2013 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

This example shows how to reload the software on the device at a future time:

```
Device# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 2013 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

Additional References For Performing Device Setup

Related Documents

| Related Topic | Document Title |
|---|--|
| Device setup commands Boot loader commands | <i>Command Reference (Catalyst 9600 Series Switches)</i> |
| Hardware installation | <i>Cisco Catalyst 9600 Series Switches Hardware Installation Guide</i> |

Feature History for Performing Device Setup Configuration

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|----------------------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Device Setup Configuration | A device setup configuration can be performed, including auto configuration of IP address assignments and DHCP. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 4

Configuring Smart Licensing

- Prerequisites for Configuring Smart Licensing, on page 71
- Introduction to Smart Licensing, on page 71
- Connecting to CSSM, on page 72
- Configuring a Connection to CSSM and Setting Up the License Level, on page 74
- Registering a Device on CSSM, on page 84
- Monitoring Smart Licensing Configuration, on page 88
- Configuration Examples for Smart Licensing, on page 89
- Additional References, on page 90
- Feature History for Smart Licensing, on page 90

Prerequisites for Configuring Smart Licensing

You must have the following in [CSSM](#):

- Cisco Smart Account
- One or more Virtual Account
- User role with proper access rights
- You should have accepted the Smart Software Licensing Agreement on CSSM to register devices.
- Network reachability to <https://tools.cisco.com>.

Introduction to Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Overview of CSSM

Cisco Smart Software Manager (CSSM) enables you to manage all your Cisco smart software licenses from one centralized portal. With CSSM, you can organize and view your licenses in groups called virtual accounts (collections of licenses and product instances).

You can access the CSSM on <https://software.cisco.com/#>, by clicking the **Smart Software Licensing** link under the **License** tab.



Note Use a Chrome 32.0, Firefox 25.0, or Safari 6.0.5 web browser to access CSSM. Also, ensure that Javascript 1.5 or a later version is enabled in your browser.

Use the CSSM to do the following tasks:

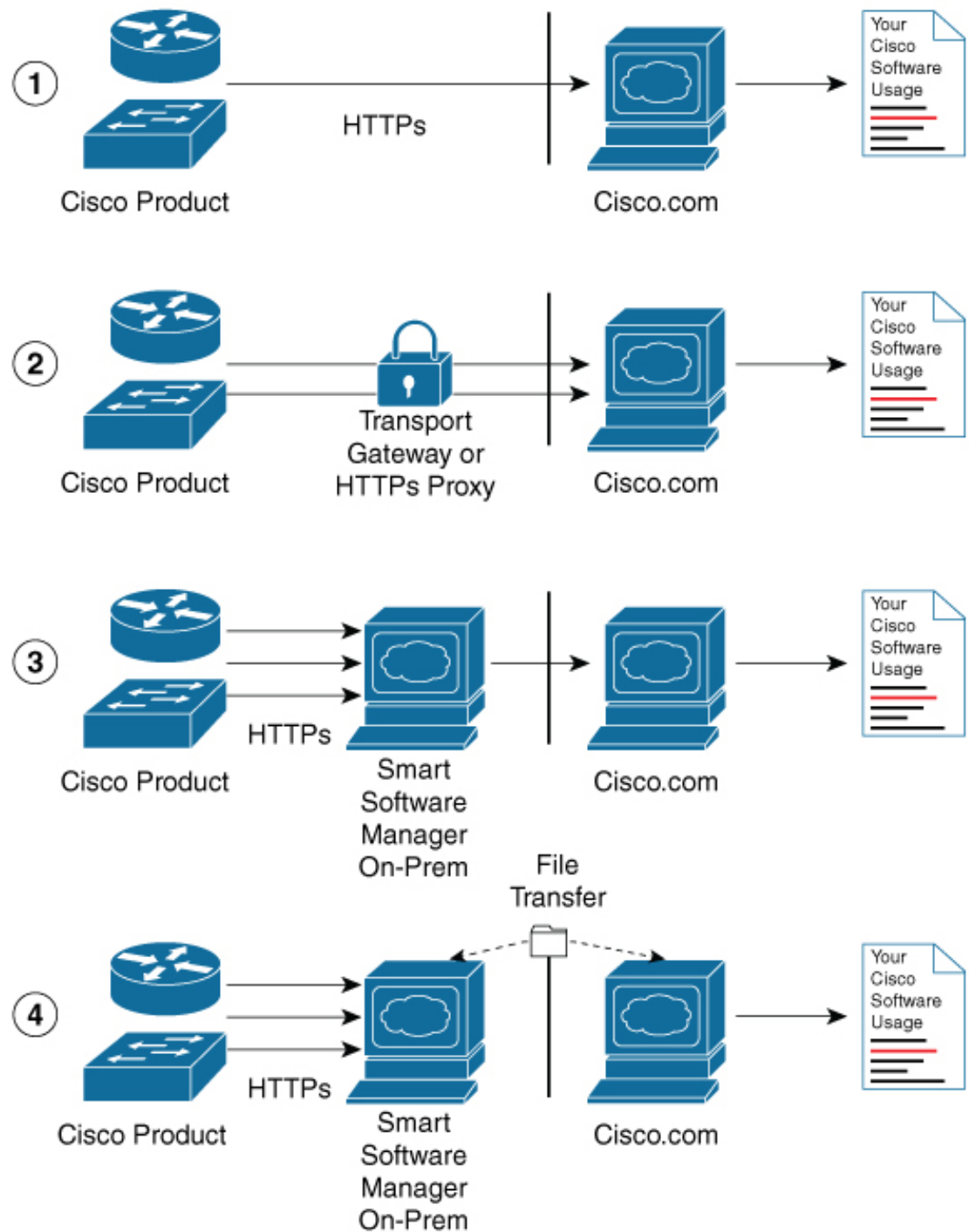
- Create, manage, or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove, or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.

CSSM Help describes the procedures for carrying out these tasks.

Connecting to CSSM

The following illustration shows the various options available to connect to CSSM:

Figure 4: Connection Options



1. Direct cloud access: In this method, Cisco products send usage information directly over the internet to Cisco.com; no additional components are needed for the connection.

2. Direct cloud access through an HTTPs proxy: In this method, Cisco products send usage information over the internet through a proxy server - either a Call Home Transport Gateway or an off-the-shelf proxy (such as Apache) to Cisco.com.
3. Mediated access through a connected on-premises collector: In this method, Cisco products send usage information to a locally-connected collector, which acts as a local license authority. Periodically, this information is exchanged to keep the databases synchronized.
4. Mediated access through a disconnected on-premises collector: In this method, Cisco products send usage information to a local disconnected collector, which acts as a local license authority. Exchange of human-readable information takes place occasionally (maybe once a month) to keep the databases synchronized.

Options 1 and 2 provide an easy connection option, and options 3 and 4 provide a secure environment connection option. Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) provides support for options 3 and 4.

Configuring a Connection to CSSM and Setting Up the License Level

The following sections provide information about how to set up a connection to CSSM and set up the license level.

Setting Up a Connection to CSSM

The following steps show how to set up a Layer 3 connection to CSSM to verify network reachability. Skip this section if you already have Layer 3 connectivity to CSSM.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | {ip ipv6} name-server server-address 1 [server-address 2] [server-address 3] [server-address 4] [server-address 5] [server-address 6] Example: Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230 | Configures Domain Name System (DNS). |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 4 | ip name-server vrf Mgmt-vrf server-address 1 [server-address 2] [server-address 3] [server-address 4] [server-address 5] [server-address 6] Example: <pre>Device(config)# ip name-server vrf Mgmt-vrf 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230</pre> | (Optional) Configures DNS on the VRF interface. Note You should configure this command as an alternative to the ip name-server command. |
| Step 5 | ip domain lookup source-interface interface-type interface-number Example: <pre>Device(config)# ip domain lookup source-interface Vlan100</pre> | (Optional) Configures the source interface for the DNS domain lookup. |
| Step 6 | ip domain name example.com Example: <pre>Device(config)# ip domain name example.com</pre> | Configures the domain name. |
| Step 7 | ip host tools.cisco.com ip-address Example: <pre>Device(config)# ip host tools.cisco.com 209.165.201.30</pre> | (Optional) Configures static hostname-to-address mappings in the DNS hostname cache if automatic DNS mapping is not available. |
| Step 8 | interface vlan_id Example: <pre>Device(config)# interface Vlan100 Device(config-if)# ip address 192.0.2.10 255.255.255.0 Device(config-if)# exit</pre> | Configures a Layer 3 interface. |
| Step 9 | ntp server ip-address [version number] [key key-id] [prefer] Example: <pre>Device(config)# ntp server 198.51.100.100 version 2 prefer</pre> | Forms a server association with the specified system. Note The ntp server command is mandatory to ensure that the device time is synchronized with CSSM. |
| Step 10 | switchport access vlan vlan_id Example: <pre>Device(config)# interface GigabitEthernet1/0/1 Device(config-if)# switchport access vlan 100 Device(config-if)# switchport mode</pre> | (Optional) Enables the VLAN for which this access port carries traffic and sets the interface as a nontrunking nontagged single-VLAN Ethernet interface. Note This step is to be configured only if the switchport access mode is required. |

| | Command or Action | Purpose |
|----------------|--|--|
| | access Device (config-if) # exit Device (config) # | |
| Step 11 | ip route <i>ip-address ip-mask subnet mask</i> Example: Device (config) # ip route 192.0.2.0 255.255.255.255 192.0.2.1 | Configures a route on the device. Note You can configure either a static route or a dynamic route. |
| Step 12 | license smart transport callhome Example: Device (config) # license smart transport callhome | Enables the transport mode as Call Home. Note The license smart transport callhome command is mandatory. |
| Step 13 | ip http client source-interface <i>interface-type interface-number</i> Example: Device (config) # ip http client source-interface Vlan100 | Configures a source interface for the HTTP client. Note The ip http client source-interface interface-type interface-number command is mandatory. |
| Step 14 | exit Example: Device (config) # exit | (Optional) Exits global configuration mode and returns to privileged EXEC mode. |
| Step 15 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring the Call Home Service for Direct Cloud Access



Note By default, the CiscoTAC-1 profile is already set up on the device. Use the **show call-home profile all** command to check the profile status.

The Call Home service provides email-based and web-based notification of critical system events to CSSM. To configure and enable the Call Home service, perform this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|-------------------|-------------------------------|
| Step 1 | enable | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|----------------|--|--|
| | Example: Device> enable | Enter your password, if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | call-home Example: Device(config)# call-home | Enters Call Home configuration mode. |
| Step 4 | no http secure server-identity-check Example: Device(config-call-home)# no http secure server-identity-check | Disables server identity check when HTTP connection is established. |
| Step 5 | contact-email-address email-address Example: Device(config-call-home)# contact-email-addr username@example.com | Assigns customer's email address. You can enter up to 200 characters in email address format with no spaces. |
| Step 6 | profile CiscoTAC-1 Example: Device(config-call-home)# profile CiscoTAC-1 | By default, the CiscoTAC-1 profile is inactive. To use this profile with the Call Home service, you must enable the profile. |
| Step 7 | destination transport-method http Example: Device(config-call-home-profile)# destination transport-method http | Enables the Call Home service via HTTP. |
| Step 8 | destination address http url Example: Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/other/services/DCService | Connects to CSSM. |
| Step 9 | active Example: Device(config-call-home-profile)# active | Enables the destination profile. |
| Step 10 | no destination transport-method email Example: Device(config-call-home-profile)# no destination transport-method email | Disables the Call Home service via email. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 11 | exit Example: Device (config-call-home-profile) # exit | Exits Call Home destination profile configuration mode and returns to Call Home configuration mode. |
| Step 12 | exit Example: Device (config-call-home) # exit | Exits Call Home configuration mode and returns to global configuration mode. |
| Step 13 | service call-home Example: Device (config) # service call-home | Enables the Call Home feature. |
| Step 14 | exit Example: Device (config) # exit | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 15 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server

The Call Home service can be configured through an HTTPs proxy server. This configuration requires no user authentication to connect to CSSM.



Note Authenticated HTTPs proxy configurations are not supported.

To configure and enable the Call Home service through an HTTPs proxy, perform this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 3 | call-home Example: Device(config)# call-home | Enters Call Home configuration mode. |
| Step 4 | contact-email-address email-address Example: Device(config-call-home)# contact-email-addr sch-smart-licensing@cisco.com | Configures the default email address as sch-smart-licensing@cisco.com. |
| Step 5 | http-proxy proxy-address proxy-port port-number Example: Device(config-call-home)# http-proxy 198.51.100.10 port 3128 | Configures the proxy server information to the Call Home service. |
| Step 6 | profile CiscoTAC-1 Example: Device(config-call-home)# profile CiscoTAC-1 | By default, the CiscoTAC-1 profile is inactive. To use this profile with the Call Home service, you must enable the profile. |
| Step 7 | destination transport-method http Example: Device(config-call-home-profile)# destination transport-method http | Enables the Call Home service via HTTP. |
| Step 8 | no destination transport-method email Example: Device(config-call-home-profile)# no destination transport-method email | Disables the Call Home service via email. |
| Step 9 | profile name Example: Device(config-call-home)# profile test1 | Enters Call Home destination profile configuration mode for the specified destination profile name. If the specified destination profile does not exist, it is created. |
| Step 10 | reporting smart-licensing-data Example: Device(config-call-home-profile)# reporting smart-licensing-data | Enables data sharing with the Call Home service via HTTP. |
| Step 11 | destination transport-method http Example: Device(config-call-home-profile)# destination transport-method http | Enables the HTTP message transport method. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 12 | destination address <i>http url</i> Example: Device (config-call-home-profile) # destination address <i>http</i> <i>https://tools.cisco.com/its/service/otbe/services/DIOService</i> | Connects to CSSM. |
| Step 13 | active Example: Device (config-call-home-profile) # active | Enables the destination profile. |
| Step 14 | exit Example: Device (config-call-home-profile) # exit | Exits Call Home destination profile configuration mode and returns to Call Home configuration mode. |
| Step 15 | exit Example: Device (config-call-home) # exit | Exits Call Home configuration mode and returns to global configuration mode. |
| Step 16 | service call-home Example: Device (config) # service call-home | Enables the Call Home feature. |
| Step 17 | ip http client proxy-server <i>proxy-address</i> proxy-port <i>port-number</i> Example: Device (config) # ip http client proxy-server <i>198.51.100.10 port 3128</i> | Enables the Call Home feature. |
| Step 18 | exit Example: Device (config) # exit | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 19 | copy running-config startup-config Example: Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Configuring the Call Home Service for Cisco Smart Software Manager On-Prem

For information about Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite), see <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html>.

To configure the Call Home service for the Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite), perform this procedure:

Procedure

| | Command or Action | Purpose |
|----------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | call-home Example: Device(config)# call-home | Enters Call Home configuration mode. |
| Step 4 | profile CiscoTAC-1 Example: Device(config-call-home)# profile CiscoTAC-1 | By default, the CiscoTAC-1 profile is inactive. To use this profile with the Call Home service, you must enable the profile. |
| Step 5 | no destination address http url Example: Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/otha/services/IOSService | Disable the default destination address. |
| Step 6 | no http secure server-identity-check Example: Device(config-call-home)# no http secure server-identity-check | Disables server identity check when HTTP connection is established. |
| Step 7 | profile name Example: Device(config-call-home)# profile test1 | Enters Call Home destination profile configuration mode for the specified destination profile name. If the specified destination profile does not exist, it is created. |
| Step 8 | reporting smart-licensing-data Example: Device(config-call-home-profile)# reporting smart-licensing-data | Enables data sharing with the Call Home service via HTTP. |
| Step 9 | destination transport-method http Example: Device(config-call-home-profile)# destination transport-method http | Enables the HTTP message transport method. |
| Step 10 | destination address http url Example: | Configures the destination URL (CSSM) to which Call Home messages are sent. |

| | Command or Action | Purpose |
|----------------|---|---|
| | <pre>Device(config-call-home-profile)# destination address http https://209.165.201.15:443/transportgateway/services/DeviceRequestHandler</pre> <p>or</p> <pre>Device(config-call-home-profile)# destination address http http://209.165.201.15:80/transportgateway/services/DeviceRequestHandler</pre> | Note Ensure the IP address or the fully qualified domain name (FQDN) in the destination URL matches the IP address or the FQDN as configured for the Satellite Name on the Cisco Smart Software Manager On-Prem. |
| Step 11 | <pre>destination preferred-msg-format {long-text short-text xml}</pre> <p>Example:</p> <pre>Device(config-call-home-profile)# destination preferred-msg-format xml</pre> | (Optional) Configures a preferred message format. The default is XML. |
| Step 12 | <pre>active</pre> <p>Example:</p> <pre>Device(config-call-home-profile)# active</pre> | Enables the destination profile. By default, a profile is enabled when it is created. |
| Step 13 | <pre>exit</pre> <p>Example:</p> <pre>Device(config-call-home-profile)# exit</pre> | Exits Call Home destination profile configuration mode and returns to Call Home configuration mode. |
| Step 14 | <pre>exit</pre> <p>Example:</p> <pre>Device(config-call-home)# exit</pre> | Exits Call Home configuration mode and returns to global configuration mode. |
| Step 15 | <pre>ip http client source-interface interface-type interface-number</pre> <p>Example:</p> <pre>Device(config)# ip http client source-interface Vlan100</pre> | Configures a source interface for the HTTP client. Note The ip http client source-interface interface-type interface-number command is mandatory for a vrf interface. |
| Step 16 | <pre>crypto pki trustpoint name</pre> <p>Example:</p> <pre>Device(config)# crypto pki trustpoint SLA-TrustPoint</pre> | (Optional) Declares the trustpoint and a given name and enters ca-trustpoint configuration mode. |
| Step 17 | <pre>revocation-check none</pre> <p>Example:</p> <pre>Device(ca-trustpoint)# revocation-check none</pre> | (Optional) Specifies that certificate checking is ignored. |
| Step 18 | <pre>end</pre> <p>Example:</p> <pre>Device(ca-trustpoint)# end</pre> | (Optional) Exits ca-trustpoint configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 19 | copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Configuring the License Level

This procedure is optional. You can use this procedure to :

- Downgrade or upgrade licenses.
- Enable or disable an evaluation or extension license
- Clear an upgrade license

The required license level(s) needs to be configured on the device before registering. The following are the license levels available for Cisco Catalyst 9000 Series Switches:

Base licenses

- Network Advantage

Add-on licenses—These can be subscribed for a fixed term of three, five, or seven years.

- DNA Advantage

To configure the license levels, follow this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | license boot level <i>license_level</i> Example: <pre>Device(config)# license boot level network-advantage</pre> | Activates the licenses on the switch. |
| Step 4 | exit Example: <pre>Device(config)# exit</pre> | Returns to the privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 5 | write memory Example: Device# write memory | Saves the license information on the switch. |
| Step 6 | show version Example: Device# show version <pre> Technology-package Current Type Next reboot Technology-package network-advantage Smart License network-advantage None Subscription Smart License None </pre> | Shows license-level information. |
| Step 7 | reload Example: Device# reload | Reloads the device. |

Registering a Device on CSSM

To register a device on CSSM, you must do the following tasks:

1. Generate a unique token from the CSSM.
2. Register the device with the generated token.

On successful registration, the device will receive an identity certificate. This certificate is saved on your device and automatically used for all future communications with Cisco. CSSM will attempt to renew the registration information every 30 days.

Additionally, license usage data is collected and a report is sent to you every month. If required, you can configure your Call Home settings to filter out sensitive information (like hostname, username and password) from the usage report.

Generating a New Token from CSSM

Tokens are generated to register new product instances to the virtual account.

Procedure

-
- Step 1** Log in to CSSM from <https://software.cisco.com/#>.

You must log in to the portal using the username and password provided by Cisco.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose the required virtual account.

Step 4 Click the **General** tab.


Step 5 Click **New Token**.

Cisco Software Central
> Smart Software Licensing

English [Change]
Hello

Smart Account Name
Feedback
Support
Help

Alerts
Inventory
License Conversion
Reports
Preferences
Satellites
Activity

Questions About Licensing?
Try our Virtual Assistant


Virtual Account:
Virtual Account 1

28 Major
9 Minor
Hide Alerts

General
Licenses
Product Instances
Event Log

Virtual Account

Description:
Account 1

Default Virtual Account:
No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

| Token | Expiration Date | Description | Export-Controlled | Created By | Actions |
|------------------------------|-----------------|-------------|-------------------|------------|---------|
| ZjgxNzdYjctOWRhMC00M2I0Lw== | Expired | Token 1 | Allowed | User 1 | Actions |
| ZTg2MjBjMzUIN2U0Ni00NDdkLw== | Expired | | Allowed | User 1 | Actions |

The **Create Registration Token** window is displayed.

Step 6 In the **Description** field, enter the token description.

Step 7 In the **Expire After** field, enter the number of days the token must be active.

Step 8 (Optional) In the **Max. Number of Uses** field, enter the maximum number of uses allowed after which the token expires.

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Virtual Account 1

Description :

Token 2

* Expire After:

30

Days

Max. Number of Uses:

Allow export-controlled functionality on the products registered with this token

Create Token

Cancel

Step 9 Check the **Allow export-controlled functionality on the products registered with this token** checkbox.

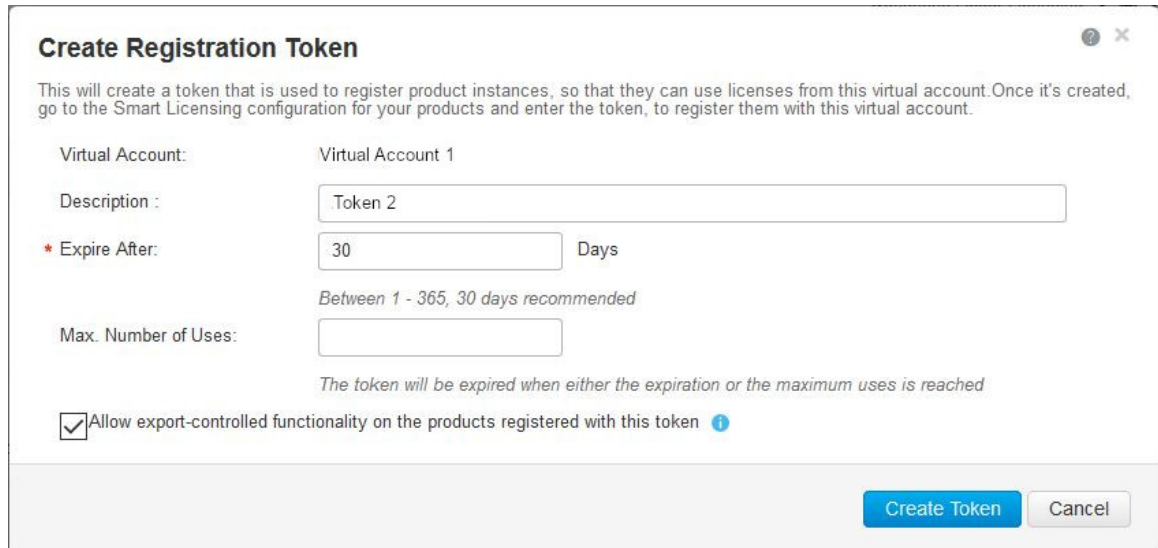
Enabling this checkbox ensures Cisco compliance with US and country-specific export policies and guidelines. For more information, see <https://www.cisco.com/c/en/us/about/legal/global-export-trade.html>.

Step 10

Click **Create Token** to create a token.

Step 11

After the token is created, click **Copy** to copy the newly created token.



Registering a Device with the New Token

To register a device with the new token, perform this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | license smart register idtoken <i>token_ID</i> Example: Device# license smart register idtoken \$T14ybnWpZPsldvUvE5anZ0RdalfBVe%0bIRmz0%30A | Registers the device with the back-end server using the token generated from CSSM. |
| Step 3 | write memory Example: Device# write memory | Saves the license information on the device. |

Verifying the License Status After Registration

To verify the status of a license after registration, use the **show license all** command.

Canceling a Device's Registration in CSSM

When your device is taken off the inventory, shipped elsewhere for redeployment, or returned to Cisco for replacement using the return merchandise authorization (RMA) process, you can use the **deregister** command to cancel the registration of your device.

To cancel device registration, follow this procedure:

Before you begin

Layer 3 connection to CSSM must be available to successfully deregister the device.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | license smart deregister Example: Device# license smart deregister | Cancels the device's registration, and sends the device into evaluation mode. All smart licensing entitlements and certificates on the corresponding platform are removed. The device product instance stored on CSSM is also removed. |

Monitoring Smart Licensing Configuration

Use the following commands in privileged EXEC mode to monitor smart licensing configuration.

Table 7: Commands to Monitor Smart Licensing Configuration

| Command | Purpose |
|----------------------------------|--|
| show license status | <p>Displays the compliance status of smart licensing. The following is the list of possible statuses:</p> <ul style="list-style-type: none"> • Enabled: Indicates that smart licensing is enabled. • Waiting: Indicates the initial state after your device has made a license entitlement request. The device establishes communication with Cisco and successfully registers itself with the CSSM. • Registered: Indicates that your device is able to communicate with the CSSM, and is authorized to initiate requests for license entitlements. • Authorized: Indicates that your device is in Compliance status and is authorized to use the requested type and count of licenses. The Authorization status has a lifetime of 90 days. At the end of 30 days, the device will send a new entitlement authorization request to the CSSM to renew the authorization. • Out Of Compliance: Indicates that one or more of your licenses are out of compliance. You must buy additional licenses. • Eval Mode: You must register the device with the CSSM within 90 days (of device usage). Otherwise, your device's evaluation period will expire. • Evaluation Period Expired: At the end of 90 days, if your device has not registered, the device enters Evaluation Expired mode. |
| show license all | Displays all the entitlements in use. Additionally, it shows the associated licensing certificates, compliance status, UDI, and other details. |
| show tech-support license | Displays the detailed debug output. |
| show license usage | Displays the license usage information. |

| Command | Purpose |
|-----------------------------|--|
| show license summary | Displays the summary of all the active licenses. |

Configuration Examples for Smart Licensing

The following sections provide various Smart Licensing configuration examples.

Example: Viewing the Call Home Profile

Example

To display the Call Home profile, use the **show call-home profile all** command:

```
Device> enable
Device# show call-home profile all
Profile Name: CiscoTAC-1
  Profile status: ACTIVE
  Profile mode: Full Reporting
  Reporting Data: Smart Call Home, Smart Licensing
  Preferred Message Format: xml
  Message Size Limit: 3145728 Bytes
  Transport Method: http
  HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
  Other address(es): default

Periodic configuration info message is scheduled every 1 day of the month at 09:15

Periodic inventory info message is scheduled every 1 day of the month at 09:00

Alert-group              Severity
-----
crash                    debug
diagnostic               minor
environment              warning
inventory                normal

Syslog-Pattern           Severity
-----
APF-.-WLC_.*            warning
.*                       major
```

Example: Registering a Device

Example

To register a device, use the **license smart register idtoken** command:

```
Device> enable
Device# license smart register idtoken
```

T14UytrNXBzbEs1ck8veUtWaG5abnZJOFdDa1FwbVRa%0Ab1RMbz0%3D%0A
 Device# write memory

Additional References

Related Documents

| Related Topic | Document Title |
|--------------------------------------|--|
| Cisco Smart Software Manager Help | Smart Software Manager Help |
| Cisco Smart Software Manager On-Prem | Cisco Smart Software Manager On-Prem |

Technical Assistance

| Description | Link |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | http://www.cisco.com/support |

Feature History for Smart Licensing

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|-----------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Smart Licensing | <p>A cloud-based, software license management solution that allows you to manage and track the status of your license, hardware, and software usage trends.</p> <p>Smart Licensing is the default and the only available method to manage licenses.</p> |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>



CHAPTER 5

Environmental Monitoring and Power Management

- [About Environmental Monitoring, on page 91](#)
- [Power Management , on page 97](#)
- [Configuration Examples for Operating States, on page 104](#)
- [Feature History for Environmental Monitoring and Power Management, on page 105](#)

About Environmental Monitoring

Environmental monitoring of chassis components provides early warning indications of possible component failure. This warning helps you to ensure the safe and reliable operation of your system and avoid network interruptions.

This section describes how to monitor critical system components so that you can identify and rapidly correct hardware-related problems.

Using CLI Commands to Monitor your Environment

Enter the **show environment** [**all** | **counters** | **history** | **location** | **sensor** | **status** | **summary** | **table**] command to display system status information. Keyword descriptions are listed in the following table.

Table 8: Keyword Descriptions

| Keyword | Purpose |
|-----------------|--|
| all | Displays a detailed listing of all the environmental monitor parameters (for example, the power supplies, temperature readings, voltage readings, and so on). This is the default. |
| counters | Displays operational counters. |
| history | Displays the sensor state change history. |
| location | Displays sensors by location. |
| sensor | Displays the sensor summary. |

| Keyword | Purpose |
|----------------|---|
| status | Displays field-replaceable unit (FRU) operational status and power and power supply fan sensor information. |
| summary | Displays the summary of all the environment monitoring sensors. |
| table | Displays a sensor state table. |

Displaying Environment Conditions

Supervisor modules and their associated line cards support multiple temperature sensors per card. The environment condition output includes the temperature reading from each sensor and the temperature thresholds for each sensor. These line cards support three thresholds: warning, critical, and shutdown.

The following example illustrates how to display the environment condition on a supervisor module. The thresholds appear within parentheses.

```
Device# show environment
```

```
Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0
```

| Slot | Sensor | Current State | Reading |
|---|----------------|---------------|--|
| Threshold(Minor, Major, Critical, Shutdown) | | | |
| ----- | | | |
| R0 | Temp: InltFrnt | Normal | 27 Celsius (45 ,50 ,55 ,60) (Celsius) |
| R0 | Temp: InltRear | Normal | 28 Celsius (45 ,50 ,55 ,60) (Celsius) |
| R0 | Temp: OtlFrnt | Normal | 35 Celsius (75 ,80 ,85 ,90) (Celsius) |
| R0 | Temp: OtlRear | Normal | 43 Celsius (75 ,80 ,85 ,90) (Celsius) |
| R0 | Temp: UADP_0_0 | Normal | 54 Celsius (105,110,120,124) (Celsius) |
| R0 | Temp: UADP_0_1 | Normal | 53 Celsius (105,110,120,124) (Celsius) |
| R0 | Temp: UADP_0_2 | Normal | 53 Celsius (105,110,120,124) (Celsius) |
| R0 | Temp: UADP_0_3 | Normal | 55 Celsius (105,110,120,124) (Celsius) |
| R0 | Temp: UADP_0_4 | Normal | 54 Celsius (105,110,120,124) (Celsius) |
| R0 | Temp: UADP_0_5 | Normal | 55 Celsius (105,110,120,124) (Celsius) |
| R0 | Temp: UADP_0_6 | Normal | 64 Celsius (105,110,120,124) (Celsius) |
| R0 | Temp: UADP_0_7 | Normal | 59 Celsius (105,110,120,124) (Celsius) |
| R0 | Temp: UADP_0_8 | Normal | 55 Celsius (105,110,120,124) (Celsius) |

<output truncated>

The following example illustrates how to display the LED status on a supervisor module.

```
Device# show hardware led
```

```
SWITCH: 1
SYSTEM: GREEN
```

```
Line Card : 1
PORT STATUS: (48) Fo1/0/1:BLACK Fo1/0/2:BLACK Fo1/0/3:BLACK Fo1/0/4:BLACK Fo1/0/5:BLACK
Fo1/0/6:BLACK Fo1/0/7:BLACK Fo1/0/8:BLACK Fo1/0/9:BLACK Fo1/0/10:BLACK Fo1/0/11:BLACK
Fo1/0/12:BLACK Fo1/0/13:BLACK Fo1/0/14:BLACK Fo1/0/15:BLACK Fo1/0/16:BLACK Fo1/0/17:BLACK
Fo1/0/18:BLACK Fo1/0/19:BLACK Fo1/0/20:BLACK Fo1/0/21:GREEN Fo1/0/22:BLACK Fo1/0/23:BLACK
Fo1/0/24:BLACK Hu1/0/25:GREEN Hu1/0/26:BLACK Hu1/0/27:BLACK Hu1/0/28:BLACK Hu1/0/29:BLACK
Hu1/0/30:BLACK Hu1/0/31:BLACK Hu1/0/32:BLACK Hu1/0/33:BLACK Hu1/0/34:BLACK Hu1/0/35:BLACK
Hu1/0/36:BLACK Hu1/0/37:BLACK Hu1/0/38:BLACK Hu1/0/39:BLACK Hu1/0/40:BLACK Hu1/0/41:BLACK
```

```
Hu1/0/42:BLACK Hu1/0/43:BLACK Hu1/0/44:BLACK Hu1/0/45:BLACK Hu1/0/46:BLACK Hu1/0/47:BLACK
Hu1/0/48:BLACK
BEACON: BLACK
STATUS: GREEN
```

Line Card : 2

```
PORT STATUS: (48) Fo2/0/1:BLACK Fo2/0/2:GREEN Fo2/0/3:GREEN Fo2/0/4:GREEN Fo2/0/5:GREEN
Fo2/0/6:GREEN Fo2/0/7:GREEN Fo2/0/8:GREEN Fo2/0/9:GREEN Fo2/0/10:GREEN Fo2/0/11:GREEN
Fo2/0/12:GREEN Fo2/0/13:GREEN Fo2/0/14:GREEN Fo2/0/15:GREEN Fo2/0/16:GREEN Fo2/0/17:GREEN
Fo2/0/18:GREEN Fo2/0/19:GREEN Fo2/0/20:GREEN Fo2/0/21:GREEN Fo2/0/22:GREEN Fo2/0/23:GREEN
Fo2/0/24:BLACK Hu2/0/25:BLACK Hu2/0/26:BLACK Hu2/0/27:BLACK Hu2/0/28:BLACK Hu2/0/29:BLACK
Hu2/0/30:BLACK Hu2/0/31:BLACK Hu2/0/32:BLACK Hu2/0/33:BLACK Hu2/0/34:BLACK Hu2/0/35:BLACK
Hu2/0/36:BLACK Hu2/0/37:BLACK Hu2/0/38:BLACK Hu2/0/39:BLACK Hu2/0/40:BLACK Hu2/0/41:BLACK
Hu2/0/42:BLACK Hu2/0/43:BLACK Hu2/0/44:BLACK Hu2/0/45:BLACK Hu2/0/46:BLACK Hu2/0/47:BLACK
Hu2/0/48:BLACK
BEACON: BLACK
STATUS: GREEN
```

```
MODULE: slot 3
SUPERVISOR: ACTIVE
PORT STATUS: (0)
BEACON: BLACK
STATUS: GREEN
SYSTEM: GREEN
ACTIVE: GREEN
```

```
MODULE: slot 4
SUPERVISOR: STANDBY
PORT STATUS: (0)
BEACON: BLACK
STATUS: GREEN
SYSTEM: GREEN
ACTIVE: AMBER
```

Line Card : 5

```
PORT STATUS: (48) Twe5/0/1:BLACK Twe5/0/2:GREEN Twe5/0/3:GREEN Twe5/0/4:GREEN Twe5/0/5:GREEN
Twe5/0/6:GREEN Twe5/0/7:GREEN Twe5/0/8:GREEN Twe5/0/9:GREEN Twe5/0/10:GREEN Twe5/0/11:GREEN
Twe5/0/12:GREEN Twe5/0/13:GREEN Twe5/0/14:GREEN Twe5/0/15:GREEN Twe5/0/16:GREEN
Twe5/0/17:GREEN Twe5/0/18:GREEN Twe5/0/19:GREEN Twe5/0/20:GREEN Twe5/0/21:GREEN
Twe5/0/22:GREEN Twe5/0/23:GREEN Twe5/0/24:GREEN Twe5/0/25:GREEN Twe5/0/26:GREEN
Twe5/0/27:GREEN Twe5/0/28:GREEN Twe5/0/29:GREEN Twe5/0/30:GREEN Twe5/0/31:GREEN
Twe5/0/32:GREEN Twe5/0/33:GREEN Twe5/0/34:GREEN Twe5/0/35:GREEN Twe5/0/36:GREEN
Twe5/0/37:GREEN Twe5/0/38:GREEN Twe5/0/39:GREEN Twe5/0/40:GREEN Twe5/0/41:GREEN
Twe5/0/42:GREEN Twe5/0/43:GREEN Twe5/0/44:GREEN Twe5/0/45:GREEN Twe5/0/46:GREEN
Twe5/0/47:BLACK Twe5/0/48:BLACK
BEACON: BLACK
STATUS: GREEN
```

Line Card : 6

```
PORT STATUS: (48) Twe6/0/1:BLACK Twe6/0/2:GREEN Twe6/0/3:GREEN Twe6/0/4:GREEN Twe6/0/5:GREEN
Twe6/0/6:GREEN Twe6/0/7:GREEN Twe6/0/8:GREEN Twe6/0/9:GREEN Twe6/0/10:GREEN Twe6/0/11:GREEN
Twe6/0/12:GREEN Twe6/0/13:GREEN Twe6/0/14:GREEN Twe6/0/15:GREEN Twe6/0/16:GREEN
Twe6/0/17:GREEN Twe6/0/18:GREEN Twe6/0/19:GREEN Twe6/0/20:GREEN Twe6/0/21:GREEN
Twe6/0/22:GREEN Twe6/0/23:GREEN Twe6/0/24:GREEN Twe6/0/25:GREEN Twe6/0/26:GREEN
Twe6/0/27:GREEN Twe6/0/28:GREEN Twe6/0/29:GREEN Twe6/0/30:GREEN Twe6/0/31:GREEN
Twe6/0/32:GREEN Twe6/0/33:GREEN Twe6/0/34:GREEN Twe6/0/35:GREEN Twe6/0/36:BLACK
Twe6/0/37:BLACK Twe6/0/38:BLACK Twe6/0/39:BLACK Twe6/0/40:GREEN Twe6/0/41:GREEN
Twe6/0/42:GREEN Twe6/0/43:GREEN Twe6/0/44:GREEN Twe6/0/45:GREEN Twe6/0/46:BLACK
Twe6/0/47:BLACK Twe6/0/48:BLACK
BEACON: BLACK
STATUS: GREEN
```

```
RJ45 CONSOLE: GREEN
```

Displaying On Board Failure Logging (OBFL) information

```
GigabitEthernet0/0 (MGMT): GREEN
TenGigabitEthernet0/1 (SFP MGMT): BLACK
FANTRAY STATUS: GREEN
FANTRAY BEACON: BLACK
```

Displaying On Board Failure Logging (OBFL) information

The OBFL feature records operating temperatures, hardware uptime, interrupts, and other important events and messages that can assist with diagnosing problems with line cards and supervisor modules installed in a switch. Data is logged to files stored in nonvolatile memory. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records. The OBFL feature provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the system. Data is recorded in one of two formats: continuous information that displays a snapshot of measurements and samples in a continuous file, and summary information that provides details about the data being collected. The data is displayed using the **show logging onboard** command. The message “No historical data to display” is seen when historical data is not available.

```
Device# show logging onboard RP active voltage detail
```

VOLTAGE SUMMARY INFORMATION

```
Number of sensors      : 33
```

| Sensor | ID | Normal Range | Maximum Sensor Value |
|--------------------|----|--------------|----------------------|
| CPU_P5V | 0 | 0 - 5 | 5 |
| CPU_P3V3 | 1 | 0 - 5 | 3 |
| CPU_P2V5_VPP | 2 | 0 - 5 | 2 |
| CPU_PVCCSCFUSESUS | 3 | 0 - 5 | 1 |
| CPU_PVCCIN | 4 | 0 - 5 | 1 |
| CPU_P1V5_PCH | 5 | 0 - 5 | 1 |
| CPU_PVCCKRHV | 6 | 0 - 5 | 1 |
| CPU_P1V2_VDDQ | 7 | 0 - 5 | 1 |
| CPU_P1V05_COMBINED | 8 | 0 - 5 | 1 |
| CPU_P0V6_VTT | 9 | 0 - 5 | 1 |
| BB_P1V0_BCM82752 | 10 | 0 - 5 | 3 |
| BB_P3V3_A | 11 | 0 - 5 | 12 |
| BB_P12V0 | 12 | 0 - 12 | 12 |
| BB_P7V0 | 13 | 0 - 7 | 7 |
| BB_P5V0 | 14 | 0 - 5 | 5 |
| BB_P1V5 | 15 | 0 - 5 | 3 |
| BB_P3V3 | 16 | 0 - 5 | 3 |
| BB_P2V5 | 17 | 0 - 5 | 2 |
| BB_P1V8 | 18 | 0 - 5 | 1 |
| BB_P0V9_DP0_PLL | 19 | 0 - 5 | 0 |
| BB_P0V9_DP1_PLL | 20 | 0 - 5 | 0 |
| BB_P0V9_DP2_PLL | 21 | 0 - 5 | 0 |
| BB_P0V8_DP0_VDD | 22 | 0 - 5 | 0 |
| BB_P0V8_DP1_VDD | 23 | 0 - 5 | 0 |
| BB_P0V8_DP2_VDD | 24 | 0 - 5 | 0 |
| BB_P0V9_DP0_AVDD | 25 | 0 - 5 | 0 |
| BB_P0V9_DP1_AVDD | 26 | 0 - 5 | 0 |
| BB_P0V9_DP2_AVDD | 27 | 0 - 5 | 1 |
| BB_P1V1_HATH | 28 | 0 - 5 | 1 |
| BB_P1V1_DP0_AVDDH | 29 | 0 - 5 | 1 |
| BB_P1V2_HATH | 30 | 0 - 5 | 3 |
| BB_3V3_IRC | 31 | 0 - 5 | 3 |

```

BB_P3V3_EUSB          32          0 - 5          0

-----
Sensor Value
Total Time of each Sensor
-----

value: 0
0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 61d, 94d, 577h, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 61d, 112d, 112d,
  112d, 112d, 112d, 112d, 112d, 112d, 50d, 0s, 0s, 0s, 0s, 112d,
value: 1
0s, 0s, 0s, 112d, 112d, 112d, 112d, 112d, 50d, 426h, 645h, 0s, 0s, 0s, 61d, 50d, 0s, 61d,
50d, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 61d, 112d, 112d, 50d, 0s, 0s,
value: 2
0s, 0s, 112d, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 61d, 50d, 0s, 0s, 0s, 0s,
  0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s,
value: 3
0s, 112d, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 61d, 50d, 0s, 0s, 0s, 61d, 50d, 0s, 0s, 0s, 0s,
  0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 61d, 112d, 0s,
value: 4
900h, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 160d, 43d, 0s, 0s, 0s, 0s, 0s, 0s,
  0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s, 0s,
value: 5
<output truncated>

```

Emergency Actions

The chassis can power down a single card, providing a detailed response to over-temperature conditions on line cards. However, the chassis cannot safely operate when the temperature of the supervisor module itself exceeds the critical threshold. The supervisor module turns off the chassis' power supplies to protect itself from overheating. When this happens, you can recover the switch only by cycling the power on and off switches on the power supplies or by cycling the AC or DC inputs to the power supplies.

Shutdown temperature emergencies on a supervisor will trigger chassis shutdown. Shutdown temperature emergencies on a linecard will shut down the linecard but not the chassis. Critical temperature emergencies will trigger a warning message and the fan will be at its highest speed, but the chassis will not shut down. This applies to all slots.

The following table lists temperature emergencies but does not distinguish between critical and shutdown emergencies.

Table 9: Emergency and Action

| | |
|--|--|
| Case 1. Complete fan failure emergency. | SYSLOG message displays and the chassis shuts down. |
| Case 2. Temperature emergency on a line card. | Power down the line card. |
| Case 3. Temperature emergency on a power supply. When the shutdown alarm threshold is exceeded, all the power supplies will shut down. | Power cycle the device to recover from power supply shut down. |
| Case 4. Temperature emergency on the active supervisor module. | Power down the chassis. |

System Alarms

Any system has two types of alarms: major and minor. A major alarm indicates a critical problem that could lead to system shutdown. A minor alarm is informational—it alerts you to a problem that could become critical if corrective action is not taken.

The following table lists the possible environment alarms.

Table 10: Possible Environmental Alarms

| | |
|--|-------|
| A temperature sensor over its warning threshold | minor |
| A temperature sensor over its critical threshold | major |
| A temperature sensor over its shutdown threshold | major |
| A partial fan failure | minor |
| A complete fan failure | major |
| Note A complete fan failure alarm does not result in system shutdown. | |

Fan failure alarms are issued as soon as the fan failure condition is detected and are canceled when the fan failure condition clears. Temperature alarms are issued as soon as the temperature reaches the threshold temperature. An LED on the supervisor module indicates whether an alarm has been issued.

When the system issues a major alarm, it starts a timer whose duration depends on the alarm. If the alarm is not canceled before the timer expires, the system takes emergency action to protect itself from the effects of overheating. The timer values and the emergency actions depend on the type of supervisor module.



Note Refer to the *Hardware Installation Guide* for information on LEDs, including the startup behavior of the supervisor module system LED.

Table 11: Alarms on Supervisor Module

| Event | Alarm Type | Supervisor LED Color | Description and Action |
|--|------------|----------------------|---|
| Card temperature exceeds the critical threshold. | Major | Red | Syslog message displays when the alarm is issued. |
| Card temperature exceeds the shutdown threshold. | Major | Red | Syslog message displays when the alarm is issued. |
| Chassis temperature exceeds the warning threshold. | Minor | Orange | Syslog message displays when the alarm is issued. |
| Chassis fan tray experiences partial failure. | Minor | Orange | Syslog message displays when the alarm is issued. |

| Event | Alarm Type | Supervisor LED Color | Description and Action |
|--|------------|----------------------|---|
| Chassis fan tray experiences complete failure. | Major | Red | Syslog message displays when the alarm is issued. |

Power Management

This section describes the power management feature in the Cisco Catalyst 9600 Series Switches and the aspects of power management that you can control and configure. For information about the hardware, including installation, removal and power supply specifications, see the *Cisco Catalyst 9600 Series Switches Hardware Installation Guide*.

Restrictions for Power Management

- When using an AC power source for the power supply modules, you cannot mix 110V and 220V inputs.
- When using a combination of AC and DC power sources for the power supply modules, the input voltage for all the power supply modules needs to be the same. The input voltage can either be 110V or 220V for all the power supply modules. This applies to both the combined mode and n+1 redundant power supply mode.

Power Supply Modes

Cisco Catalyst 9600 Series Switches offer combined and redundant configuration modes for power supplies.

Combined Mode

This is the default power supply mode.

The system operates on one to four power supplies. All available power supplies are active and sharing power and can operate at up to 100 percent capacity.

Available power in the combined mode is the sum of the individual power supplies.

Redundant Mode

In a redundant configuration, a given power supply module can be either active, or in standby mode, and switch to active when required.

You can configure an n+1 redundant mode.

- n+1 redundant Mode—n number of power supply modules are active (n can be one to seven power supply modules). +1 is the power supply module reserved for redundancy.

The default power supply slot is PS4.

Specify a standby slot, by entering the **power redundancy-mode redundant n+1 standby-PSslot** command.

Enter the **show power detail** command in privileged EXEC mode, to display detailed information about the currently configured power supply mode.

Operating States

The operating state refers to the system's capacity to respond to a situation where all active power supply modules fail. The system deems the chassis operating state as full protected, normal protected, or combined depending on these factors:

- Total active output power, which is the total output power that is available from all the active power supply modules in the chassis.
- Required budgeted power, which is the power the system requires only for the supervisor modules, switching modules (line cards), and fan tray to operate in the chassis.

In the **show** command outputs (**show power**, **show power detail**), this is displayed as `System Power`.

- Total standby output power, which is the total output power that is available from all the power supply modules in the chassis that are configured as standby.

Whether in the n+1, the system considers the chassis in a full protected state, when ALL of these conditions are met:

- Total active output power is greater than the required budgeted power
- Total standby output power is greater than or equal to total active output power

Whether in the n+1, the system considers the chassis in a normal protected state, when ALL of these conditions are met:

- Total active output power is greater than the required budgeted power
- Total standby output power is lesser than the total active output power

The system operates in a combined state, when it encounters these conditions (any redundancy configuration is rejected):

- Total active output power is lesser than the required budgeted power
- A standby power supply module is not configured or installed.

Information about the operating state is also displayed in the **show power** and **show power detail** command output.

Power Management Considerations

It is possible to configure a switch that requires more power than the power supplies provide.

The following list the conditions where the power requirements for the installed modules exceed the power provided by the power supplies.

- If the switch has a single power supply module that is unable to meet power requirements, the following error message is displayed:

`Insufficient power supplies present for specified configuration`

The **show power** command output will also indicate this state of insufficient input power.

- If the switch has more than one power supply module, and requirements for the installed modules still exceed the power provided by the power supplies, the following error message is displayed:

```
Insufficient number of power supplies (2) are installed for power redundancy mode
```

The **show power** command output will also indicate this state of insufficient input power.

If you attempt to insert additional modules into your switch and exceed the power supply, the switch immediately places the newly inserted module into reset mode, and the following error message is displayed:

```
Power doesn't meet minimum system power requirement.
```

Additionally, if you power down a functioning chassis and insert an additional linecard or change the module configuration so that the power requirements exceed the available power, one or more linecards enter reset mode when you power on the switch again.

Selecting a Power Supply Mode

Your switch hardware configuration dictates which power supply or supplies you should use. For example, if your switch configuration requires more power than a single power supply provides, use the [Cisco power calculator](#) on cisco.com to help determine the number of power supplies that is required for either combined or redundant mode.

Configuring the Redundant Mode

By default, the power supplies in the switch are set to operate in combined mode. To effectively use redundant mode, note the following:

- If you have the power supply mode set to redundant mode and only one power supply installed, your switch accepts the configuration but operates without redundancy.
- Choose a power supply module that is powerful enough to support the switch configuration.
- Use the [Cisco Power Calculator](#) to help assess the number of power supplies required by the system. Ensure that you install a sufficient number of power supply modules, so that the chassis and PoE requirements are less than the maximum available power. Power supplies automatically adjust the power resources at startup to accommodate the chassis and PoE requirements. Modules are brought up first, followed by IP phones.
- For optimal use of system power, choose power supply modules of the same capacity when configuring a redundant mode on the switch.

To configure redundant mode, perform this task:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: Device# configure terminal | Enters the global configuration mode. |
| Step 2 | power redundancy-mode redundant [n+1 standby-PSslot n+1 standby-PSslot] | power redundancy-mode redundant n+1 standby-PSslot —Configures the n+1 redundant |

| | Command or Action | Purpose |
|---------------|---|--|
| | Example: Device(config)# power redundancy-mode redundant n+1 4 | mode. Enter the standby power supply module slot number. In the n+1 example here, the power supply module in slot PS4 is the designated standby module and has been configured accordingly. Operational power supply modules installed in all other slots, are active. If you are using power supply modules of different capacities, you must configure the power supply module with the highest wattage or capacity as the standby for the n+1 redundant mode. |
| Step 3 | end Example: Device(config)# end | Exits global configuration mode. |
| Step 4 | show power Example: Device# show power | Displays the power redundancy mode information. |

Configuring the Combined Mode

To use the combined mode effectively, follow these guidelines:

- If you have the power supply mode set to combined mode and only one power supply installed, your switch accepts the configuration, but power is available from only one power supply.
- When your switch is configured to combined mode, available power is the sum of the individual power supplies

To configure combined mode on your switch, perform this task:

Before you begin

Note that this mode utilizes the available power from all the power supplies; however, your switch has no power redundancy.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters the global configuration mode. |
| Step 2 | power redundancy-mode combined Example: | Sets the power supply mode to combined mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Device(config)# power redundancy-mode combined | |
| Step 3 | end Example: Device(config)# end | Exits global configuration mode. |
| Step 4 | show power Example: Device# show power | Displays the power redundancy mode information. |

Power Budgeting for Supervisor Modules

The power budget, or required budgeted power, is the power the system **requires** and **reserves** for supervisor modules, switching modules (line cards), and the fan tray to operate in the chassis. In the **show power**, and **show power detail** command outputs, this is displayed as `System Power`. The system does not allow any part of this required budgeted power to be automatically redirected for use by other components in the system.

This section describes how power budgeting works with respect to supervisor modules and the configuration options that are available.

By default, the system reserves power for a redundant setup, to ensure high availability. This means that the system reserves the power required by both the supervisor modules in the chassis, as part of the required budgeted power (`System Power`).

You can also configure the system to reserve power for a single supervisor. This configuration option is suited to situations where a single supervisor is installed and the total available power is not sufficient to enable all line cards and PoE ports. In such a scenario, configuring the switch to reserve power for a single supervisor enables you to free-up power and use it for other components, such as PoE ports, or line cards instead.

Note the following restrictions and guidelines:

- If you have installed both supervisor modules, you cannot configure the power budget mode for a single supervisor. The system rejects the configuration and following message is displayed: `cannot enable single sup mode when remote supervisor is present.`
- If you have installed both supervisor modules and the default setting is effective, you must install the necessary number of power supply modules to meet overall system requirements (including line cards and fan tray). Do not remove the second supervisor to remedy a situation where there is an insufficient number of power supply modules.
- If you have installed a single supervisor module and configured the power budget mode for a single supervisor, and you install a second supervisor:
 - The system will reject the configuration, and allow the first supervisor to come up.
 - If this action is accompanied by a low power condition where the system does not have sufficient power, linecards maybe denied power.

For information about how to safely move from a single to a dual supervisor setup, see task *Moving from a Single to a Dual Supervisor Setup* below.

The following tasks describe the available configuration options:

Configuring the Power Budget Mode for a Single Supervisor

Beginning in the privileged EXEC mode, perform these steps to configure the power budget mode for a single supervisor setup:

Before you begin

Ensure that these prerequisites are met:

- You have installed only one supervisor module in the chassis.
- You have installed a blank in the second supervisor slot.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters the global configuration mode. |
| Step 2 | power budget mode {single-sup} Example: Device(config)# power budget mode single-sup | Reserves power for one supervisor module in the chassis. |
| Step 3 | end Example: Device(config)# end | Exits the global configuration mode. |

Moving from a Single to a Dual Supervisor Setup

Beginning in the privileged EXEC mode, perform these steps to move from single to a dual supervisor setup:

Before you begin

Calculate the required power for a dual supervisor setup. Cisco Power Calculator (CPC) enables you to calculate the power supply requirements for a specified configuration:

1. Go to <https://cpc.cloudapps.cisco.com/cpc> → **Launch Cisco Power Calculator**.
2. Select applicable values for the `Product Family`, `Chassis`, `Supervisor Engine` (both supervisor slots), `Input Voltage`, and `Line Card` fields. Click **Next** to display results.
3. In the results that are displayed, locate the `Configuration Details` section and note the `Output Power` for the supervisor module. This is the amount of spare power that must be available in the system to safely install the second supervisor.
4. Enter the **show power** command in privileged EXEC mode.

This command displays power supply configuration information.

In the output, check the difference between the `Total Maximum Available` and `Total Used`, this must be greater than what the CPC says in the `Output Power` column for the supervisor module. If this is the case, proceed with the task, if not, first install the required number of additional power supply modules.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: Device# <code>configure terminal</code> | Enters the global configuration mode. |
| Step 2 | no power budget mode {single-sup} Example: Device(config)# <code>no power budget mode single-sup</code> | Reverts to the default setting where the system reserves power for both the supervisor modules in the chassis. |
| Step 3 | end Example: Device(config)# <code>end</code> | Exits configuration mode. |
| Step 4 | Insert the second supervisor module in the supervisor slot. | For detailed steps, see the Supervisor Module Installation Note → Removal and Replacement Procedures, on cisco.com. |

Powering Down a Line Card

If your system does not have enough power for all modules installed in the switch, you can power down one or more line cards and place them in power-off mode.

To power down a line card, perform this task:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: Device# <code>configure terminal</code> | Enters the global configuration mode. |
| Step 2 | hw-module slot <i>card slot/slot number</i> shutdown unpowered Example: Device(config)# <code>hw-module slot 1/0 shutdown unpowered</code> | Powers down the specified module by placing it in low power mode. |
| Step 3 | end Example: | Exits the global configuration mode |

| | Command or Action | Purpose |
|--|------------------------------|---------|
| | Device (config) # end | |

Configuration Examples for Operating States

The examples in this section show how to view the operating states of the system.

show power

The following is sample output of the **show power** command.

```

Device# show power
Power
Supply      Model No          Type Capacity  Status      Fan States
-----
PS1         C9600-PWR-2KWAC   ac   2000 W     active      good good
PS2         C9600-PWR-2KWAC   ac   2000 W     active      good good
PS3         C9600-PWR-2KWAC   ac   2000 W     active      good good
PS4         C9600-PWR-2KWAC   ac   2000 W     active      good good

PS Current Configuration Mode : Combined
PS Current Operating State : none

Power supplies currently active : 4
Power supplies currently available : 4

Power Summary Maximum
(in Watts) Used Available
-----
System Power 2860 7820
-----
Total 2860 7820

```

show power detail

The **show power detail** command includes the output of **show power** and **show power module** command in privileged EXEC mode.

```

Device# show power detail
Power
Supply      Model No          Type Capacity  Status      Fan States
-----
PS1         C9600-PWR-2KWAC   AC    2000 W     active      good good good good
PS2         C9600-PWR-2KWAC   AC    2000 W     active      good good good good
PS3         C9600-PWR-2KWAC   AC    2000 W     active      good good good good
PS4         C9600-PWR-2KWAC   AC    2100 W     active      good good good good

PS Current Configuration Mode : Combined
PS Current Operating State : none

Power supplies currently active : 4
Power supplies currently available : 4

Power Summary          Maximum
(in Watts)      Used      Available
-----

```

```

System Power    2860    7820
-----
Total           2860    7820

```

Power Budget Mode : Dual Sup

| Mod | Model No | Priority | Power State | Budget | Instantaneous | Peak | Out of Reset | In Reset |
|-----|---------------|----------|----------------|--------|---------------|------|-----------------|-------------|
| 1 | C9600-LC-24C | 0 | accepted | 200 | 0 | 0 | 200 | 10 |
| 2 | C9600-LC-48YL | 1 | accepted | 230 | 0 | 0 | 230 | 10 |
| 3 | C9600-SUP-1 | 0 | accepted | 775 | 0 | 0 | 775 | 202 |
| 4 | C9600-SUP-1 | 0 | accepted | 775 | 0 | 0 | 775 | 202 |
| 5 | C9600-LC-48YL | 2 | accepted | 230 | 0 | 0 | 230 | 10 |
| 6 | C9600-LC-24C | 3 | accepted | 200 | 0 | 0 | 200 | 10 |
| FM1 | C9606-FAN | | accepted | 450 | -- | -- | 450 | -- |

Total allocated power: 2860

Total required power: 2860

Feature History for Environmental Monitoring and Power Management

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | Environmental Monitoring and Power Management | Environmental monitoring of chassis components provides early warning indications of possible component failure. This warning helps you to ensure the safe and reliable operation of your system and avoid network interruptions. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 6

Configuring SDM Templates

- [Information About SDM Templates, on page 107](#)
- [SDM Templates and Switch Stacks, on page 107](#)
- [How to Configure SDM Templates, on page 108](#)
- [Monitoring and Maintaining SDM Templates, on page 109](#)
- [Configuration Examples for SDM Templates, on page 109](#)
- [Additional References for SDM Templates, on page 112](#)
- [Feature History for SDM Templates, on page 113](#)

Information About SDM Templates

You can use SDM templates to configure system resources to optimize support for specific features, depending on how your device is used in the network. You can select a template to provide maximum system usage for some functions.

Cisco Catalyst 9600 Series Switches support the following templates:

- Core
- SDA
- NAT
- Distribution

After you change the template and the system reboots, you can use the **show sdm prefer** privileged EXEC command to verify the new template configuration. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

SDM Templates and Switch Stacks

In a switch stack, all stack members must use the same SDM template that is stored on the active switch. When a new switch is added to a stack, the SDM configuration that is stored on the active switch overrides the template configured on an individual switch.

You can use the **show switch** privileged EXEC command to see if any stack members are in SDM mismatch mode.

How to Configure SDM Templates

Setting the SDM Template

Follow these steps to use the SDM template to maximize feature usage:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | sdm prefer { core nat sda distribution } Example: Device(config)# sdm prefer nat | Specifies the SDM template to be used on the switch. The keywords have these meanings: <ul style="list-style-type: none"> • core —Sets the Core template. • nat —Maximizes the NAT configuration on the switch. • sda —Sets the SDA template. • distribution —Sets the Distribution template. <p>Note The no sdm prefer command and a default template is not supported.</p> |
| Step 4 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 5 | reload Example: Device# reload | Reloads the operating system. After the system reboots, you can use the show sdm prefer privileged EXEC command to verify the new template configuration. If you enter the show sdm prefer command before |

| | Command or Action | Purpose |
|--|-------------------|---|
| | | you enter the reload privileged EXEC command, the show sdm prefer command shows the template currently in use and the template that will become active after a reload. |

Monitoring and Maintaining SDM Templates

| Command | Purpose |
|-----------------|---|
| show sdm prefer | Displays the SDM template in use. |
| reload | Reloads the switch to activate the newly configured SDM template. |



Note The SDM templates contain only those commands that are defined as part of the templates. If a template enables another related command that is not defined in the template, then this other command will be visible when the **show running config** command is entered. For example, if the SDM template enables the **switchport voice vlan** command, then the **spanning-tree portfast edge** command may also be enabled (although it is not defined on the SDM template).

If the SDM template is removed, then other such related commands are also removed and have to be reconfigured explicitly.

Configuration Examples for SDM Templates

Examples: Displaying SDM Templates

The following example output shows the core template information:

```
Device# show sdm prefer core
This is the Core template.
Security Ingress IPv4 Access Control Entries*: 7168 (current) - 7168 (proposed)
Security Ingress Non-IPv4 Access Control Entries*: 5120 (current) - 5120 (proposed)
Security Egress IPv4 Access Control Entries*: 7168 (current) - 7168 (proposed)
Security Egress Non-IPv4 Access Control Entries*: 8192 (current) - 8192 (proposed)
QoS Ingress IPv4 Access Control Entries*: 5632 (current) - 5632 (proposed)
QoS Ingress Non-IPv4 Access Control Entries*: 2560 (current) - 2560 (proposed)
QoS Egress IPv4 Access Control Entries*: 6144 (current) - 6144 (proposed)
QoS Egress Non-IPv4 Access Control Entries*: 2048 (current) - 2048 (proposed)
Netflow Input Access Control Entries*: 1024 (current) - 1024 (proposed)
Netflow Output Access Control Entries*: 1024 (current) - 1024 (proposed)
Flow SPAN Input Access Control Entries*: 512 (current) - 512 (proposed)
Flow SPAN Output Access Control Entries*: 512 (current) - 512 (proposed)
Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 768
Overflow L2 Multicast entries: 2304
```

```

L3 Multicast entries: 32768
Overflow L3 Multicast entries: 768
Ipv4/Ipv6 shared unicast routes: 212992
Overflow shared unicast routes: 1536
Policy Based Routing ACEs / NAT ACEs: 3072
Tunnels: 2816
LISP Instance Mapping Entries: 512
Control Plane Entries: 1024
Input Netflow flows: 32768
Output Netflow flows: 32768
SGT/DGT (or) MPLS VPN entries: 32768
SGT/DGT (or) MPLS VPN Overflow entries: 768
Wired clients: 2048
MACSec SPD Entries: 256
MPLS L3 VPN VRF: 1024
MPLS Labels: 45056
MPLS L3 VPN Routes VRF Mode: 209920
MPLS L3 VPN Routes Prefix Mode: 32768
MVPN MDT Tunnels: 1024
L2 VPN EOMPLS Attachment Circuit: 1024
MAX VPLS Bridge Domains : 1000
MAX VPLS Peers Per Bridge Domain: 128
MAX VPLS/VPWS Pseudowires : 16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cl

```

The following example output shows the NAT template information:

Device# **show sdm prefer nat**

This is the NAT template.

```

Security Ingress IPv4 Access Control Entries*: 7168 (current) - 7168 (proposed)
Security Ingress Non-IPv4 Access Control Entries*: 5120 (current) - 5120 (proposed)
Security Egress IPv4 Access Control Entries*: 3072 (current) - 3072 (proposed)
Security Egress Non-IPv4 Access Control Entries*: 5120 (current) - 5120 (proposed)
QoS Ingress IPv4 Access Control Entries*: 2560 (current) - 2560 (proposed)
QoS Ingress Non-IPv4 Access Control Entries*: 1536 (current) - 1536 (proposed)
QoS Egress IPv4 Access Control Entries*: 3072 (current) - 3072 (proposed)
QoS Egress Non-IPv4 Access Control Entries*: 1024 (current) - 1024 (proposed)
Netflow Input Access Control Entries*: 1024 (current) - 1024 (proposed)
Netflow Output Access Control Entries*: 1024 (current) - 1024 (proposed)
Flow SPAN Input Access Control Entries*: 512 (current) - 512 (proposed)
Flow SPAN Output Access Control Entries*: 512 (current) - 512 (proposed)
Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 768
Overflow L2 Multicast entries: 2304
L3 Multicast entries: 32768
Overflow L3 Multicast entries: 768
Ipv4/Ipv6 shared unicast routes: 212992
Overflow shared unicast routes: 1536
Policy Based Routing ACEs / NAT ACEs: 15872
Tunnels: 1792
LISP Instance Mapping Entries: 1024
Control Plane Entries: 1024
Input Netflow flows: 32768
Output Netflow flows: 32768
SGT/DGT (or) MPLS VPN entries: 32768
SGT/DGT (or) MPLS VPN Overflow entries: 768
Wired clients: 2048
MACSec SPD Entries: 256
MPLS L3 VPN VRF: 1024
MPLS Labels: 45056
MPLS L3 VPN Routes VRF Mode: 209920
MPLS L3 VPN Routes Prefix Mode: 32768
MVPN MDT Tunnels: 1024

```

```

L2 VPN EOMPLS Attachment Circuit:          1024
MAX VPLS Bridge Domains :                  1000
MAX VPLS Peers Per Bridge Domain:          128
MAX VPLS/VPWS Pseudowires :                16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli

```

The following example output shows the SDA template information:

```

Device# show sdm prefer sda
This is the SDA template.
Security Ingress IPv4 Access Control Entries*: 2048 (current) - 2048 (proposed)
Security Ingress Non-IPv4 Access Control Entries*: 3072 (current) - 3072 (proposed)
Security Egress IPv4 Access Control Entries*: 16384 (current) - 16384 (proposed)
Security Egress Non-IPv4 Access Control Entries*: 6144 (current) - 6144 (proposed)
QoS Ingress IPv4 Access Control Entries*: 5632 (current) - 5632 (proposed)
QoS Ingress Non-IPv4 Access Control Entries*: 2560 (current) - 2560 (proposed)
QoS Egress IPv4 Access Control Entries*: 6144 (current) - 6144 (proposed)
QoS Egress Non-IPv4 Access Control Entries*: 2048 (current) - 2048 (proposed)
Netflow Input Access Control Entries*: 1024 (current) - 1024 (proposed)
Netflow Output Access Control Entries*: 1024 (current) - 1024 (proposed)
Flow SPAN Input Access Control Entries*: 512 (current) - 512 (proposed)
Flow SPAN Output Access Control Entries*: 512 (current) - 512 (proposed)
Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 768
Overflow L2 Multicast entries: 2304
L3 Multicast entries: 32768
Overflow L3 Multicast entries: 768
Ipv4/Ipv6 shared unicast routes: 212992
Overflow shared unicast routes: 1536
Policy Based Routing ACEs / NAT ACEs: 2048
Tunnels: 2816
LIISP Instance Mapping Entries: 2048
Control Plane Entries: 1024
Input Netflow flows: 32768
Output Netflow flows: 32768
SGT/DGT (or) MPLS VPN entries: 32768
SGT/DGT (or) MPLS VPN Overflow entries: 768
Wired clients: 2048
MACSec SPD Entries: 256
MPLS L3 VPN VRF: 1024
MPLS Labels: 45056
MPLS L3 VPN Routes VRF Mode: 209920
MPLS L3 VPN Routes Prefix Mode: 32768
MVPN MDT Tunnels: 1024
L2 VPN EOMPLS Attachment Circuit: 1024
MAX VPLS Bridge Domains : 1000
MAX VPLS Peers Per Bridge Domain: 128
MAX VPLS/VPWS Pseudowires : 16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli

```

The following example output shows the distribution template information:

```

Device# show sdm prefer distribution
This is the Distribution template.
Security Ingress IPv4 Access Control Entries*: 7168 (current) - 7168 (proposed)
Security Ingress Non-IPv4 Access Control Entries*: 5120 (current) - 5120 (proposed)
Security Egress IPv4 Access Control Entries*: 7168 (current) - 7168 (proposed)
Security Egress Non-IPv4 Access Control Entries*: 8192 (current) - 8192 (proposed)
QoS Ingress IPv4 Access Control Entries*: 5632 (current) - 5632 (proposed)
QoS Ingress Non-IPv4 Access Control Entries*: 2560 (current) - 2560 (proposed)
QoS Egress IPv4 Access Control Entries*: 6144 (current) - 6144 (proposed)

```

```

QoS Egress Non-IPv4 Access Control Entries*:      2048 (current) - 2048 (proposed)
Netflow Input Access Control Entries*:            1024 (current) - 1024 (proposed)
Netflow Output Access Control Entries*:           1024 (current) - 1024 (proposed)
Flow SPAN Input Access Control Entries*:          512 (current) - 512 (proposed)
Flow SPAN Output Access Control Entries*:         512 (current) - 512 (proposed)
Number of VLANs:                                4094
Unicast MAC addresses:                           81920
Overflow Unicast MAC addresses:                    768
Overflow L2 Multicast entries:                     2304
L3 Multicast entries:                             16384
Overflow L3 Multicast entries:                     768
Ipv4/Ipv6 shared unicast routes:                  114688
Overflow shared unicast routes:                    1536
Policy Based Routing ACEs / NAT ACEs:              3072
Tunnels:                                           2816
LISP Instance Mapping Entries:                     1024
Control Plane Entries:                            1024
Input Netflow flows:                              49152
Output Netflow flows:                             49152
SGT/DGT (or) MPLS VPN entries:                    32768
SGT/DGT (or) MPLS VPN Overflow entries:            768
Wired clients:                                    2048
MACSec SPD Entries:                               256
MPLS L3 VPN VRF:                                  1024
MPLS Labels:                                       45056
MPLS L3 VPN Routes VRF Mode:                      112640
MPLS L3 VPN Routes Prefix Mode:                   32768
MVPN MDT Tunnels:                                 1024
L2 VPN EOMPLS Attachment Circuit:                 1024
MAX VPLS Bridge Domains :                          1000
MAX VPLS Peers Per Bridge Domain:                  128
MAX VPLS/VPWS Pseudowires :                       16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli

```

Examples: Configuring SDM Templates

```

Device(config)# sdm prefer distribution
Device(config)# exit
Device# reload
Proceed with reload? [confirm]

```

Additional References for SDM Templates

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

Feature History for SDM Templates

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|--------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | SDM Template | Standard SDM templates can be used to configure system resources to optimize support for specific features. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 7

Configuring System Message Logs

- [Information About Configuring System Message Logs, on page 115](#)
- [How to Configure System Message Logs, on page 118](#)
- [Monitoring and Maintaining System Message Logs, on page 125](#)
- [Configuration Examples for System Message Logs, on page 125](#)
- [Additional References for System Message Logs, on page 126](#)
- [Feature History for System Message Logs, on page 126](#)

Information About Configuring System Message Logs

System Message Logging

By default, a switch sends the output from system messages and **debug** privileged EXEC commands to a logging process. Member switches in a stack can trigger system messages. A member switch that generates a system message appends its hostname in the form of hostname-n, where n is a switch , and redirects the output to the logging process on the active switch . Though the active switch is a stack member, it does not append its hostname to system messages. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the active consoles after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management. For information on possible messages, see the system message guide for this release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer on a standalone switch, and in the case of a switch stack, on the active switch . If a standalone switch or the active switch fails, the log is lost unless you had saved it to flash memory.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet, through the console port, or through the Ethernet management port. In a switch stack, all member switch consoles provide the same console output.



Note The syslog format is compatible with 4.3 BSD UNIX.

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Depending on the switch, messages appear in one of these formats:

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

The part of the message preceding the percent sign depends on the setting of these global configuration commands:

- **service sequence-numbers**
- **service timestamps log datetime**
- **service timestamps log datetime [localtime] [msec] [show-timezone]**
- **service timestamps log uptime**

Table 12: System Log Message Elements

| Element | Description |
|---|--|
| <i>seq no:</i> | Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured. |
| <i>timestamp</i> formats: <i>mm/dd h h:mm:ss</i> or <i>hh:mm:ss</i> (short uptime) or <i>d h</i> (long uptime) | Date and time of the message or event. This information appears only if the service timestamps log [datetime log] global configuration command is configured. |
| <i>facility</i> | The facility to which the message refers (for example, SNMP, SYS, and so forth). |
| <i>severity</i> | Single-digit code from 0 to 7 that is the severity of the message. |
| <i>MNEMONIC</i> | Text string that uniquely describes the message. |
| <i>description</i> | Text string containing detailed information about the event being reported. |

Default System Message Logging Settings

Table 13: Default System Message Logging Settings

| Feature | Default Setting |
|---------------------------------------|------------------------|
| System message logging to the console | Enabled. |
| Console severity | Debugging. |
| Logging file configuration | No filename specified. |
| Logging buffer size | 4096 bytes. |
| Logging history size | 1 message. |
| Time stamps | Disabled. |
| Synchronous logging | Disabled. |
| Logging server | Disabled. |
| Syslog server IP address | None configured. |
| Server facility | Local7 |
| Server severity | Informational. |

Syslog Message Limits

If you enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** global configuration command, you can change the level of messages sent and stored in the switch history table. You also can change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels are stored in the history table even if syslog traps are not enabled.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

The history table lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, *emergencies* equal 1, not 0, and *critical* equals 3, not 2.

How to Configure System Message Logs

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

This task is optional.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | logging buffered <i>[size]</i> Example: Device(config)# logging buffered 8192 | <p>Logs messages to an internal buffer on the switch or on a standalone switch or, in the case of a switch stack, on the active switch.. The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes.</p> <p>If a standalone switch or the active switch fails, the log file is lost unless you previously saved it to flash memory. See Step 4.</p> <p>Note Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should <i>not</i> be set to this amount.</p> |
| Step 3 | logging <i>host</i> Example: Device(config)# logging 125.1.1.100 | <p>Logs messages to a UNIX syslog server host.</p> <p><i>host</i> specifies the name or IP address of the host to be used as the syslog server.</p> <p>To build a list of syslog servers that receive logging messages, enter this command more than once.</p> |
| Step 4 | end Example: | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Device(config)# end | |
| Step 5 | terminal monitor Example: Device# terminal monitor | Logs messages to a nonconsole terminal during the current session. Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages. |

Synchronizing Log Messages

You can synchronize unsolicited messages and **debug** privileged EXEC command output with solicited device output and prompts for a specific console port line or virtual terminal line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also configure the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and **debug** command output is enabled, unsolicited device output appears on the console or printed after solicited device output appears or is printed. Unsolicited messages and **debug** command output appears on the console after the prompt for user input is returned. Therefore, unsolicited messages and **debug** command output are not interspersed with solicited device output and prompts. After the unsolicited messages appear, the console again displays the user prompt.

This task is optional.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | line [console vty] line-number [ending-line-number] Example: Device(config)# line console | Specifies the line to be configured for synchronous logging of messages. <ul style="list-style-type: none"> • console—Specifies configurations that occur through the switch console port or the Ethernet management port. • line vty line-number—Specifies which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet session. The range of line numbers is from 0 to 15. |

| | Command or Action | Purpose |
|---------------|--|---|
| | | <p>You can change the setting of all 16 vty lines at once by entering:</p> <pre>line vty 0 15</pre> <p>You can also change the setting of the single vty line being used for your current connection. For example, to change the setting for vty line 2, enter:</p> <pre>line vty 2</pre> <p>When you enter this command, the mode changes to line configuration.</p> |
| Step 3 | <p>logging synchronous [level [<i>severity-level</i> all] limit <i>number-of-buffers</i>]</p> <p>Example:</p> <pre>Device(config)# logging synchronous level 3 limit 1000</pre> | <p>Enables synchronous logging of messages.</p> <ul style="list-style-type: none"> • (Optional) level <i>severity-level</i>—Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers mean greater severity and high numbers mean lesser severity. The default is 2. • (Optional) level all—Specifies that all messages are printed asynchronously regardless of the severity level. • (Optional) limit <i>number-of-buffers</i>—Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The range is 0 to 2147483647. The default is 20. |
| Step 4 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |

Disabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Disabling the logging process can slow down the switch because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press **Return**.

To reenable message logging after it has been disabled, use the **logging on** global configuration command.

This task is optional.

Procedure

| | Command or Action | Purpose |
|---------------|---|-----------------------------------|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | no logging console Example: Device(config)# no logging console | Disables message logging. |
| Step 3 | end Example: Device(config)# end | Returns to privileged EXEC mode. |

Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time-stamped.

This task is optional.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | Use one of these commands: <ul style="list-style-type: none"> • service timestamps log uptime • service timestamps log datetime[msec localtime show-timezone] Example: | Enables log time stamps. <ul style="list-style-type: none"> • log uptime—Enables time stamps on log messages, showing the time since the system was rebooted. • log datetime—Enables time stamps on log messages. Depending on the options |

| | Command or Action | Purpose |
|---------------|---|--|
| | <pre>Device(config)# service timestamps log uptime</pre> <p>or</p> <pre>Device(config)# service timestamps log datetime</pre> | selected, the time stamp can include the date, time in milliseconds relative to the local time zone, and the time zone name. |
| Step 3 | <pre>end</pre> <p>Example:</p> <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |

Enabling and Disabling Sequence Numbers in Log Messages

If there is more than one log message with the same time stamp, you can display messages with sequence numbers to view these messages. By default, sequence numbers in log messages are not displayed.

This task is optional.

Procedure

| | Command or Action | Purpose |
|---------------|--|-----------------------------------|
| Step 1 | <pre>configure terminal</pre> <p>Example:</p> <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 2 | <pre>service sequence-numbers</pre> <p>Example:</p> <pre>Device(config)# service sequence-numbers</pre> | Enables sequence numbers. |
| Step 3 | <pre>end</pre> <p>Example:</p> <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |

Defining the Message Severity Level

Limit messages displayed to the selected device by specifying the severity level of the message.

This task is optional.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | logging console <i>level</i> Example: Device(config)# logging console 3 | Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels. |
| Step 3 | logging monitor <i>level</i> Example: Device(config)# logging monitor 3 | Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels. |
| Step 4 | logging trap <i>level</i> Example: Device(config)# logging trap 3 | Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels. |
| Step 5 | end Example: Device(config)# end | Returns to privileged EXEC mode. |

Limiting Syslog Messages Sent to the History Table and to SNMP

This task explains how to limit syslog messages that are sent to the history table and to SNMP.

This task is optional.

Procedure

| | Command or Action | Purpose |
|---------------|---|-----------------------------------|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | logging history <i>level</i> Example: <pre>Device(config)# logging history 3</pre> | <p>Changes the default level of syslog messages stored in the history file and sent to the SNMP server.</p> <p>By default, warnings, errors, critical, alerts, and emergencies messages are sent.</p> |
| Step 3 | logging history size <i>number</i> Example: <pre>Device(config)# logging history size 200</pre> | <p>Specifies the number of syslog messages that can be stored in the history table.</p> <p>The default is to store one message. The range is 0 to 500 messages.</p> |
| Step 4 | end Example: <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |

Logging Messages to a UNIX Syslog Daemon

This task is optional.



Note Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

Before you begin

- Log in as root.
- Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | <p>Add a line to the file /etc/syslog.conf.</p> <p>Example:</p> <pre>local7.debug /usr/adm/logs/cisco.log</pre> | <ul style="list-style-type: none"> • local7—Specifies the logging facility. • debug—Specifies the syslog level. The file must already exist, and the syslog daemon must have permission to write to it. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | <p>Enter these commands at the UNIX shell prompt.</p> <p>Example:</p> <pre>\$ touch /var/log/cisco.log \$ chmod 666 /var/log/cisco.log</pre> | Creates the log file. The syslog daemon sends messages at this level or at a more severe level to this file. |
| Step 3 | <p>Make sure the syslog daemon reads the new changes.</p> <p>Example:</p> <pre>\$ kill -HUP `cat /etc/syslog.pid`</pre> | For more information, see the man syslog.conf and man syslogd commands on your UNIX system. |

Monitoring and Maintaining System Message Logs

Monitoring Configuration Archive Logs

| Command | Purpose |
|---|--|
| show archive log config {all number [end-number] user username [session number] number [end-number] statistics} [provisioning] | Displays the entire configuration log or the log for specified parameters. |

Configuration Examples for System Message Logs

Example: Switch System Message

This example shows a partial switch system message on a switch:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Additional References for System Message Logs

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

Feature History for System Message Logs

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|---------------------|--|
| Cisco IOS XE Gibraltar 16.11.1 | System Message Logs | A switch sends the output from system messages to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 8

Configuring Online Diagnostics

- [Information About Configuring Online Diagnostics, on page 127](#)
- [How to Configure Online Diagnostics, on page 129](#)
- [Monitoring and Maintaining Online Diagnostics, on page 130](#)
- [Configuration Examples for Online Diagnostic Tests, on page 130](#)
- [Additional References for Online Diagnostics, on page 131](#)
- [Feature Information for Configuring Online Diagnostics, on page 131](#)

Information About Configuring Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the device while the device is connected to a live network. The online diagnostics contain packet switching tests that check different hardware components and verify the data path and the control signals.

The online diagnostics detect problems in these areas:

- Hardware components
- Interfaces (Ethernet ports and so forth)
- Solder joints

Online diagnostics are categorized as on-demand, scheduled, or health-monitoring diagnostics. On-demand diagnostics run from the CLI; scheduled diagnostics run at user-designated intervals or at specified times when the device is connected to a live network; and health-monitoring runs in the background with user-defined intervals. The health-monitoring test runs for every 90, 100, or 150 seconds based on the test.

After you configure online diagnostics, you can manually start diagnostic tests or display the test results. You can also see which tests are configured for the device or switch stack and the diagnostic tests that have already run.

Generic Online Diagnostics (GOLD)



Note

- Before you enable online diagnostics tests, enable console logging to see all the warning messages.
- While tests are running, all the ports are shut down because a stress test is being performed with looping ports internally and external traffic might affect the test results. The switch must be rebooted to bring the switch to normal operation. When you issue the command to reload a switch, the system will ask you if the configuration should be saved. Do not save the configuration.
- If you are running the tests on other modules, after a test is initiated and complete, you must reset the module.

TestPortTxMonitoring

This test periodically monitors data-path traffic in the transmitted direction of each network port that is physically connected to a device with status as UP. This test is completed within a millisecond per port. This test also monitors the transmit counters at the ASIC level to verify that the ports are not stuck. The test displays syslog messages, and users can take corrective actions using the Cisco IOS Embedded Event Manager (EEM).

Configure the time interval and threshold by entering the **diagnostic monitor interval** and **diagnostic monitor threshold** commands, respectively. The test leverages the Cisco Discovery Protocol (CDP) protocol that transmits packets. The test runs every 75 seconds, and the failure threshold is set to five by default.

| Attribute | Description |
|-----------------------------|--|
| Disruptive or Nondisruptive | Nondisruptive. |
| Recommendation | Do not disable. |
| Default | On. |
| Corrective action | Displays a syslog message indicating that a port has failed. |
| Hardware support | All modules, including supervisor engines. |

TestUnusedPortLoopback

This test periodically verifies the data path between the supervisor module and network ports of a module during runtime to determine if any incoming network interface ports are locked. In this test, a Layer 2 packet is flooded on to the VLAN associated with the test port and the inband port of the supervisor engine. The packet loops back into the test port and returns to the supervisor engine on the same VLAN. This test runs only on unused (admin down, that is, the ports are shut down) network ports irrespective of whether a cable is connected or not, and completes within a millisecond per port. This test substitutes the lack of a nondisruptive loopback test in current ASICs, and test runs every 60 seconds.

| Attribute | Description |
|-----------------------------|----------------|
| Disruptive or Nondisruptive | Nondisruptive. |

| Attribute | Description |
|-------------------|---|
| Recommendation | Do not disable. This test is automatically disabled during CPU-usage spikes to maintain accuracy. |
| Default | On. |
| Corrective action | Displays a syslog message indicating that a port has failed. In modules other than supervisor engines, if all port groups fail (for example, at least one port per port ASIC fails more than the failure threshold for all port ASICs), the default action is to reset the module and power down the module after two resets. |
| Hardware support | All modules, including supervisor engines. |

How to Configure Online Diagnostics

Starting Online Diagnostic Tests

After you configure diagnostic tests to run on the device, use the **diagnostic start** privileged EXEC command to begin diagnostic testing.

After starting the tests, you cannot stop the testing process.

Use this privileged EXEC command to manually start online diagnostic testing:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | diagnostic start module <i>number</i> test {<i>name</i> <i>test-id</i> <i>test-id-range</i> all basic complete minimal non-disruptive per-port} Example: <pre>Device# diagnostic start module 2 test basic</pre> | <p>Starts the diagnostic tests.</p> <p>The switch <i>number</i> keyword is supported only on stacking device.</p> <p>You can specify the tests by using one of these options:</p> <ul style="list-style-type: none"> • <i>name</i>—Enters the name of the test. • <i>test-id</i>—Enters the ID number of the test. • <i>test-id-range</i>—Enters the range of test IDs by using integers separated by a comma and a hyphen. • <i>all</i>—Starts all of the tests. • <i>basic</i>— Starts the basic test suite. • <i>complete</i>—Starts the complete test suite. |

| | Command or Action | Purpose |
|--|-------------------|--|
| | | <ul style="list-style-type: none"> • minimal—Starts the minimal bootup test suite. • non-disruptive—Starts the non-disruptive test suite. • per-port—Starts the per-port test suite. |

Configuring Online Diagnostics

You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.

Monitoring and Maintaining Online Diagnostics

Configuration Examples for Online Diagnostic Tests

Examples: Start Diagnostic Tests

This example shows how to start a diagnostic test by using the test name:

```
Device#
diagnostic start module 3 test DiagFanTest
```

This example shows how to start all of the basic diagnostic tests:

```
Device# diagnostic start module 3 test all
```

Examples: Displaying Online Diagnostics

This example shows how to display on demand diagnostic settings:

```
Device# show diagnostic ondemand settings

Test iterations = 1
Action on test failure = continue
```

This example shows how to display diagnostic events for errors:

```
Device# show diagnostic events event-type error

Diagnostic events (storage for 500 events, 0 events recorded)
Number of events matching above criteria = 0
```


No diagnostic log entry exists.

This example shows how to display the description for a diagnostic test:

```
Device# show diagnostic description module 3 test all
TestGoldPktLoopback :
The GOLD packet Loopback test verifies the MAC level loopback
functionality. In this test, a GOLD packet, for which doppler
provides the support in hardware, is sent. The packet loops back
at MAC level and is matched against the stored packet. It is a
non-disruptive test.

TestFantray :
This test verifies all fan modules have been inserted and working
properly on the board. It is a non-disruptive test and can be
run as a health monitoring test.

TestPhyLoopback :
The PHY Loopback test verifies the PHY level loopback
functionality. In this test, a packet is sent which loops back
at PHY level and is matched against the stored packet. It is a
disruptive test and cannot be run as a health monitoring test.

TestThermal :
This test verifies the temperature reading from the sensor is
below the yellow temperature threshold. It is a non-disruptive
test and can be run as a health monitoring test.

TestScratchRegister :
The Scratch Register test monitors the health of
application-specific integrated circuits (ASICs) by writing values
into registers and reading back the values from these registers.
It is a non-disruptive test and can be run as a health monitoring
test.

TestMemory :
This test runs the exhaustive ASIC memory test during normal
switch operation. Switch utilizes mbist for this test. Memory test
is very disruptive in nature and requires switch reboot after
the test.

Device#
```

Additional References for Online Diagnostics

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

Feature Information for Configuring Online Diagnostics

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|--------------------|--|
| Cisco IOS XE Gibraltar 16.11.1 | Online Diagnostics | With online diagnostics, you can test and verify the hardware functionality of the device while the device is connected to a live network. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 9

Managing Configuration Files

- [Prerequisites for Managing Configuration Files, on page 133](#)
- [Restrictions for Managing Configuration Files, on page 133](#)
- [Information About Managing Configuration Files, on page 133](#)
- [How to Manage Configuration File Information, on page 140](#)
- [Feature History for Managing Configuration Files, on page 167](#)

Prerequisites for Managing Configuration Files

- You should have at least a basic familiarity with the Cisco IOS environment and the command-line interface.
- You should have at least a minimal configuration running on your system. You can create a basic configuration file using the **setup** command.

Restrictions for Managing Configuration Files

- Many of the Cisco IOS commands described in this document are available and function only in certain configuration modes on the device.
- Some of the Cisco IOS configuration commands are only available on certain device platforms, and the command syntax may vary on different platforms.

Information About Managing Configuration Files

Types of Configuration Files

Configuration files contain the Cisco IOS software commands used to customize the functionality of your Cisco device. Commands are parsed (translated and executed) by the Cisco IOS software when the system is booted (from the startup-config file) or when you enter commands at the CLI in a configuration mode.

Startup configuration files (startup-config) are used during system startup to configure the software. Running configuration files (running-config) contain the current configuration of the software. The two configuration

files can be different. For example, you may want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration using the **configure terminal** EXEC command but not save the configuration using the **copy running-config startup-config** EXEC command.

To change the running configuration, use the **configure terminal** command, as described in the [Modifying the Configuration File, on page 141](#) section. As you use the Cisco IOS 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 using the **copy running-config startup-config** EXEC command or copy a configuration file from a file server to the startup configuration (see the [Copying a Configuration File from a TFTP Server to the Device](#) section for more information).

Configuration Mode and Selecting a Configuration Source

To enter configuration mode on the device, enter the **configure** command at the privileged EXEC prompt. The Cisco IOS software responds with the following prompt asking you to specify the terminal, memory, or a file stored on a network server (network) as the source of configuration commands:

```
Configuring from terminal, memory, or network [terminal]?
```

Configuring from the terminal allows you to enter configuration commands at the command line, as described in the following section. See the [Re-executing the Configuration Commands in the Startup Configuration File](#) section for more information.

Configuring from the network allows you to load and execute configuration commands over the network. See the [Copying a Configuration File from a TFTP Server to the Device](#) section for more information.

Configuration File Changes Using the CLI

The Cisco IOS software accepts one configuration command per line. You can enter as many configuration commands as you want. You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!). Because comments are *not* stored in NVRAM or in the active copy of the configuration file, comments do not appear when you list the active configuration with the **show running-config** or **more system:running-config** EXEC command. Comments are not displayed when you list the startup configuration with the **show startup-config** or **more nvram:startup-config** EXEC mode command. Comments are stripped out of the configuration file when it is loaded onto the device. However, you can list the comments in configuration files stored on a File Transfer Protocol (FTP), Remote Copy Protocol (RCP), or Trivial File Transfer Protocol (TFTP) server. When you configure the software using the CLI, the software executes the commands as you enter them.

Location of Configuration Files

Configuration files are stored in the following locations:

- The running configuration is stored in RAM.
- On all platforms except the Class A Flash file system platforms, the startup configuration is stored in nonvolatile random-access memory (NVRAM).

- On Class A Flash file system platforms, the startup configuration is stored in the location specified by the CONFIG_FILE environment variable (see the [Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems](#), on page 162 section). The CONFIG_FILE variable defaults to NVRAM and can be a file in the following file systems:

- **nvr**am: (NVRAM)
- **flash**: (internal flash memory)
- **usbflash0**: (external usbflash file system)
- **usbflash1**: (external usbflash file system)

Copy Configuration Files from a Network Server to the Device

You can copy configuration files from a TFTP, rcp, or FTP server to the running configuration or startup configuration of the device. You may want to perform this function for one of the following reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another device. For example, you may add another device to your network and want it to have a similar configuration to the original device. By copying the file to the new device, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on to all of the devices in your network so that all of the devices have similar configurations.

The **copy {ftp: | rcp: | tftp:} system:running-config** EXEC command loads the configuration files into the device as if you were typing the commands on the command line. The device does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration may not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

To restore a configuration file to an exact copy of a file stored on a server, you need to copy the configuration file directly to the startup configuration (using the **copy ftp:|rcp:|tftp: nvram:startup-config** command) and reload the device.

To copy configuration files from a server to a device, perform the tasks described in the following sections.

The protocol that you use depends on which type of server you are using. The FTP and rcp transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because the FTP and rcp transport mechanisms are built on and use the TCP/IP stack, which is connection-oriented.

Copying a Configuration File from the Device to a TFTP Server

In some implementations of TFTP, you must create a dummy file on the TFTP server and give it read, write, and execute permissions before copying a file over it. Refer to your TFTP documentation for more information.

Copying a Configuration File from the Device to an RCP Server

You can copy a configuration file from the device to an RCP server.

One of the first attempts to use the network as a resource in the UNIX community resulted in the design and implementation of the remote shell protocol, which included the remote shell (rsh) and remote copy (rcp) functions. Rsh and rcp give users the ability to execute commands remotely and copy files to and from a file system residing on a remote host or server on the network. The Cisco implementation of rsh and rcp interoperates with standard implementations.

The rcp **copy** commands rely on the rsh server (or daemon) on the remote system. To copy files using rcp, you need not create a server for file distribution, as you do with TFTP. You need only to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, rcp creates it for you.

Although the Cisco rcp implementation emulates the functions of the UNIX rcp implementation—copying files among systems on the network—the Cisco command syntax differs from the UNIX rcp command syntax. The Cisco rcp support offers a set of **copy** commands that use rcp as the transport mechanism. These rcp **copy** commands are similar in style to the Cisco TFTP **copy** commands, but they offer an alternative that provides faster performance and reliable delivery of data. These improvements are possible because the rcp transport mechanism is built on and uses the TCP/IP stack, which is connection-oriented. You can use rcp commands to copy system images and configuration files from the device to a network server and vice versa.

You also can enable rcp support to allow users on remote systems to copy files to and from the device.

To configure the Cisco IOS software to allow remote users to copy files to and from the device, use the **ip rcmd rcp-enable** global configuration command.

Restrictions

The RCP protocol requires a client to send a remote username on each RCP request to a server. When you copy a configuration file from the device to a server using RCP, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The username specified in the **copy EXEC** command, if a username is specified.
2. The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the device through Telnet and was authenticated through the **username** command, the device software sends the Telnet username as the remote username.
4. The device host name.

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, you can specify that user name as the remote username.

Use the **ip rcmd remote-username** command to specify a username for all copies. (Rcmd is a UNIX routine used at the super-user level to execute commands on a remote machine using an authentication scheme based on reserved port numbers. Rcmd stands for “remote command”). Include the username in the **copy** command if you want to specify a username for that copy operation only.

If you are writing to the server, the RCP server must be properly configured to accept the RCP write request from the user on the device. For UNIX systems, you must add an entry to the `.rhosts` file for the remote user on the RCP server. For example, suppose the device contains the following configuration lines:

```
hostname Device1
ip rcmd remote-username User0
```

If the device IP address translates to `device1.example.com`, then the `.rhosts` file for `User0` on the RCP server should contain the following line:

```
Device1.example.com Device1
```

Requirements for the RCP Username

The RCP protocol requires a client to send a remote username on each RCP request to a server. When you copy a configuration file from the device to a server using RCP, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The username specified in the **copy EXEC** command, if a username is specified.
2. The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the device through Telnet and is authenticated through the **username** command, the device software sends the Telnet username as the remote username.
4. The device host name.

For the RCP copy request to execute, an account must be defined on the network server for the remote username. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

Refer to the documentation for your RCP server for more information.

Copying a Configuration File from the Device to an FTP Server

You can copy a configuration file from the device to an FTP server.

Understanding the FTP Username and Password



Note The password must not contain the special character '@'. If the character '@' is used, the copy fails to parse the IP address of the server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the device to a server using FTP, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The username specified in the **copy EXEC** command, if a username is specified.
2. The username set by the **ip ftp username** global configuration command, if the command is configured.

3. Anonymous.

The device sends the first valid password it encounters in the following sequence:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The device forms a password *username @devicename.domain*. The variable *username* is the username associated with the current session, *devicename* is the configured host name, and *domain* is the domain of the device.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the device.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

Refer to the documentation for your FTP server for more information.

Use the **ip ftp username** and **ip ftp password** global configuration commands to specify a username and password for all copies. Include the username in the **copy EXEC** command if you want to specify a username for that copy operation only.

Copying files through a VRF

You can copy files through a VRF interface specified in the **copy** command. Specifying the VRF in the **copy** command is easier and more efficient as you can directly change the source interface without using a change request for the configuration.

Example

The following example shows how to copy files through a VRF, using the **copy** command:

```
Device#
Address or name of remote host [10.1.2.3]?
Source username [ScpUser]?
Source filename [/auto/tftp-server/ScpUser/vrf_test.txt]?
Destination filename [vrf_test.txt]?
Getting the vrf name as test-vrf
Password:
Sending file modes: C0644 10 vrf_test.txt
!
223 bytes copied in 22.740 secs (10 bytes/sec)
```

Copy Configuration Files from a Switch to Another Switch

You can copy the configurations from one switch to another. This is a 2-step process - Copy the configurations from the switch to the TFTP server, and then from TFTP to another switch.

To copy your current configurations from the switch, run the command **copy startup-config tftp:** and follow the instructions. The configurations are copied onto the TFTP server.

Then, login to another switch and run the command **copy tftp: startup-config** and follow the instructions. The configurations are now copied onto the other switch.

After the configurations are copied, to save your configurations, use **write memory** command and then either reload the switch or run the **copy startup-config running-config** command

Configuration Files Larger than NVRAM

To maintain a configuration file that exceeds the size of NVRAM, you should be aware of the information in the following sections.

Compressing the Configuration File

The **service compress-config** global configuration command specifies that the configuration file be stored compressed in NVRAM. Once the configuration file has been compressed, the device functions normally. When the system is booted, it recognizes that the configuration file is compressed, expands it, and proceeds normally. The **more nvram:startup-config EXEC** command expands the configuration before displaying it.

Before you compress configuration files, refer to the appropriate hardware installation and maintenance publication. Verify that your system's ROMs support file compression. If not, you can install new ROMs that support file compression.

The size of the configuration must not exceed three times the NVRAM size. For a 128-KB size NVRAM, the largest expanded configuration file size is 384 KB.

The **service compress-config** global configuration command works only if you have Cisco IOS software Release 10.0 or later release boot ROMs. Installing new ROMs is a one-time operation and is necessary only if you do not already have Cisco IOS Release 10.0 in ROM. If the boot ROMs do not recognize a compressed configuration, the following message is displayed:

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

Storing the Configuration in Flash Memory on Class A Flash File Systems

On class A Flash file system devices, you can store the startup configuration in flash memory by setting the **CONFIG_FILE** environment variable to a file in internal flash memory or flash memory in a PCMCIA slot.

See the [Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems](#), on page 162 section for more information.

Care must be taken when editing or changing a large configuration. Flash memory space is used every time a **copy system:running-config nvram:startup-config EXEC** command is issued. Because file management for flash memory (such as optimizing free space) is not done automatically, you must pay close attention to available flash memory. Use the **squeeze** command to reclaim used space. We recommend that you use a large-capacity Flash card of at least 20 MB.

Loading the Configuration Commands from the Network

You can also store large configurations on FTP, RCP, or TFTP servers and download them at system startup. To use a network server to store large configurations, see the [Copying a Configuration File from the Device to a TFTP Server](#), on page 142 and [Configuring the Device to Download Configuration Files](#), on page 139 sections for more information on these commands.

Configuring the Device to Download Configuration Files

You can configure the device to load one or two configuration files at system startup. The configuration files are loaded into memory and read in as if you were typing the commands at the command line. Thus, the

configuration for the device is a mixture of the original startup configuration and the one or two downloaded configuration files.

Network Versus Host Configuration Files

For historical reasons, the first file the device downloads is called the network configuration file. The second file the device downloads is called the host configuration file. Two configuration files can be used when all of the devices on a network use many of the same commands. The network configuration file contains the standard commands used to configure all of the devices. The host configuration files contain the commands specific to one particular host. If you are loading two configuration files, the host configuration file should be the configuration file you want to have precedence over the other file. Both the network and host configuration files must reside on a network server reachable via TFTP, RCP, or FTP, and must be readable.

How to Manage Configuration File Information

Displaying Configuration File Information

To display information about configuration files, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show boot Example: <pre>Device# show boot</pre> | Lists the contents of the BOOT environment variable (if set), the name of the configuration file pointed to by the CONFIG_FILE environment variable, and the contents of the BOOTLDR environment variable. |
| Step 3 | more <i>file-url</i> Example: <pre>Device# more 10.1.1.1</pre> | Displays the contents of a specified file. |
| Step 4 | show running-config Example: <pre>Device# show running-config</pre> | Displays the contents of the running configuration file. (Command alias for the more system:running-config command.) |
| Step 5 | show startup-config Example: <pre>Device# show startup-config</pre> | Displays the contents of the startup configuration file. (Command alias for the more nvram:startup-config command.) |

| | Command or Action | Purpose |
|--|-------------------|---|
| | | <p>On all platforms except the Class A Flash file system platforms, the default startup-config file usually is stored in NVRAM.</p> <p>On the Class A Flash file system platforms, the CONFIG_FILE environment variable points to the default startup-config file.</p> <p>The CONFIG_FILE variable defaults to NVRAM.</p> |

Modifying the Configuration File

The Cisco IOS software accepts one configuration command per line. You can enter as many configuration commands as you want. You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!). Because comments are *not* stored in NVRAM or in the active copy of the configuration file, comments do not appear when you list the active configuration with the **show running-config** or **more system:running-config EXEC** commands. Comments do not display when you list the startup configuration with the **show startup-config** or **more nvram:startup-config EXEC** mode commands. Comments are stripped out of the configuration file when it is loaded onto the device. However, you can list the comments in configuration files stored on a File Transfer Protocol (FTP), Remote Copy Protocol (RCP), or Trivial File Transfer Protocol (TFTP) server. When you configure the software using the CLI, the software executes the commands as you enter them. To configure the software using the CLI, use the following commands in privileged EXEC mode:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | configuration command Example: <pre>Device(config)# configuration command</pre> | Enter the necessary configuration commands. The Cisco IOS documentation set describes configuration commands organized by technology. |
| Step 4 | <p>Do one of the following:</p> <ul style="list-style-type: none"> • end • ^Z Example: | <p>Ends the configuration session and exits to EXEC mode.</p> <p>Note When you press the Ctrl and Z keys simultaneously, ^Z is displayed to the screen.</p> |

| | Command or Action | Purpose |
|---------------|--|--|
| | Device(config)# end | |
| Step 5 | copy system:running-config nvram:startup-config Example: Device# copy system:running-config nvram:startup-config | Saves the running configuration file as the startup configuration file. You may also use the copy running-config startup-config command alias, but you should be aware that this command is less precise. On most platforms, this command saves the configuration to NVRAM. On the Class A Flash file system platforms, this step saves the configuration to the location specified by the CONFIG_FILE environment variable (the default CONFIG_FILE variable specifies that the file should be saved to NVRAM). |

Examples

In the following example, the device prompt name of the device is configured. The comment line, indicated by the exclamation mark (!), does not execute any command. The **hostname** command is used to change the device name from device to new_name. By pressing Ctrl-Z (^Z) or entering the **end** command, the user quits configuration mode. The **copy system:running-config nvram:startup-config** command saves the current configuration to the startup configuration.

```
Device# configure terminal
Device(config)# !The following command provides the switch host name.
Device(config)# hostname new_name
new_name(config)# end
new_name# copy system:running-config nvram:startup-config
```

When the startup configuration is NVRAM, it stores the current configuration information in text format as configuration commands, recording only non-default settings. The memory is checksummed to guard against corrupted data.



Note Some specific commands might not get saved to NVRAM. You need to enter these commands again if you reboot the machine. These commands are noted in the documentation. We recommend that you keep a list of these settings so that you can quickly reconfigure your device after rebooting.

Copying a Configuration File from the Device to a TFTP Server

To copy configuration information on a TFTP network server, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | copy system:running-config tftp: [[[//location]/directory]/filename] Example: <pre>Device# copy system:running-config tftp: //server1/topdir/file10</pre> | Copies the running configuration file to a TFTP server. |
| Step 3 | copy nvram:startup-config tftp: [[[//location]/directory]/filename] Example: <pre>Device# copy nvram:startup-config tftp: //server1/1stidir/file10</pre> | Copies the startup configuration file to a TFTP server. |

Examples

The following example copies a configuration file from a device to a TFTP server:

```
Device# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] Y
Writing tokyo-config!!! [OK]
```

What to Do Next

After you have issued the **copy** command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from the Device to an RCP Server

To copy a startup configuration file or a running configuration file from the device to an RCP server, use the following commands beginning in privileged EXEC mode:

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------------|---|
| Step 1 | enable Example: | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Device> enable | |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip rcmd remote-username <i>username</i> Example: Device(config)# ip rcmd remote-username NetAdmin1 | (Optional) Changes the default remote username. |
| Step 4 | end Example: Device(config)# end | (Optional) Exits global configuration mode. |
| Step 5 | Do one of the following: <ul style="list-style-type: none"> • copy system:running-config rcp: [[[/<i>username@</i>]/<i>location</i>]/<i>directory</i>]/<i>filename</i>] • copy nvram:startup-config rcp: [[[/<i>username@</i>]/<i>location</i>]/<i>directory</i>]/<i>filename</i>] Example: Device# copy system:running-config rcp: //NetAdmin1@example.com/dir-files/file1 | <ul style="list-style-type: none"> • Specifies that the device running configuration file is to be stored on an RCP server or • Specifies that the device startup configuration file is to be stored on an RCP server |

Examples

Storing a Running Configuration File on an RCP Server

The following example copies the running configuration file named runfile2-config to the netadmin1 directory on the remote host with an IP address of 172.16.101.101:

```
Device# copy system:running-config rcp://netadmin1@172.16.101.101/runfile2-config
Write file runfile2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Device#
```

Storing a Startup Configuration File on an RCP Server

The following example shows how to store a startup configuration file on a server by using RCP to copy the file:

```

Device# configure terminal

Device(config)# ip rcmd remote-username netadmin2

Device(config)# end

Device# copy nvram:startup-config rcp:

Remote host[]? 172.16.101.101

Name of configuration file to write [start-config]?
Write file start-config on host 172.16.101.101?[confirm]
![OK]

```

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from the Device to the FTP Server

To copy a startup configuration file or a running configuration file from the device to an FTP server, complete the following tasks:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode on the device. |
| Step 3 | ip ftp username <i>username</i> Example: <pre>Device(config)# ip ftp username NetAdmin1</pre> | (Optional) Specifies the default remote username. |
| Step 4 | ip ftp password <i>password</i> Example: <pre>Device(config)# ip ftp password adminpassword</pre> | (Optional) Specifies the default password. |
| Step 5 | end Example: | (Optional) Exits global configuration mode. This step is required only if you override the |

| | Command or Action | Purpose |
|---------------|--|---|
| | Device(config)# end | default remote username or password (see Steps 2 and 3). |
| Step 6 | Do one of the following: <ul style="list-style-type: none"> • copy system:running-config ftp: [[[//username[:password]]@]location]/directory]/filename] or • copy nvram:startup-config ftp: [[[//username[:password]]@]location]/directory]/filename] Example: Device# copy system:running-config ftp: | Copies the running configuration or startup configuration file to the specified location on the FTP server. |

Examples

Storing a Running Configuration File on an FTP Server

The following example copies the running configuration file named runfile-confg to the netadmin1 directory on the remote host with an IP address of 172.16.101.101:

```
Device# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/runfile-confg
Write file runfile-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Device#
```

Storing a Startup Configuration File on an FTP Server

The following example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
Device# configure terminal

Device(config)# ip ftp username netadmin2

Device(config)# ip ftp password mypass

Device(config)# end

Device# copy nvram:startup-config ftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [start-confg]?
Write file start-confg on host 172.16.101.101?[confirm]
![OK]
```


What to Do Next

After you have issued the **copy EXEC** command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from a TFTP Server to the Device

To copy a configuration file from a TFTP server to the device, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | copy tftp: [[[//location]/directory]/filename] system:running-config Example: <pre>Device# copy tftp://server1/dir10/datasource system:running-config</pre> | Copies a configuration file from a TFTP server to the running configuration. |
| Step 3 | copy tftp: [[[//location]/directory]/filename] nvrnram:startup-config Example: <pre>Device# copy tftp://server1/dir10/datasource nvrnram:startup-config</pre> | Copies a configuration file from a TFTP server to the startup configuration. |
| Step 4 | copy tftp: [[[//location]/directory]/filename] flash-[n]/directory/startup-config Example: <pre>Device# copy tftp://server1/dir10/datasource flash:startup-config</pre> | Copies a configuration file from a TFTP server to the startup configuration. |

Examples

In the following example, the software is configured from the file named **tokyo-config** at IP address 172.16.2.155:

```
Device# copy tftp://172.16.2.155/tokyo-config system:running-config
```

```
Configure using tokyo-config from 172.16.2.155? [confirm] Y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from the rcp Server to the Device

To copy a configuration file from an rcp server to the running configuration or startup configuration, complete the following tasks:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | (Optional) Enters configuration mode from the terminal. This step is required only if you override the default remote username (see Step 3). |
| Step 3 | ip rcmd remote-username <i>username</i> Example: <pre>Device(config)# ip rcmd remote-username NetAdmin1</pre> | (Optional) Specifies the remote username. |
| Step 4 | end Example: <pre>Device(config)# end</pre> | (Optional) Exits global configuration mode. This step is required only if you override the default remote username (see Step 2). |
| Step 5 | Do one of the following: <ul style="list-style-type: none"> • copy <pre>ip://username@win162155:8021/runningconf</pre> • copy <pre>ip://username@win162155:8021/startupconf</pre> Example: <pre>Device# copy</pre> | Copies the configuration file from an rcp server to the running configuration or startup configuration. |

| | Command or Action | Purpose |
|--|---|---------|
| | <code>rcp://[user1@example.com/dir10/fileone] nvram:startup-config</code> | |

Examples

Copy RCP Running-Config

The following example copies a configuration file named `host1-config` from the `netadmin1` directory on the remote server with an IP address of `172.16.101.101`, and loads and runs the commands on the device:

```
device# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:[OK]
device#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

Copy RCP Startup-Config

The following example specifies a remote username of `netadmin1`. Then it copies the configuration file named `host2-config` from the `netadmin1` directory on the remote server with an IP address of `172.16.101.101` to the startup configuration.

```
device# configure terminal
device(config)# ip rcmd remote-username netadmin1
device(config)# end
device# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
[OK]
device#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from 172.16.101.101
```

What to Do Next

After you have issued the **copy EXEC** command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from an FTP Server to the Device

To copy a configuration file from an FTP server to the running configuration or startup configuration, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|-------------------|-------------------------------|
| Step 1 | enable | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Example: Device> enable | <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | (Optional) Allows you to enter global configuration mode. This step is required only if you want to override the default remote username or password (see Steps 3 and 4). |
| Step 3 | ip ftp username <i>username</i> Example: Device(config)# ip ftp username NetAdmin1 | (Optional) Specifies the default remote username. |
| Step 4 | ip ftp password <i>password</i> Example: Device(config)# ip ftp password adminpassword | (Optional) Specifies the default password. |
| Step 5 | end Example: Device(config)# end | (Optional) Exits global configuration mode. This step is required only if you override the default remote username or password (see Steps 3 and 4). |
| Step 6 | Do one of the following: <ul style="list-style-type: none"> copy ftp: [[[/<i>username[:password]@]location</i>] <i>/directory</i> <i>/filename</i>]system:running-config copy ftp: [[[<i>username[:password]@location</i>]system:startup-config Example: Device# copy ftp:nvram:startup-config | Using FTP copies the configuration file from a network server to running memory or the startup configuration. |

Examples

Copy FTP Running-Config

The following example copies a host configuration file named host1-config from the netadmin1 directory on the remote server with an IP address of 172.16.101.101, and loads and runs the commands on the device:

```
device# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
```

```
device#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

Copy FTP Startup-Config

The following example specifies a remote username of `netadmin1`. Then it copies the configuration file named `host2-config` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
device# configure terminal
device(config)# ip ftp username netadmin1
device(config)# ip ftp password mypass
device(config)# end
device# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[host1-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
[OK]
device#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from 172.16.101.101
```

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Maintaining Configuration Files Larger than NVRAM

To maintain a configuration file that exceeds the size of NVRAM, perform the tasks described in the following sections:

Compressing the Configuration File

To compress configuration files, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 3 | service compress-config Example: <pre>Device(config)# service compress-config</pre> | Specifies that the configuration file be compressed. |
| Step 4 | end Example: <pre>Device(config)# end</pre> | Exits global configuration mode. |
| Step 5 | Do one of the following: <ul style="list-style-type: none"> • Use FTP, RCP, or TFTP to copy the new configuration. • configure terminal Example: <pre>Device# configure terminal</pre> | Enters the new configuration: <ul style="list-style-type: none"> • If you try to load a configuration that is more than three times larger than the NVRAM size, the following error message is displayed: <pre>“[buffer overflow - file-size /buffer-size bytes].”</pre> |
| Step 6 | copy system:running-config nvram:startup-config Example: <pre>Device(config)# copy system:running-config nvram:startup-config</pre> | When you have finished changing the running-configuration, save the new configuration. |

Examples

The following example compresses a 129-KB configuration file to 11 KB:

```
Device# configure terminal
Device(config)# service compress-config
Device(config)# end
Device# copy tftp://172.16.2.15/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
Device# copy system:running-config nvram:startup-config
Building configuration...
Compressing configuration from 129648 bytes to 11077 bytes
[OK]
```

Storing the Configuration in Flash Memory on Class A Flash File Systems

To store the startup configuration in flash memory, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | copy nvram:startup-config flash-filesystem:filename Example: <pre>Device# copy nvram:startup-config usbflash0:switch-config</pre> | Copies the current startup configuration to the new location to create the configuration file. |
| Step 3 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 4 | boot config flash-filesystem: filename Example: <pre>Device(config)# boot config usbflash0:switch-config</pre> | Specifies that the startup configuration file be stored in flash memory by setting the CONFIG_FILE variable. |
| Step 5 | end Example: <pre>Device(config)# end</pre> | Exits global configuration mode. |
| Step 6 | Do one of the following: <ul style="list-style-type: none"> • Use FTP, RCP, or TFTP to copy the new configuration. If you try to load a configuration that is more than three times larger than the NVRAM size, the following error message is displayed: “[buffer overflow - file-size /buffer-size bytes].” • configure terminal Example: <pre>Device# configure terminal</pre> | Enters the new configuration. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 7 | copy system:running-config nvram:startup-config Example: <pre>Device(config)# copy system:running-config nvram:startup-config</pre> | When you have finished changing the running-configuration, save the new configuration. |

Examples

The following example stores the configuration file in usbflash0:

```
Device# copy nvram:startup-config usbflash0:switch-config
Device# configure terminal
Device(config)# boot config usbflash0:switch-config
Device(config)# end
Device# copy system:running-config nvram:startup-config
```

Loading the Configuration Commands from the Network

To use a network server to store large configurations, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | copy system:running-config {ftp: rcp: tftp:} Example: <pre>Device# copy system:running-config ftp:</pre> | Saves the running configuration to an FTP, RCP, or TFTP server. |
| Step 3 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 4 | boot network {ftp:[[/[username [:password]@]location]/directory]/filename] rcp:[[/[username@]location]/directory | Specifies that the startup configuration file be loaded from the network server at startup. |

| | Command or Action | Purpose |
|---------------|---|---|
| | <pre>]/filename] tftp:[[[//location]/directory]/filename]}</pre> <p>Example:</p> <pre>Device(config)# boot network ftp://user1:guessme@example.com/dir10/file1</pre> | |
| Step 5 | <p>service config</p> <p>Example:</p> <pre>Device(config)# service config</pre> | Enables the switch to download configuration files at system startup. |
| Step 6 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | Exits global configuration mode. |
| Step 7 | <p>copy system:running-config nvram:startup-config</p> <p>Example:</p> <pre>Device# copy system:running-config nvram:startup-config</pre> | Saves the configuration. |

Copying Configuration Files from Flash Memory to the Startup or Running Configuration

To copy a configuration file from flash memory directly to your startup configuration in NVRAM or your running configuration, enter one of the commands in Step 2:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Device> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | <p>Do one of the following:</p> <ul style="list-style-type: none"> • copy filesystem: [partition-number:][filename] nvram:startup-config • copy filesystem: [partition-number:][filename] system:running-config | <ul style="list-style-type: none"> • Loads a configuration file directly into NVRAM or • Copies a configuration file to your running configuration |

| | Command or Action | Purpose |
|--|---|---------|
| | Example: Device# copy usbflash0:4:ios-upgrade-1 nvram:startup-config | |

Examples

The following example copies the file named ios-upgrade-1 from partition 4 of the flash memory PC Card in usbflash0 to the device startup configurations:

```
Device# copy usbflash0:4:ios-upgrade-1 nvram:startup-config
```

```
Copy 'ios-upgrade-1' from flash device as 'startup-config' ? [yes/no] yes
```

```
[OK]
```

Copying Configuration Files Between Flash Memory File Systems

On platforms with multiple flash memory file systems, you can copy files from one flash memory file system, such as internal flash memory to another flash memory file system. Copying files to different flash memory file systems lets you create backup copies of working configurations and duplicate configurations for other devices. To copy a configuration file between flash memory file systems, use the following commands in EXEC mode:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show source-filesystem: Example: Device# show flash: | Displays the layout and contents of flash memory to verify the filename. |
| Step 3 | copy source-filesystem: [partition-number:][filename] dest-filesystem:[partition-number:][filename] Example: Device# copy flash: usbflash0: | Copies a configuration file between flash memory devices. <ul style="list-style-type: none"> • The source device and the destination device cannot be the same. For example, the copy usbflash0: usbflash0: command is invalid. |

The following example copies the file named `running-config` from partition 1 on internal flash memory to partition 1 of `usbflash0` on a device. In this example, the source partition is not specified, so the device prompts for the partition number:

```
Device# copy flash: usbflash0:

System flash
Partition Size Used Free Bank-Size State Copy Mode
1 4096K 3070K 1025K 4096K Read/Write Direct
2 16384K 1671K 14712K 8192K Read/Write Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
System flash directory, partition 1:
File Length Name/status
1 3142748 dirt/network/mars-test/c3600-j-mz.latest
2 850 running-config
[3143728 bytes used, 1050576 available, 4194304 total]
usbflash0 flash directory:
File Length Name/status
1 1711088 dirt/gate/c3600-i-mz
2 850 running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config

Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)... OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'running-config' from flash: device
as 'running-config' into usbflash0: device WITH erase? [yes/no] yes

Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased!

[OK - 850/4194304 bytes]
Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum... OK (0x16)
```

To copy a configuration file from an FTP server to a flash memory device, complete the task in this section:

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: | (Optional) Enters global configuration mode. This step is required only if you override the default remote username or password (see Steps 3 and 4). |

| | Command or Action | Purpose |
|---------------|--|--|
| | Device# <code>configure terminal</code> | |
| Step 3 | ip ftp username <i>username</i> Example: Device(config)# <code>ip ftp username Admin01</code> | (Optional) Specifies the remote username. |
| Step 4 | ip ftp password <i>password</i> Example: Device(config)# <code>ip ftp password adminpassword</code> | (Optional) Specifies the remote password. |
| Step 5 | end Example: Device(config)# <code>end</code> | (Optional) Exits configuration mode. This step is required only if you override the default remote username (see Steps 3 and 4). |
| Step 6 | copy ftp: <code>[[//location]/directory]/bundle_name</code> flash: Example: Device> <code>copy</code> <code>ftp:/cat9k_iosxe.16.11.01.SPA.bin flash:</code> | Copies the configuration file from a network server to the flash memory device using FTP. |

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from an RCP Server to Flash Memory Devices

To copy a configuration file from an RCP server to a flash memory device, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> <code>enable</code> | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: | (Optional) Enters global configuration mode. This step is required only if you override the |

| | Command or Action | Purpose |
|---------------|---|---|
| | Device# configure terminal | default remote username or password (see Step 3). |
| Step 3 | ip rcmd remote-username <i>username</i> Example: Device(config)# ip rcmd remote-username Admin01 | (Optional) Specifies the remote username. |
| Step 4 | end Example: Device(config)# end | (Optional) Exits configuration mode. This step is required only if you override the default remote username or password (see Step 3). |
| Step 5 | copy rcp: [[[/[<i>username@</i>] <i>location</i>]/ <i>directory</i>]/ <i>bundle_name</i> flash: Example: Device# copy rcp://netadmin@172.16.101.101/bundle1 flash: | Copies the configuration file from a network server to the flash memory device using RCP. Respond to any device prompts for additional information or confirmation. Prompting depends on how much information you provide in the copy command and the current setting of the file prompt command. |

Copying a Configuration File from a TFTP Server to Flash Memory Devices

To copy a configuration file from a TFTP server to a flash memory device, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | copy tftp: [[[/ <i>location</i>]/ <i>directory</i>]/ <i>bundle_name</i> flash: Example: Device# copy tftp://at3_catalyst9500-3A.03.12.02.EP.150-12.02.EP.150-12.02.EP.bin flash: | Copies the file from a TFTP server to the flash memory device. Reply to any device prompts for additional information or confirmation. Prompting depends on how much information you provide in the copy command and the current setting of the file prompt command. |

Examples

The following example shows the copying of the configuration file named switch-config from a TFTP server to the flash memory card inserted in usbflash0. The copied file is renamed new-config.

```
Device#
copy tftp:switch-config usbflash0:new-config
```

Re-executing the Configuration Commands in the Startup Configuration File

To re-execute the commands located in the startup configuration file, complete the task in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure memory Example: Device# configure memory | Re-executes the configuration commands located in the startup configuration file. |

Clearing the Startup Configuration

You can clear the configuration information from the startup configuration. If you reboot the device with no startup configuration, the device enters the Setup command facility so that you can configure the device from scratch. To clear the contents of your startup configuration, complete the task in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | erase nvram Example: | Clears the contents of your startup configuration. |

| | Command or Action | Purpose |
|--|---------------------|--|
| | Device# erase nvram | Note For all platforms except the Class A Flash file system platforms, this command erases NVRAM. The startup configuration file cannot be restored once it has been deleted. On Class A Flash file system platforms, when you use the erase startup-config EXEC command, the device erases or deletes the configuration pointed to by the CONFIG_FILE environment variable. If this variable points to NVRAM, the device erases NVRAM. If the CONFIG_FILE environment variable specifies a flash memory device and configuration filename, the device deletes the configuration file. That is, the device marks the file as “deleted,” rather than erasing it. This feature allows you to recover a deleted file. |

Deleting a Specified Configuration File

To delete a specified configuration on a specific flash device, complete the task in this section:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | delete <i>flash-filesystem:filename</i> Example: | Deletes the specified configuration file on the specified flash device. |

| | Command or Action | Purpose |
|--|--|---|
| | <pre>Device# delete usbflash0:myconfig</pre> | <p>Note On Class A and B Flash file systems, when you delete a specific file in flash memory, the system marks the file as deleted, allowing you to later recover a deleted file using the undelete EXEC command. Erased files cannot be recovered. To permanently erase the configuration file, use the squeeze EXEC command. On Class C Flash file systems, you cannot recover a file that has been deleted. If you attempt to erase or delete the configuration file specified by the CONFIG_FILE environment variable, the system prompts you to confirm the deletion.</p> |

Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems

On Class A flash file systems, you can configure the Cisco IOS software to load the startup configuration file specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM. To change the CONFIG_FILE environment variable, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Device> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | <p>copy <i>[flash-url ftp-url rcp-url tftp-url system:running-config nvram:startup-config] dest-flash-url</i></p> <p>Example:</p> <pre>Device# copy system:running-config nvram:startup-config</pre> | <p>Copies the configuration file to the flash file system from which the device loads the file on restart.</p> |
| Step 3 | <p>configure terminal</p> <p>Example:</p> | <p>Enters global configuration mode.</p> |

| | Command or Action | Purpose |
|---------------|---|---|
| | Device# <code>configure terminal</code> | |
| Step 4 | boot config <i>dest-flash-url</i> Example: Device(config)# <code>boot config 172.16.1.1</code> | Sets the CONFIG_FILE environment variable. This step modifies the runtime CONFIG_FILE environment variable. |
| Step 5 | end Example: Device(config)# <code>end</code> | Exits global configuration mode. |
| Step 6 | copy system:running-config nvram:startup-config Example: Device# <code>copy system:running-config nvram:startup-config</code> | Saves the configuration performed in Step 3 to the startup configuration. |
| Step 7 | show boot Example: Device# <code>show boot</code> | (Optional) Allows you to verify the contents of the CONFIG_FILE environment variable. |

Examples

The following example copies the running configuration file to the device. This configuration is then used as the startup configuration when the system is restarted:

```
Device# copy system:running-config usbflash0:config2
Device# configure terminal
Device(config)# boot config usbflash0:config2
Device(config)# end
Device# copy system:running-config nvram:startup-config
[ok]
Device# show boot
BOOT variable = usbflash0:rsp-boot-m
CONFIG_FILE variable = nvram:
Current CONFIG_FILE variable = usbflash0:config2
Configuration register is 0x010F
```

What to Do Next

After you specify a location for the startup configuration file, the **nvram:startup-config** command is aliased to the new location of the startup configuration file. The **more nvram:startup-config EXEC** command displays the startup configuration, regardless of its location. The **erase nvram:startup-config EXEC** command erases the contents of NVRAM and deletes the file pointed to by the CONFIG_FILE environment variable.

When you save the configuration using the **copy system:running-config nvram:startup-config** command, the device saves a complete version of the configuration file to the location specified by the `CONFIG_FILE` environment variable and a distilled version to NVRAM. A distilled version is one that does not contain access list information. If NVRAM contains a complete configuration file, the device prompts you to confirm your overwrite of the complete version with the distilled version. If NVRAM contains a distilled configuration, the device does not prompt you for confirmation and proceeds with overwriting the existing distilled configuration file in NVRAM.



Note If you specify a file in a flash device as the `CONFIG_FILE` environment variable, every time you save your configuration file with the **copy system:running-config nvram:startup-config** command, the old configuration file is marked as “deleted,” and the new configuration file is saved to that device. Eventually, Flash memory fills up as the old configuration files still take up memory. Use the **squeeze EXEC** command to permanently delete the old configuration files and reclaim the space.

Configuring the Device to Download Configuration Files

You can specify an ordered list of network configuration and host configuration filenames. The Cisco IOS XE software scans this list until it loads the appropriate network or host configuration file.

To configure the device to download configuration files at system startup, perform at least one of the tasks described in the following sections:

- [Configuring the Device to Download the Network Configuration File](#)
- [Configuring the Device to Download the Host Configuration File](#)

If the device fails to load a configuration file during startup, it tries again every 10 minutes (the default setting) until a host provides the requested files. With each failed attempt, the device displays the following message on the console terminal:

```
Booting host-config... [timed out]
```

If there are any problems with the startup configuration file, or if the configuration register is set to ignore NVRAM, the device enters the Setup command facility.

Configuring the Device to Download the Network Configuration File

To configure the Cisco IOS software to download a network configuration file from a server at startup, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | boot network {ftp:[[/[username [:password]@]location]/directory]/filename] rcp:[[/[username@]location]/directory]/filename] tftp:[[/[location]/directory]/filename]} Example: <pre>Device(config)# boot network tftp:hostfile1</pre> | <p>Specifies the network configuration file to download at startup, and the protocol to be used (TFTP, RCP, or FTP).</p> <ul style="list-style-type: none"> • If you do not specify a network configuration filename, the Cisco IOS software uses the default filename network-config. If you omit the address, the device uses the broadcast address. • You can specify more than one network configuration file. The software tries them in order entered until it loads one. This procedure can be useful for keeping files with different configuration information loaded on a network server. |
| Step 4 | service config Example: <pre>Device(config)# service config</pre> | Enables the system to automatically load the network file on restart. |
| Step 5 | end Example: <pre>Device(config)# end</pre> | Exits global configuration mode. |
| Step 6 | copy system:running-config nvram:startup-config Example: <pre>Device# copy system:running-config nvram:startup-config</pre> | Saves the running configuration to the startup configuration file. |

Configuring the Device to Download the Host Configuration File

To configure the Cisco IOS software to download a host configuration file from a server at startup, complete the tasks in this section:

Procedure

| | Command or Action | Purpose |
|---------------|-------------------|-------------------------------|
| Step 1 | enable | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| | Example: Device> enable | <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | boot host {ftp:[[/[/[username [:password]@]location]/directory]/filename] rcp:[[/[/[username@]location]/directory]/filename] tftp:[[/[/[location]/directory]/filename] } Example: Device(config)# boot host tftp:hostfile1 | <p>Specifies the host configuration file to download at startup, and the protocol to be used (FTP, RCP, or TFTP):</p> <ul style="list-style-type: none"> If you do not specify a host configuration filename, the device uses its own name to form a host configuration filename by converting the name to all lowercase letters, removing all domain information, and appending “-config.” If no host name information is available, the software uses the default host configuration filename device-config. If you omit the address, the device uses the broadcast address. You can specify more than one host configuration file. The Cisco IOS software tries them in order entered until it loads one. This procedure can be useful for keeping files with different configuration information loaded on a network server. |
| Step 4 | service config Example: Device(config)# service config | Enables the system to automatically load the host file upon restart. |
| Step 5 | end Example: Device(config)# end | Exits global configuration mode. |
| Step 6 | copy system:running-config nvram:startup-config Example: Device# copy system:running-config nvram:startup-config | Saves the running configuration to the startup configuration file. |

Example

In the following example, a device is configured to download the host configuration file named `hostfile1` and the network configuration file named `networkfile1`. The device uses TFTP and the broadcast address to obtain the file:

```
Device# configure terminal
Device(config)# boot host tftp:hostfile1
Device(config)# boot network tftp:networkfile1
Device(config)# service config
Device(config)# end
Device# copy system:running-config nvram:startup-config
```

Feature History for Managing Configuration Files

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|------------------------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Managing Configuration Files | Configuration files contain the Cisco IOS software commands used to customize the functionality of your Cisco device. Commands are parsed (translated and executed) by the Cisco IOS software when the system is booted (from the startup-config file) or when you enter commands at the CLI in a configuration mode. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 10

Secure Copy

This document provides the procedure to configure a Cisco device for Secure Copy (SCP) server-side functionality.

- [Prerequisites for Secure Copy, on page 169](#)
- [Information About Secure Copy, on page 169](#)
- [How to Configure Secure Copy, on page 170](#)
- [How to Configure Secure Copy, on page 173](#)
- [Additional References for Secure Copy, on page 173](#)
- [Feature History for Secure Copy, on page 174](#)

Prerequisites for Secure Copy

- Configure Secure Shell (SSH), authentication, and authorization on the device.
- Because SCP relies on SSH for its secure transport, the device must have a Rivest, Shamir, and Adelman (RSA) key pair.

Information About Secure Copy

The Secure Copy feature provides a secure and authenticated method for copying switch configurations or switch image files. The Secure Copy Protocol (SCP) relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

The behavior of SCP is similar to that of Remote Copy Protocol (RCP), which comes from the Berkeley r-tools suite (Berkeley university's own set of networking applications), except that SCP relies on SSH for security. In addition, SCP requires authentication, authorization, and accounting (AAA) to be configured to ensure that the device can determine whether a user has the correct privilege level.

SCP allows only users with a privilege level of 15 to copy a file in the Cisco IOS File System (Cisco IFS) to and from a device by using the **copy** command. An authorized administrator can also perform this action from a workstation.

**Note**

- Enable the SCP option while using the `pscp.exe` file.
- An RSA public-private key pair must be configured on the device for SSH to work.

Similar to SCP, SSH File Transfer Protocol (SFTP) can be used to copy switch configuration or image files. For more information, refer the *Configuring SSH File Transfer Protocol* chapter of the *Security Configuration Guide*.

How to Configure Secure Copy

Configuring Secure Copy

To configure a Cisco device for SCP server-side functionality, perform the following steps.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Sets AAA authentication at login. |
| Step 4 | aaa authentication login {default list-name} method1 [method2...] Example: Device(config)# aaa authentication login default group tacacs+ | Enables the AAA access control system. |
| Step 5 | username name [privilege level] password encryption-type encrypted-password Example: | Establishes a username-based authentication system. |

| | Command or Action | Purpose |
|---------------|---|---|
| | <pre>Device(config)# username superuser privilege 2 password 0 superpassword</pre> | Note You can omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured. |
| Step 6 | ip scp server enable Example: <pre>Device(config)# ip scp server enable</pre> | Enables SCP server-side functionality. |
| Step 7 | exit Example: <pre>Device(config)# exit</pre> | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 8 | debug ip scp Example: <pre>Device# debug ip scp</pre> | (Optional) Troubleshoots SCP authentication problems. |

Enabling Secure Copy Protocol on the SSH Server

The following task shows how to configure the server-side functionality for SCP. This task shows a typical configuration that allows a device to securely copy files from a remote workstation.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | aaa new-model Example: <pre>Device(config)# aaa new-model</pre> | Enables the Authentication, Authorization, and Accounting (AAA) access control model. |
| Step 4 | aaa authentication login default local Example: | Sets AAA authentication to use the local username database for authentication at login. |

| | Command or Action | Purpose |
|----------------|---|--|
| | Device(config)# aaa authentication login default local | |
| Step 5 | aaa authorization exec default local Example: Device(config)# aaa authorization exec default local | Sets the parameters that restrict user access to a network, runs the authorization to determine if the user ID is allowed to run an EXEC shell, and specifies that the system must use the local database for authorization. |
| Step 6 | username name privilege privilege-level password password Example: Device(config)# username samplename privilege 15 password password1 | Establishes a username-based authentication system, and specifies the username, privilege level, and an unencrypted password. Note The minimum value for the <i>privilege-level</i> argument is 15. A privilege level of less than 15 results in the connection closing. |
| Step 7 | ip ssh time-out seconds Example: Device(config)# ip ssh time-out 120 | Sets the time interval (in seconds) that the device waits for the SSH client to respond. |
| Step 8 | ip ssh authentication-retries integer Example: Device(config)# ip ssh authentication-retries 3 | Sets the number of authentication attempts after which the interface is reset. |
| Step 9 | ip scp server enable Example: Device(config)# ip scp server enable | Enables the device to securely copy files from a remote workstation. |
| Step 10 | ip ssh bulk-mode Example: Device(config)# ip ssh bulk-mode | (Optional) Enables SSH bulk data transfer mode to enhance the throughput performance of SCP. |
| Step 11 | exit Example: Device(config)# exit | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 12 | debug ip scp Example: Device# debug ip scp | (Optional) Provides diagnostic information about SCP authentication problems. |

How to Configure Secure Copy

Example: Secure Copy Configuration Using Local Authentication

The following example shows how to configure the server-side functionality of SCP. This example uses a locally defined username and password.

```
! AAA authentication and authorization must be configured properly in order for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
Device(config)# ip scp server enable
Device(config)# end
```

Example: SCP Server-Side Configuration Using Network-Based Authentication

The following example shows how to configure the server-side functionality of SCP using a network-based authentication mechanism:

```
! AAA authentication and authorization must be configured properly for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default group tacacs+
Device(config)# aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
Device(config)# ip ssh time-out 120
Device(config)# ip ssh authentication-retries 3
Device(config)# ip scp server enable
Device(config)# end
```

Additional References for Secure Copy

Related Documents

| Related Topic | Document Title |
|--------------------------------------|---------------------------------|
| Secure Shell Version 1 and 2 support | <i>Configuring Secure Shell</i> |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature History for Secure Copy

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|-------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Secure Copy | <p>The Secure Copy feature provides a secure and authenticated method for copying device configurations or device image files. SCP relies on SSH, an application and protocol that provide a secure replacement for the Berkeley r-tools suite.</p> <p>The following commands were introduced or modified: debug ip scp and ip scp server enable.</p> |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 11

Configuration Replace and Configuration Rollback

- [Prerequisites for Configuration Replace and Configuration Rollback, on page 175](#)
- [Restrictions for Configuration Replace and Configuration Rollback, on page 176](#)
- [Information About Configuration Replace and Configuration Rollback, on page 176](#)
- [How to Use Configuration Replace and Configuration Rollback, on page 179](#)
- [Configuration Examples for Configuration Replace and Configuration Rollback, on page 185](#)
- [Additional References for Configuration Replace and Configuration Rollback, on page 187](#)
- [Feature History for Configuration Replace and Configuration Rollback, on page 188](#)

Prerequisites for Configuration Replace and Configuration Rollback

The format of the configuration files used as input by the Configuration Replace and Configuration Rollback feature must comply with standard Cisco software configuration file indentation rules as follows:

- Start all commands on a new line with no indentation, unless the command is within a configuration submode.
- Indent commands within a first-level configuration submode one space.
- Indent commands within a second-level configuration submode two spaces.
- Indent commands within subsequent submodes accordingly.

These indentation rules describe how the software creates configuration files for such commands as **show running-config** or **copy running-config destination-url**. Any configuration file generated on a Cisco device complies with these rules.

Free memory larger than the combined size of the two configuration files (the current running configuration and the saved replacement configuration) is required.

Restrictions for Configuration Replace and Configuration Rollback

If the device does not have free memory larger than the combined size of the two configuration files (the current running configuration and the saved replacement configuration), the configuration replace operation is not performed.

Certain Cisco configuration commands such as those pertaining to physical components of a networking device (for example, physical interfaces) cannot be added or removed from the running configuration. For example, a configuration replace operation cannot remove the **interface ethernet 0** command line from the current running configuration if that interface is physically present on the device. Similarly, the **interface ethernet 1** command line cannot be added to the running configuration if no such interface is physically present on the device. A configuration replace operation that attempts to perform these types of changes results in error messages indicating that these specific command lines failed.

In very rare cases, certain Cisco configuration commands cannot be removed from the running configuration without reloading the device. A configuration replace operation that attempts to remove this type of command results in error messages indicating that these specific command lines failed.

Information About Configuration Replace and Configuration Rollback

Configuration Archive

The Cisco IOS configuration archive is intended to provide a mechanism to store, organize, and manage an archive of Cisco IOS configuration files to enhance the configuration rollback capability provided by the **configure replace** command. Before this feature was introduced, you could save copies of the running configuration using the **copy running-config destination-url** command, storing the replacement file either locally or remotely. However, this method lacked any automated file management. On the other hand, the Configuration Replace and Configuration Rollback feature provides the capability to automatically save copies of the running configuration to the Cisco IOS configuration archive. These archived files serve as checkpoint configuration references and can be used by the **configure replace** command to revert to previous configuration states.

The **archive config** command allows you to save Cisco IOS configurations in the configuration archive using a standard location and filename prefix that is automatically appended with an incremental version number (and optional timestamp) as each consecutive file is saved. This functionality provides a means for consistent identification of saved Cisco IOS configuration files. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved in the archive, the oldest file is automatically deleted when the next, most recent file is saved. The **show archive** command displays information for all configuration files saved in the Cisco IOS configuration archive.

The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the **configure replace** command, can be located on the following file systems: FTP, HTTP, RCP, TFTP.

Configuration Replace

The **configure replace** privileged EXEC command provides the capability to replace the current running configuration with any saved Cisco IOS configuration file. This functionality can be used to revert to a previous configuration state, effectively rolling back any configuration changes that were made since the previous configuration state was saved.

When using the **configure replace** command, you must specify a saved Cisco IOS configuration as the replacement configuration file for the current running configuration. The replacement file must be a complete configuration generated by a Cisco IOS device (for example, a configuration generated by the **copy running-config destination-url** command), or, if generated externally, the replacement file must comply with the format of files generated by Cisco IOS devices. When the **configure replace** command is entered, the current running configuration is compared with the specified replacement configuration and a set of diffs is generated. The algorithm used to compare the two files is the same as that employed by the **show archive config differences** command. The resulting diffs are then applied by the Cisco IOS parser to achieve the replacement configuration state. Only the diffs are applied, avoiding potential service disruption from reapplying configuration commands that already exist in the current running configuration. This algorithm effectively handles configuration changes to order-dependent commands (such as access lists) through a multiple pass process. Under normal circumstances, no more than three passes are needed to complete a configuration replace operation, and a limit of five passes is performed to preclude any looping behavior.

The Cisco IOS **copy source-url running-config** privileged EXEC command is often used to copy a stored Cisco IOS configuration file to the running configuration. When using the **copy source-url running-config** command as an alternative to the **configure replace target-url** privileged EXEC command, the following major differences should be noted:

- The **copy source-url running-config** command is a merge operation and preserves all of the commands from both the source file and the current running configuration. This command does not remove commands from the current running configuration that are not present in the source file. In contrast, the **configure replace target-url** command removes commands from the current running configuration that are not present in the replacement file and adds commands to the current running configuration that need to be added.
- The **copy source-url running-config** command applies every command in the source file, whether or not the command is already present in the current running configuration. This algorithm is inefficient and, in some cases, can result in service outages. In contrast, the **configure replace target-url** command only applies the commands that need to be applied—no existing commands in the current running configuration are reapplied.
- A partial configuration file may be used as the source file for the **copy source-url running-config** command, whereas a complete Cisco IOS configuration file must be used as the replacement file for the **configure replace target-url** command.

A locking feature for the configuration replace operation was introduced. When the **configure replace** command is used, the running configuration file is locked by default for the duration of the configuration replace operation. This locking mechanism prevents other users from changing the running configuration while the replacement operation is taking place, which might otherwise cause the replacement operation to terminate unsuccessfully. You can disable the locking of the running configuration by using the **no lock** keyword when issuing the **configure replace** command.

The running configuration lock is automatically cleared at the end of the configuration replace operation. You can display any locks that may be currently applied to the running configuration using the **show configuration lock** command.

Configuration Rollback

The concept of rollback comes from the transactional processing model common to database operations. In a database transaction, you might make a set of changes to a given database table. You then must choose whether to commit the changes (apply the changes permanently) or to roll back the changes (discard the changes and revert to the previous state of the table). In this context, rollback means that a journal file containing a log of the changes is discarded, and no changes are applied. The result of the rollback operation is to revert to the previous state, before any changes were applied.

The **configure replace** command allows you to revert to a previous configuration state, effectively rolling back changes that were made since the previous configuration state was saved. Instead of basing the rollback operation on a specific set of changes that were applied, the Cisco IOS configuration rollback capability uses the concept of reverting to a specific configuration state based on a saved Cisco IOS configuration file. This concept is similar to the database idea of saving a checkpoint (a saved version of the database) to preserve a specific state.

If the configuration rollback capability is desired, you must save the Cisco IOS running configuration before making any configuration changes. Then, after entering configuration changes, you can use that saved configuration file to roll back the changes (using the **configure replace target-url** command). Furthermore, because you can specify any saved Cisco IOS configuration file as the replacement configuration, you are not limited to a fixed number of rollbacks, as is the case in some rollback models.

Configuration Rollback Confirmed Change

The Configuration Rollback Confirmed Change feature allows configuration changes to be performed with an optional requirement that they be confirmed. If this confirmation is not received, the configuration is returned to the state prior to the changes being applied. The mechanism provides a safeguard against inadvertent loss of connectivity between a network device and the user or management application due to configuration changes.

Benefits of Configuration Replace and Configuration Rollback

- Allows you to revert to a previous configuration state, effectively rolling back configuration changes.
- Allows you to replace the current running configuration file with the startup configuration file without having to reload the device or manually undo CLI changes to the running configuration file, therefore reducing system downtime.
- Allows you to revert to any saved Cisco IOS configuration state.
- Simplifies configuration changes by allowing you to apply a complete configuration file to the device, where only the commands that need to be added or removed are affected.
- When using the **configure replace** command as an alternative to the **copy source-url running-config** command, increases efficiency and prevents risk of service outages by not reapplying existing commands in the current running configuration.

How to Use Configuration Replace and Configuration Rollback

Creating a Configuration Archive

No prerequisite configuration is needed to use the **configure replace** command. Using the **configure replace** command in conjunction with the Cisco IOS configuration archive and the **archive config** command is optional but offers significant benefit for configuration rollback scenarios. Before using the **archive config** command, the configuration archive must be configured. Perform this task to configure the characteristics of the configuration archive.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | archive Example: <pre>Device(config)# archive</pre> | Enters archive configuration mode. |
| Step 4 | path <i>url</i> Example: <pre>Device(config-archive)# path flash:myconfiguration</pre> | Specifies the location and filename prefix for the files in the Cisco IOS configuration archive. Note If a directory is specified in the path instead of file, the directory name must be followed by a forward slash as follows: path flash:/directory/. The forward slash is not necessary after a filename; it is only necessary when specifying a directory. |
| Step 5 | maximum <i>number</i> Example: <pre>Device(config-archive)# maximum 14</pre> | (Optional) Sets the maximum number of archive files of the running configuration to be saved in the Cisco IOS configuration archive. <ul style="list-style-type: none"> • The <i>number</i> argument is the maximum number of archive files of the running configuration to be saved in the Cisco IOS |

| | Command or Action | Purpose |
|---------------|--|--|
| | | configuration archive. Valid values are from 1 to 14. The default is 10. Note Before using this command, you must configure the path command to specify the location and filename prefix for the files in the Cisco IOS configuration archive. |
| Step 6 | time-period <i>minutes</i> Example: Device(config-archive)# time-period 1440 | (Optional) Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco IOS configuration archive. • The <i>minutes</i> argument specifies how often, in minutes, to automatically save an archive file of the current running configuration in the Cisco IOS configuration archive. Note Before using this command, you must configure the path command to specify the location and filename prefix for the files in the Cisco IOS configuration archive. |
| Step 7 | end Example: Device(config-archive)# end | Exits to privileged EXEC mode. |
| Step 8 | archive config Example: Device# archive config | Saves the current running configuration file to the configuration archive. Note The path command must be configured before using this command. |

Performing a Configuration Replace or Configuration Rollback Operation

Perform this task to replace the current running configuration file with a saved Cisco IOS configuration file.



Note You must create a configuration archive before performing this procedure. See [Creating a Configuration Archive](#) for detailed steps. The following procedure details how to return to that archived configuration in the event of a problem with the current running configuration.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure replace <i>target-url</i> [nolock] [list] [force] [ignore case] [revert trigger [error]] [timer <i>minutes</i>] time <i>minutes</i>]] Example: <pre>Device# configure replace flash: startup-config time 120</pre> | Replaces the current running configuration file with a saved Cisco IOS configuration file. <ul style="list-style-type: none"> • The <i>target - url</i> argument is a URL (accessible by the Cisco IOS file system) of the saved Cisco IOS configuration file that is to replace the current running configuration, such as the configuration file created using the archive config command. • The list keyword displays a list of the command lines applied by the Cisco IOS software parser during each pass of the configuration replace operation. The total number of passes performed is also displayed. • The force keyword replaces the current running configuration file with the specified saved Cisco IOS configuration file without prompting you for confirmation. • The time <i>minutes</i> keyword and argument specify the time (in minutes) within which you must enter the configure confirm command to confirm replacement of the current running configuration file. If the configure confirm command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the configure replace command). • The nolock keyword disables the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replace operation. |

| | Command or Action | Purpose |
|---------------|---|---|
| | | <ul style="list-style-type: none"> The revert trigger keywords set the following triggers for reverting to the original configuration: <ul style="list-style-type: none"> error —Reverts to the original configuration upon error. timer minutes —Reverts to the original configuration if specified time elapses. The ignore case keyword allows the configuration to ignore the case of the confirmation command. |
| Step 3 | configure revert { now timer { minutes idle minutes } } Example: Device# configure revert now | (Optional) To cancel the timed rollback and trigger the rollback immediately, or to reset parameters for the timed rollback, use the configure revert command in privileged EXEC mode. <ul style="list-style-type: none"> now —Triggers the rollback immediately. timer —Resets the configuration revert timer. <ul style="list-style-type: none"> Use the <i>minutes</i> argument with the timer keyword to specify a new revert time in minutes. Use the idle keyword along with a time in minutes to set the maximum allowable time period of no activity before reverting to the saved configuration. |
| Step 4 | configure confirm Example: Device# configure confirm | (Optional) Confirms replacement of the current running configuration file with a saved Cisco IOS configuration file. Note Use this command only if the time seconds keyword and argument of the configure replace command are specified. |
| Step 5 | exit Example: Device# exit | Exits to user EXEC mode. |

Monitoring and Troubleshooting the Feature

Perform this task to monitor and troubleshoot the Configuration Replace and Configuration Rollback feature.

Procedure

Step 1 enable

Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
Device> enable
Device#
```

Step 2 show archive

Use this command to display information about the files saved in the Cisco IOS configuration archive.

Example:

```
Device# show archive
There are currently 1 archive configurations saved.
The next archive file will be named flash:myconfiguration-2
Archive #   Name
0
1          flash:myconfiguration-1 <- Most Recent
2
3
4
5
6
7
8
9
10
11
12
13
14
```

The following is sample output from the **show archive** command after several archive files of the running configuration have been saved. In this example, the maximum number of archive files to be saved is set to three.

Example:

```
Device# show archive
There are currently 3 archive configurations saved.
The next archive file will be named flash:myconfiguration-8
Archive #   Name
0
1          :Deleted
2          :Deleted
3          :Deleted
4          :Deleted
5          flash:myconfiguration-5
6          flash:myconfiguration-6
7          flash:myconfiguration-7 <- Most Recent
```

```

8
9
10
11
12
13
14

```

Step 3 debug archive versioning

Use this command to enable debugging of the Cisco IOS configuration archive activities to help monitor and troubleshoot configuration replace and rollback.

Example:

```

Device# debug archive versioning
Jan  9 06:46:28.419:backup_running_config
Jan  9 06:46:28.419:Current = 7
Jan  9 06:46:28.443:Writing backup file flash:myconfiguration-7
Jan  9 06:46:29.547: backup worked

```

Step 4 debug archive config timestamp

Use this command to enable debugging of the processing time for each integral step of a configuration replace operation and the size of the configuration files being handled.

Example:

```

Device# debug archive config timestamp
Device# configure replace flash:myconfiguration force
Timing Debug Statistics for IOS Config Replace operation:
  Time to read file usbflash0:sample_2.cfg = 0 msec (0 sec)
  Number of lines read:55
  Size of file          :1054
Starting Pass 1
  Time to read file system:running-config = 0 msec (0 sec)
  Number of lines read:93
  Size of file          :2539
  Time taken for positive rollback pass = 320 msec (0 sec)
  Time taken for negative rollback pass = 0 msec (0 sec)
  Time taken for negative incremental diffs pass = 59 msec (0 sec)
  Time taken by PI to apply changes = 0 msec (0 sec)
  Time taken for Pass 1 = 380 msec (0 sec)
Starting Pass 2
  Time to read file system:running-config = 0 msec (0 sec)
  Number of lines read:55
  Size of file          :1054
  Time taken for positive rollback pass = 0 msec (0 sec)
  Time taken for negative rollback pass = 0 msec (0 sec)
  Time taken for Pass 2 = 0 msec (0 sec)
Total number of passes:1
Rollback Done

```

Step 5 exit

Use this command to exit to user EXEC mode.

Example:

```
Device# exit
Device>
```

Configuration Examples for Configuration Replace and Configuration Rollback

Creating a Configuration Archive

The following example shows how to perform the initial configuration of the Cisco IOS configuration archive. In this example, flash:myconfiguration is specified as the location and filename prefix for the files in the configuration archive and a value of 10 is set as the maximum number of archive files to be saved.

```
configure terminal
!
archive
 path flash:myconfiguration
 maximum 10
end
```

Replacing the Current Running Configuration with a Saved Cisco IOS Configuration File

The following example shows how to replace the current running configuration with a saved Cisco IOS configuration file named flash:myconfiguration. The **configure replace** command interactively prompts you to confirm the operation.

```
Device# configure replace flash:myconfiguration
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
```

In the following example, the **list** keyword is specified in order to display the command lines that were applied during the configuration replace operation:

```
Device# configure replace flash:myconfiguration list
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
!Pass 1
!List of Commands:
no snmp-server community public ro
```

```
snmp-server community mystring ro

end
Total number of passes: 1
Rollback Done
```

Reverting to the Startup Configuration File

The following example shows how to revert to the Cisco IOS startup configuration file using the **configure replace** command. This example also shows the use of the optional **force** keyword to override the interactive user prompt:

```
Device# configure replace flash:startup-config force
Total number of passes: 1
Rollback Done
```

Performing a Configuration Replace Operation with the **configure confirm** Command

The following example shows the use of the **configure replace** command with the **time minutes** keyword and argument. You must enter the **configure confirm** command within the specified time limit to confirm replacement of the current running configuration file. If the **configure confirm** command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the **configure replace** command).

```
Device# configure replace flash:startup-config time 120
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
Device# configure confirm
```

The following example shows the use of the **configure revert** command with the **timer** keyword. You must enter the **configure revert** command to cancel the timed rollback and trigger the rollback immediately, or to reset parameters for the timed rollback.

```
Device# configure revert timer 100
```

Performing a Configuration Rollback Operation

The following example shows how to make changes to the current running configuration and then roll back the changes. As part of the configuration rollback operation, you must save the current running configuration before making changes to the file. In this example, the **archive config** command is used to save the current running configuration. The generated output of the **configure replace** command indicates that only one pass was performed to complete the rollback operation.



Note Before using the **archive config** command, you must configure the **path** command to specify the location and filename prefix for the files in the Cisco IOS configuration archive.

You first save the current running configuration in the configuration archive as follows:

```
archive config
```

You then enter configuration changes as shown in the following example:

```
configure terminal
!  
user netops2 password rain  
user netops3 password snow  
exit
```

After having made changes to the running configuration file, assume you now want to roll back these changes and revert to the configuration that existed before the changes were made. The **show archive** command is used to verify the version of the configuration to be used as a replacement file. The **configure replace** command is then used to revert to the replacement configuration file as shown in the following example:

```
Device# show archive  
There are currently 1 archive configurations saved.  
The next archive file will be named flash:myconfiguration-2  
Archive #   Name  
0  
1          flash:myconfiguration-1 <- Most Recent  
2  
3  
4  
5  
6  
7  
8  
9  
10  
Device# configure replace flash:myconfiguration-1  
Total number of passes: 1  
Rollback Done
```

Additional References for Configuration Replace and Configuration Rollback

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

Feature History for Configuration Replace and Configuration Rollback

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|--|--|
| Cisco IOS XE Gibraltar 16.11.1 | Configuration Replace and Configuration Rollback | The Cisco IOS configuration archive is intended to provide a mechanism to store, organize, and manage an archive of Cisco IOS configuration files to enhance the configuration rollback capability provided by the configure replace command. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 12

BIOS Protection

- [Introduction to BIOS Protection, on page 189](#)
- [ROMMON Upgrade, on page 189](#)
- [Feature History for BIOS Protection, on page 190](#)

Introduction to BIOS Protection

BIOS protection feature enables write-protection and secure upgrade of the golden ROMMON image. ROMMON is a bootstrap program that initializes the hardware and boots the Cisco IOS XE software image when you power on or restart the device. ROMMON upgrades can be required to resolve firmware defects or to support new features. Typically, ROM Monitor upgrades are infrequent and not required for every Cisco IOS XE software upgrade.

Without BIOS protection feature, golden ROMMON may be corrupted by malicious code during software upgrades.

ROMMON Upgrade

ROMMON images are stored on the SPI flash device as primary ROMMON and golden ROMMON. Primary ROMMON boots every time the device is powered on or restarted. If the primary ROMMON gets corrupted, the device uses the golden ROMMON to boot the IOS XE software image. When the device boots from the primary ROMMON, golden ROMMON is locked. With BIOS protection, golden ROMMON is made write-protected and cannot be upgraded using the flash utility upgrade mechanism. Access policies are governed by the FPGA firmware. FPGA blocks the disallowed operations such as write, erase etc on the golden ROMMON SPI flash device.



Note Golden ROMMON upgrade is not enabled without secure-boot FPGA upgrade.

Primary ROMMON, primary FPGA and golden FPGA (secure-boot FPGA) is automatically upgraded when the device boots. Golden ROMMON can only be upgraded using the capsule upgrade.

The upgrade process varies between standalone and high availability systems and is explained below.

Standalone Systems

For a standalone device, when you upgrade the device in install mode, the primary ROMMON is automatically upgraded when the device boots. Golden ROMMON can be upgraded using the capsule upgrade.

High Availability and StackWise Virtual Systems

We recommend that you perform In-Service-Software-Upgrade (ISSU) for devices in a high availability setup. FPGA upgrades occur as part of ISSU.

If you are performing the upgrade in install mode with reload, do not reload both the supervisors at the same time. With the standby supervisor in ROMMON state, boot the active supervisor. When ROMMON upgrade is completed on each supervisor, FPGA and software image is upgraded.

Boot the standby supervisor and allow the standby supervisor to upgrade and reach standby hot state.

Capsule Upgrade

In a capsule upgrade, a secure update capsule is created and signed which is used by the primary ROMMON after authentication for upgrading the golden ROMMON. The secure update capsule requires a secure flash certificate. Secure flash certificate is created using the product key and added to the primary ROMMON image to verify the authenticity of the update capsule. A capsule is now created using the secure flash certificate and a secure boot 16 MB flash image and signed.

When the device boots, the primary ROMMON triggers the capsule upgrade for the golden ROMMON. To perform capsule upgrade for the golden ROMMON, use the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode.

The following processes occur in a capsule upgrade:

- The device checks if secure-boot FPGA upgrade is enabled. If not, the process exits.
- The device checks if bootloader protection is enabled. If not, a one-time upgrade of primary ROMMON, golden ROMMON, and primary FPGA is initiated.
- If bootloader protection is already active, IOS copies the secure update capsule to bootflash and the device reboots.
- When the device reboots, secure update capsule is picked for performing the upgrade.

Feature History for BIOS Protection

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|-----------------------------------|-----------------|---|
| Cisco IOS XE Gibraltar 16.12.1 | BIOS Protection | BIOS Protection feature enables write-protection and secure upgrade of the golden ROMMON image. |

| Release | Feature | Feature Information |
|-------------------------------|-----------------|---|
| Cisco IOS XE Amsterdam 17.1.1 | Capsule Upgrade | Support for capsule upgrade for golden ROMMON using upgrade rom-monitor capsule switch active command was enabled. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 13

Software Maintenance Upgrade

The Software Maintenance Upgrade (SMU) is a package that can be installed on a system to provide a fix or a security resolution to a released image.

- [Restrictions for Software Maintenance Upgrade, on page 193](#)
- [Information About Software Maintenance Upgrade, on page 193](#)
- [How to Manage Software Maintenance Updates, on page 194](#)
- [Configuration Examples for Software Maintenance Upgrade, on page 196](#)
- [Additional References for Software Maintenance Upgrade, on page 201](#)
- [Feature History for Software Maintenance Upgrade, on page 202](#)

Restrictions for Software Maintenance Upgrade

- SMU supports patching using install mode only.

Information About Software Maintenance Upgrade

SMU Overview

The SMU is a package that can be installed on a system to provide a fix or a security resolution to a released image. An SMU package is provided on a per release and per component basis.

An SMU provides a significant benefit over classic Cisco IOS software because it allows you to address network issues quickly while reducing the time and scope of the testing required. The Cisco IOS XE platform internally validates SMU compatibility and does not allow you to install noncompatible SMUs.

All the SMUs are integrated into the subsequent Cisco IOS XE software maintenance releases. An SMU is an independent and self-sufficient package and it does not have any prerequisites or dependencies. You can choose which SMUs to install or uninstall in any order.

SMUs are supported only on Extended Maintenance releases and for the full lifecycle of the underlying software release.

Perform these basic steps to install an SMU:

1. Add the SMU to the filesystem.

2. Activate the SMU on the system.
3. Commit the SMU changes so that it is persistent across reloads.

SMU Workflow

The SMU process is initiated with a request to the Cisco Customer Support. Contact your customer support to raise an SMU request.

At release time, the SMU package is posted to the [Cisco Software Download](#) page and can be downloaded and installed.

SMU Package

The SMU package contains a small set of files for patching the release along with metadata that describes the contents of the package, and fix for the reported issue that the SMU is requested for.

SMU Reload

The SMU type describes the effect the installed SMU has on the corresponding system. SMUs might not have an impact on traffic, or might result in device restart, reload, or switchover. Run the **show install package flash: filename** command to verify whether a reload is required or not.

Hot patching enables SMU to take effect after activation without the system having to be reloaded. After the SMU is committed, the changes are persistent across reloads. In certain cases, SMUs may require a cold (complete) reload of the operating system. This action affects the traffic flow for the duration of the reload. If a cold reload is required, users will be prompted to confirm the action.

How to Manage Software Maintenance Updates

The following sections provide information about managing SMUs.

You can install, activate, and commit an SMU package using a single command (1-step process) or using separate commands (3-step process).



Tip Use the 1-step process when you have to install just one SMU package file and use the 3-step process when you have to install multiple SMUs. The 3-step process minimises the number of reloads required when you have more than one SMU package file to install.

Installing an SMU Package

This task shows how to use the **install add file activate commit** command for installing an SMU package.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | install add file flash: <i>filename</i> [activate commit] Example: Device# install add file flash:cat9k_iosxe.BLD_SMU_20180302_085005- TWIG_LATEST_20180306_013805.3.SSA.smu.bin activate commit | Copies the maintenance update package from a remote location (through FTP, HTTP, HTTPS, or TFTP) to the device, performs a compatibility check for the platform and image versions, activates the SMU package, and makes the package persistent across reloads. This command extracts the individual components of the .bin file into the subpackages and packages.conf files. Note If the SMU file is copied using tftp, use bootflash to activate the SMU. |
| Step 3 | exit Example: Device# exit | Exits privileged EXEC mode and returns to user EXEC mode. |

Managing an SMU Package

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | install add file flash: <i>filename</i> Example: Device# install add file flash:cat9k_iosxe.BLD_SMU_20180302_085005- TWIG_LATEST_20180306_013805.3.SSA.smu.bin | Copies the SMU package from a source location to the device (in case source location is remote), and then performs a compatibility check for the platform and image versions, and adds the SMU package on all member nodes or FRUs, as applicable. This command also runs base compatibility checks on a file to ensure that the SMU package is supported on the platform. It also adds an entry in the package/SMU.sta file, so that its status can be monitored and maintained. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 3 | install activate file flash: <i>filename</i> Example: <pre>Device# install activate add file flash:cat9k_iosxe.BLD_SMU_20180302_085005_ TWIG_LATEST_20180306_013805.3.SSA.smu.bin</pre> | Runs compatibility checks, installs the package, and updates the package status details. |
| Step 4 | install commit Example: <pre>Device# install commit</pre> | Commits the activation changes to be persistent across reloads. The commit can be done after activation when the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload. |
| Step 5 | install rollback to {base committed id commit-ID} Example: <pre>Device# install rollback to committed</pre> | Returns the device to the previous installation state. |
| Step 6 | install deactivate file flash: <i>filename</i> Example: <pre>Device# install deactivate file flash:cat9k_iosxe.BLD_SMU_20180302_085005_ TWIG_LATEST_20180306_013805.3.SSA.smu.bin</pre> | Deactivates an active package and updates the package status. |
| Step 7 | install remove {file flash: <i>filename</i> inactive} Example: <pre>Device# install remove file flash:cat9k_iosxe.BLD_SMU_20180302_085005_ TWIG_LATEST_20180306_013805.3.SSA.smu.bin</pre> | Verifies if the specified SMU is inactive and if it is, deletes it from the file system. The inactive option deletes all the inactive packages from the file system. |
| Step 8 | show version Example: <pre>Device# show version</pre> | Displays the image version on the device. |
| Step 9 | show install summary Example: <pre>Device# show install summary</pre> | Displays information about the installation status of packages. The output of this command varies according to the install commands that are configured. |

Configuration Examples for Software Maintenance Upgrade

The following is a list of SMU configuration examples.

Example: Managing an SMU



Note

- The examples used in this section are of hot patching SMU.

The following example shows how to copy an SMU file to flash:

```
Device# copy ftp://172.16.0.10//auto/ftpboot/user/
cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

flash:
Destination filename
[cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin]?
Accessing ftp://172.16.0.10//auto/ftpboot/folder1/
cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin...
Loading /auto/ftpboot/folder1/
cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin from
172.16.0.10 (via GigabitEthernet0): !
[OK - 17668 bytes]
17668 bytes copied in 0.058 secs (304621 bytes/sec)
```

The following example shows how to add a maintenance update package file:

```
Device# install add file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

install_add: START Mon Mar  5 21:48:51 PST 2018
install_add: Adding SMU

--- Starting initial file syncing ---
Info: Finished copying
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin to the
selected switch(es)
Finished initial file syncing

Executing pre scripts....

Executing pre scripts done.
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:49:00 PST 2018
```

The following is a sample output from the **show install summary** command after adding an SMU package file to the device:

```
Device# show install summary

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
```

Example: Managing an SMU

```

-----
Type  St   Filename/Version
-----
SMU   I    flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin
IMG   C    16.9.1.0.43131
-----

Auto abort timer: inactive
-----

```

The following example shows how to activate an added SMU package file:

```

Device# install activate file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

install_activate: START Mon Mar  5 21:49:22 PST 2018
install_activate: Activating SMU
Executing pre scripts....

Executing pre scripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
  [1] SMU_ACTIVATE package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

SUCCESS: install_activate
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:49:34 PST 2018

```

The following is a sample output from the **show version** command:

```

Device# show version

Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20180302_085005_2 - SMU-PATCHED
Cisco IOS Software [Fujii], Catalyst L3 Switch Software (CAT9K_IOSXE), Experimental Version
 16.9.20180302:
085957 [polaris_dev-/nobackup/mcpre/BLD-BLD_POLARIS_DEV_LATEST_20180302_085005 166]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 02-Mar-18 09:50 by mcpre
...

```

The following is a sample output from the **show install summary** command displays the status of the SMU package as active and uncommitted:

```

Device# show install summary

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
SMU   U    flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin
IMG   C    16.9.1.0.43131
-----

Auto abort timer: active on install_activate, time before rollback - 01:59:50

```

The following is a sample output from the **show install active** command:

```
Device# show install active

[ Switch 1 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
SMU   U    flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin
IMG   C    16.9.1.0.43131
```

The following example shows how to execute the **install commit** command:

```
Device# install commit

install_commit: START Mon Mar  5 21:50:52 PST 2018
install_commit: Committing SMU
Executing pre scripts....

Executing pre scripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
  [1] SMU_COMMIT package(s) on switch 1
  [1] Finished SMU_COMMIT on switch 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

SUCCESS: install_commit
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:51:01 PST 2018
```

The following is a sample output from the **show install summary** command displays that the update package is now committed, and that it will be persistent across reloads:

```
Device# show install summary

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
SMU   C    flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin
IMG   C    16.9.1.0.43131

-----
Auto abort timer: inactive
-----
```

The following example shows how to rollback an update package to the committed package:

```
Device# install rollback to committed

install_rollback: START Mon Mar  5 21:52:18 PST 2018
install_rollback: Rolling back SMU
Executing pre scripts....
```

Example: Managing an SMU

```

Executing pre scripts done.

--- Starting SMU Rollback operation ---
Performing SMU_ROLLBACK on all members
  [1] SMU_ROLLBACK package(s) on switch 1
  [1] Finished SMU_ROLLBACK on switch 1
Checking status of SMU_ROLLBACK on [1]
SMU_ROLLBACK: Passed on [1]
Finished SMU Rollback operation

SUCCESS: install_rollback
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:52:30 PST 2018

```

The following is a sample output from the **show install summary** command:

```

Device# show install summary

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
IMG   C    16.9.1.0.43131
-----

Auto abort timer: inactive
-----

```

The following example shows how to deactivate an SMU package file:

```

Device# install deactivate file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

install_deactivate: START Mon Mar  5 21:54:06 PST 2018
install_deactivate: Deactivating SMU
Executing pre scripts....

Executing pre scripts done.

--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on all members
  [1] SMU_DEACTIVATE package(s) on switch 1
  [1] Finished SMU_DEACTIVATE on switch 1
Checking status of SMU_DEACTIVATE on [1]
SMU_DEACTIVATE: Passed on [1]
Finished SMU Deactivate operation

SUCCESS: install_deactivate
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:54:17 PST 2018

```

The following is a sample output from the **show install summary** command:

```

Device# show install summary

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----

```

```
SMU   D   flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin
IMG   C   16.9.1.0.43131
```

```
-----
Auto abort timer: active on install_deactivate, time before rollback - 01:59:50
-----
```

The following example shows how to remove an SMU from the device:

```
Device# install remove file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

install_remove: START Mon Mar  5 22:03:50 PST 2018
install_remove: Removing SMU
Executing pre scripts....

Executing pre scripts done.

--- Starting SMU Remove operation ---
Performing SMU_REMOVE on all members
  [1] SMU_REMOVE package(s) on switch 1
  [1] Finished SMU_REMOVE on switch 1
Checking status of SMU_REMOVE on [1]
SMU_REMOVE: Passed on [1]
Finished SMU Remove operation

SUCCESS: install_remove
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 22:03:58 PST 2018
```

The following is a sample output from the **show install summary** command:

```
Device# show install summary

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
IMG   C    16.9.1.0.43131
-----

Auto abort timer: inactive
-----
```

Additional References for Software Maintenance Upgrade

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

Feature History for Software Maintenance Upgrade

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|------------------------------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Software Maintenance Upgrade (SMU) | An SMU is a package that can be installed on a system to provide a fix or a security resolution to a released image. Feature support includes hot patching and PKI patching support. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 14

Working with the Flash File System

- [Information About the Flash File System, on page 203](#)
- [Displaying Available File Systems, on page 203](#)
- [Setting the Default File System, on page 205](#)
- [Displaying Information About Files on a File System, on page 205](#)
- [Changing Directories and Displaying the Working Directory , on page 206](#)
- [Creating Directories , on page 207](#)
- [Copying Files, on page 207](#)
- [Creating, Displaying and Extracting Files , on page 209](#)
- [Additional References for Flash File System, on page 210](#)
- [Feature History for Flash File System, on page 211](#)

Information About the Flash File System

The flash file system is a single flash device on which you can store files. It also provides several commands to help you manage software bundles and configuration files. The default flash file system on the device is named flash:.

As viewed from the active device, flash: refers to the local flash device, which is the device attached to the same device on which the file system is being viewed. In a device stack, each of the flash devices from the various stack members can be viewed from the active device. The names of these flash file systems include the corresponding device member numbers. For example, flash-3:, as viewed from the active device, refers to the same file system as does flash: on stack member 3. Use the **show file systems** privileged EXEC command to list all file systems, including the flash file systems in the device stack.

Only one user at a time can manage the software bundles and configuration files for a device stack.

Displaying Available File Systems

To display the available file systems on your device, use the **show file systems** privileged EXEC command as shown in this example for a standalone device:

Table 14: show file systems Field Descriptions

| Field | Value |
|----------|---|
| Size(b) | Amount of memory in the file system in bytes. |
| Free(b) | Amount of free memory in the file system in bytes. |
| Type | <p>Type of file system.</p> <p>disk—The file system is for a flash memory device, USB flash, and crashinfo file.</p> <p>network—The file system for network devices; for example, an FTP server or and HTTP server.</p> <p>nvr—The file system is for a NVRAM device.</p> <p>opaque—The file system is a locally generated pseudo file system (for example, the system) or a download interface, such as brimux.</p> <p>unknown—The file system is an unknown type.</p> |
| Flags | <p>Permission for file system.</p> <p>ro—read-only.</p> <p>rw—read/write.</p> <p>wo—write-only.</p> |
| Prefixes | <p>Alias for file system.</p> <p>crashinfo:—Crashinfo file.</p> <p>flash:—Flash file system.</p> <p>ftp:—FTP server.</p> <p>http:—HTTP server.</p> <p>https:—Secure HTTP server.</p> <p>nvr:—NVRAM.</p> <p>null:—Null destination for copies. You can copy a remote file to null to find its size.</p> <p>rcp:—Remote Copy Protocol (RCP) server.</p> <p>scp:—Session Control Protocol (SCP) server.</p> <p>system:—Contains the system memory, including the running configuration.</p> <p>tftp:—TFTP network server.</p> <p>usbflash0:—USB flash memory.</p> <p>y—Obtain the file from a network machine by using the Ymodem protocol.</p> |

Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the **cd** *filesystem:* privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

By default, the default file system is *flash:*.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

Displaying Information About Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command. To display information about files on a file system, use one of the privileged EXEC commands listed in the following table.

Table 15: Commands for Displaying Information About Files

| Command | Description |
|---|---|
| dir [/all] [<i>filesystem:filename</i>] | Displays a list of files on a file system. |
| show file systems | Displays more information about each of the files on a file system. |
| show file information <i>file-url</i> | Displays information about a specific file. |
| show file descriptors | Displays a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open. |

For example, to display a list of all files in a file system, use the **dir** privileged EXEC command:

```
Device# dir flash:
Directory of bootflash:/

616513  drwx           4096  Jul 15 2015 07:11:35 +00:00  .installer
608402  -rw-          33818  Sep 25 2015 11:41:35 +00:00  bootloader_evt_handle.log
608403  drwx           4096  Feb 27 2017 13:56:47 +00:00  .ssh
608410  -rw-             0   Jun 5 2015 10:16:17 +00:00  dc_stats.txt
608411  drwx          20480  Sep 23 2015 11:50:13 +00:00  core
624625  drwx           4096  Sep 23 2015 12:29:27 +00:00  .prst_sync
640849  drwx           4096  Feb 27 2017 13:57:30 +00:00  .rollback_timer
608412  drwx           4096  Jun 17 2015 18:12:47 +00:00  orch_test_logs
608413  -rw-       33554432  Sep 25 2015 11:43:15 +00:00  nvram_config
608417  -rw-             35  Sep 25 2015 20:17:42 +00:00  pnp-tech-time
608439  -rw-        214054  Sep 25 2015 20:17:48 +00:00  pnp-tech-discovery-summary
608419  drwx           4096  Jul 23 2015 07:50:25 +00:00  util
```

```

616514 drwx          4096 Mar 18 2015 11:09:04 +00:00 onep
608442 -rw-           556 Mar 18 2015 11:19:34 +00:00 vlan.dat
608448 -rw-        1131779 Mar 28 2015 13:13:48 +00:00 log.txt
616516 drwx          4096 Apr 1 2015 09:34:56 +00:00 gs_script
616517 drwx          4096 Apr 6 2015 09:42:38 +00:00 tools
608440 -rw-           252 Sep 25 2015 11:41:52 +00:00 boothelper.log
624626 drwx          4096 Apr 17 2015 06:10:55 +00:00 SD_AVC_AUTO_CONFIG
608488 -rw-        98869 Sep 25 2015 11:42:15 +00:00 memleak.tcl
608437 -rw-        17866 Jul 16 2015 04:01:10 +00:00 ardbeg_x86
632745 drwx          4096 Aug 20 2015 11:35:09 +00:00 CRDU
632746 drwx          4096 Sep 16 2015 08:57:44 +00:00 ardmore
608418 -rw-       1595361 Jul 8 2015 11:18:33 +00:00
system-report_RP_0_20150708-111832-UTC.tar.gz
608491 -rw-        67587176 Aug 12 2015 05:30:35 +00:00 mcln_x86_kernel_20170628.SSA
608492 -rw-       74880100 Aug 12 2015 05:30:57 +00:00 stardust.x86.idprom.0718B

11250098176 bytes total (9128050688 bytes free)
Device#

```

Changing Directories and Displaying the Working Directory

Follow these steps to change directories and to display the working directory:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | dir filesystem: Example: Device# dir flash: | Displays the directories on the specified file system. For <i>filesystem:</i> , use flash: for the system board flash device. |
| Step 3 | cd directory_name Example: Device# cd new_configs | Navigates to the specified directory. The command example shows how to navigate to the directory named <i>new_configs</i> . |
| Step 4 | pwd Example: Device# pwd | Displays the working directory. |
| Step 5 | cd Example: Device# cd | Navigates to the default directory. |

Creating Directories

Beginning in privileged EXEC mode, follow these steps to create a directory:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | dir <i>filesystem:</i> Example: Device# dir flash: | Displays the directories on the specified file system. For <i>filesystem:</i> , use flash: for the system board flash device. |
| Step 2 | mkdir <i>directory_name</i> Example: Device# mkdir new_configs | Creates a new directory. Directory names are case sensitive and are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, slashes, quotes, semicolons, or colons. |
| Step 3 | dir <i>filesystem:</i> Example: Device# dir flash: | Verifies your entry. |

Removing Directories

To remove a directory with all its files and subdirectories, use the **delete /force /recursive** *filesystem:/file-url* privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process.

For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the name of the directory to be deleted. All of the files in the directory and the directory are removed.



Caution When directories are deleted, their contents cannot be recovered.

Copying Files

To copy a file from a source to a destination, use the **copy** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

You can also copy from special file systems (**xmodem:**, **ymodem:**) as the source for the file from a network machine that uses the Xmodem or Ymodem protocol. SSH File Transfer Protocol (SFTP) is also another option to copy switch configuration or image files. For more information, refer the *Configuring SSH File Transfer Protocol* chapter of the *Security Configuration Guide*.

Network file system URLs include ftp:, rcp:, tftp:, scp:, http:, and https: and have these syntaxes:

- FTP—ftp:[[/username [:password]@location]/directory]/filename
- RCP—rcp:[[/username@location]/directory]/filename
- TFTP—tftp:[[/location]/directory]/filename
- SCP—scp:[[/username [:password]@location]/directory]/filename
- HTTP—http:[[/username [:password]@location]/directory]/filename
- HTTPS—https:[[/username [:password]@location]/directory]/filename



Note The password must not contain the special character '@'. If the character '@' is used, the copy fails to parse the IP address of the server.

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration

Deleting Files

When you no longer need a file on a flash memory device, you can permanently delete it. To delete a file or directory from a specified flash device, use the **delete** [/force] [/recursive] [filesystem:]file-url privileged EXEC command.

Use the **/recursive** keyword for deleting a directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

If you omit the *filesystem:* option, the device uses the default device specified by the **cd** command. For *file-url*, you specify the path (directory) and the name of the file to be deleted.

When you attempt to delete any files, the system prompts you to confirm the deletion.



Caution When files are deleted, their contents cannot be recovered.

This example shows how to delete the file *myconfig* from the default flash memory device:

```
Device# delete myconfig
```

Creating, Displaying and Extracting Files

You can create a file and write files into it, list the files in a file, and extract the files from a file as described in the next sections.

Beginning in privileged EXEC mode, follow these steps to create a file, display the contents, and extract it:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | <p>archive tar /create <i>destination-url</i> flash: /<i>file-url</i></p> <p>Example:</p> <pre>Device# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs</pre> | <p>Creates a file and adds files to it.</p> <p>For <i>destination-url</i>, specify the destination URL alias for the local or network file system and the name of the file to create:</p> <ul style="list-style-type: none"> Local flash file system syntax: flash: FTP syntax: ftp:[[/<i>username</i>[:<i>password</i>]/@<i>location</i>]/<i>directory</i>]/-<i>filename</i>. RCP syntax: rcp:[[/<i>username</i>@<i>location</i>]/<i>directory</i>]/-<i>filename</i>. TFTP syntax: tftp:[[/<i>location</i>]/<i>directory</i>]/-<i>filename</i>. <p>For flash:/file-url, specify the location on the local flash file system in which the new file is created. You can also specify an optional list of files or directories within the source directory to add to the new file. If none are specified, all files and directories at this level are written to the newly created file.</p> |
| Step 2 | <p>archive tar /table <i>source-url</i></p> <p>Example:</p> <pre>Device# archive tar /table flash: /new_configs</pre> | <p>Displays the contents of a file.</p> <p>For <i>source-url</i>, specify the source URL alias for the local or network file system. The <i>-filename</i> is the file to display. These options are supported:</p> <ul style="list-style-type: none"> Local flash file system syntax: flash: FTP syntax: ftp:[[/<i>username</i>[:<i>password</i>]/@<i>location</i>]/<i>directory</i>]/-<i>filename</i>. RCP syntax: rcp:[[/<i>username</i>@<i>location</i>]/<i>directory</i>]/-<i>filename</i>. TFTP syntax: |

| | Command or Action | Purpose |
|---------------|---|--|
| | | tftp: [[//location]/directory]/-filename. You can also limit the file displays by specifying a list of files or directories after the file. Only those files appear. If none are specified, all files and directories appear. |
| Step 3 | archive tar /xtract source-url flash:/file-url [dir/file...] Example: <pre>Device# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs</pre> | Extracts a file into a directory on the flash file system. For <i>source-url</i> , specify the source URL alias for the local file system. The <i>-filename.</i> is the file from which to extract files. These options are supported: <ul style="list-style-type: none"> Local flash file system syntax: flash: FTP syntax: ftp[[//username[password]@location]/directory]/-filename. RCP syntax: rcp[[//username@location]/directory]/-filename. TFTP syntax: tftp[[//location]/directory]/-filename. For flash:/file-url [dir/file...] , specify the location on the local flash file system from which the file is extracted. Use the <i>dir/file...</i> option to specify a list of files or directories within the file to be extracted. If none are specified, all files and directories are extracted. |
| Step 4 | more [/ascii /binary /ebcdic] /file-url Example: <pre>Device# more flash:/new-configs</pre> | Displays the contents of any readable file, including a file on a remote file system. |

Additional References for Flash File System

Related Documents

| Related Topic | Document Title |
|---|---|
| Commands for managing flash: file systems | <i>Cisco IOS Configuration Fundamentals Command Reference</i> |

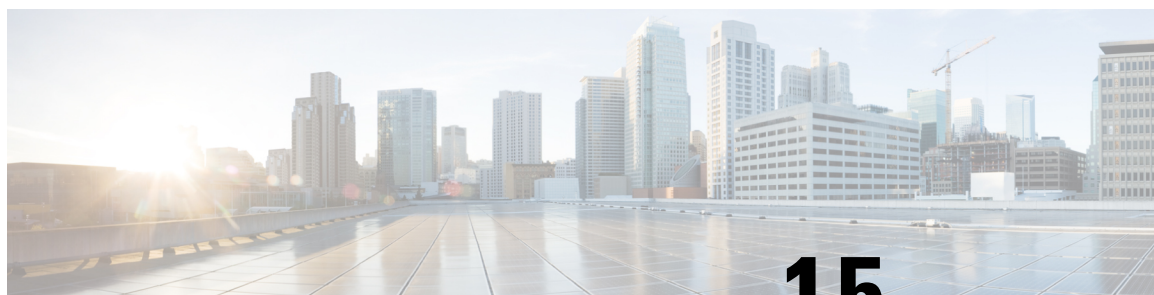
Feature History for Flash File System

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|-------------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Flash File System | The flash file system is a single flash device on which you can store files. It also provides several commands to help you manage software bundles and configuration files. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 15

Performing Factory Reset

- [Prerequisites for Performing a Factory Reset, on page 213](#)
- [Restrictions for Performing a Factory Reset, on page 213](#)
- [Information About Factory Reset, on page 213](#)
- [How to Perform a Factory Reset, on page 214](#)
- [Configuration Example for Performing a Factory Reset, on page 215](#)
- [Additional References for Factory Reset, on page 216](#)
- [Feature History for Performing a Factory Reset, on page 216](#)

Prerequisites for Performing a Factory Reset

- Ensure that all the software images, including the current image, configurations, and personal data are backed up before you begin the factory reset process.
- Ensure that there is uninterrupted power supply when the factory reset process is in progress.
- Ensure that In-Service Software Upgrade (ISSU) or In-Service Software Downgrade (ISSD) are not in progress before you begin the factory reset process.

Restrictions for Performing a Factory Reset

- Software patches, if installed on the device, will not be restored after the factory reset process.
- If the **factory-reset** command is issued through a VTY session, the session is not restored after completion of the factory reset process.
- Factory reset is supported only in standalone mode and not in stacking mode. For modular chassis devices configured in high-availability (HA) mode, factory reset is applied for each supervisor module.

Information About Factory Reset

Factory reset erases all the customer-specific data stored in a device and restores the device to its original configuration at the time of shipping. Data erased includes configurations, log files, boot variables, core files, and credentials like Federal Information Processing Standard-related (FIPS-related) keys.

The factory reset process is used in the following two scenarios:

- Return Material Authorization (RMA) for a device: If you have to return a device to Cisco for RMA, remove all the customer-specific data before obtaining an RMA certificate for the device.
- Recovering a compromised device: If the key material or credentials that are stored on a device is compromised, reset the device to factory configuration, and then reconfigure the device.

During the factory reset, the device reloads and enters ROMmon mode. After a factory reset, the device removes all its environment variables, including the **MAC_ADDRESS** and the **SERIAL_NUMBER** variables, which are required to locate and load the software. Perform a reset in ROMmon mode to automatically set the environment variables.

After the system reset in ROMmon mode is complete, add the Cisco IOS image either through a USB or TFTP.

The following table provides details about the data that is erased and retained during the factory reset process:

Table 16: Data Erased and Retained During Factory Reset

| Data Erased | Data Retained |
|---|--|
| All Cisco IOS images, including the current boot image | Data from remote field-replaceable units (FRUs) |
| Crash information and logs | Value of the configuration register. |
| User data, startup and running configuration, and contents of removable storage devices such as Serial Advanced Technology Attachment (SATA), Solid State Drive (SSD), or USB | — |
| Credentials such as FIPS-related keys | Credentials such as Secure Unique Device Identifier (SUDI) certificates, public key infrastructure (PKI) keys. |
| Onboard Failure Logging (OBFL) logs | |
| ROMmon variables added by the user. | — |
| Licenses | — |

How to Perform a Factory Reset

To perform a factory reset, complete this procedure:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | factory-reset {all config boot-vars} Example: Device# factory-reset all | Resets the device to its configuration at the time of its shipping. No system configuration is required to use the factory reset command. The following options are available: <ul style="list-style-type: none"> • all: Erases all the content from the NVRAM, all the Cisco IOS images, including the current boot image, boot variables, startup and running configuration data, and user data. Cisco recommends using the option all. • config: Resets the startup configurations. • boot-vars: Resets the user-added boot variables. After the factory reset process is successfully completed, the device reboots and enters ROMmon mode. |

Configuration Example for Performing a Factory Reset

The following example shows how to perform a factory reset:

```

Device> enable
Device# factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]

```

Additional References for Factory Reset

Related Documents

| Related Topic | Document Title |
|--|-----------------------------------|
| For complete syntax and usage information for the commands used in this chapter. | Command Reference |

Feature History for Performing a Factory Reset

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|---|--|
| Cisco IOS XE Gibraltar 16.11.1 | Factory Reset | Factory reset erases all the customer-specific data stored in a device and restores the device to its original configuration at the time of shipping |
| Cisco IOS XE Gibraltar 16.12.1 | Factory Reset for Removable Storage Devices | Performing a factory reset erases the contents of removable storage devices, such as SATA, SSD, or USB. |
| Cisco IOS XE Amsterdam 17.2.1 | Factory Reset with 3-pass Overwrite | A factory reset can be performed to erase all the content from the device securely with 3-pass overwrite. The secure 3-pass keyword was introduced. |
| | Enhanced Factory Reset Option for Stack and Cisco StackWise Virtual | Support for factory reset on stacked devices and for Cisco StackWise Virtual enabled devices is introduced. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 16

Configuring Secure Storage

- [Information About Secure Storage, on page 217](#)
- [Enabling Secure Storage , on page 217](#)
- [Disabling Secure Storage , on page 218](#)
- [Verifying the Status of Encryption, on page 218](#)
- [Feature Information for Secure Storage, on page 219](#)

Information About Secure Storage

Secure Storage feature allows you to secure critical configuration information by encrypting it. It encrypts asymmetric key-pairs, pre-shared secrets, the type 6 password encryption key and certain credentials. An instance-unique encryption key is stored in the hardware trust anchor to prevent it from being compromised.

Enabling Secure Storage

Before you begin

By default, this feature is enabled. Perform this procedure only after disabling secure storage on the device.

Procedure

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters the global configuration mode. |
| Step 2 | service private-config-encryption Example: DEvice(config)# service private-config-encryption | Enables the Secure Storage feature on your device. |
| Step 3 | end Example: | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Device(config)# end | |
| Step 4 | write memory Example: Device# write memory | Encrypts the private-config file and saves the file in an encrypted format. |

Disabling Secure Storage

Before you begin

To disable Secure Storage feature on a device, perform this task:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters the global configuration mode. |
| Step 2 | no service private-config-encryption Example: Device(config)# no service private-config-encryption | Disables the Secure Storage feature on your device. When secure storage is disabled, all the user data is stored in plain text in the NVRAM. |
| Step 3 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 4 | write memory Example: Device# write memory | Decrypts the private-config file and saves the file in plane format. |

Verifying the Status of Encryption

Use the **show parser encrypt file status** command to verify the status of encryption. The following command output indicates that the feature is available but the file is not encrypted. The file is in 'plain text' format.

```
Device#show parser encrypt file status
Feature: Enabled
File Format: Plain Text
Encryption Version: Ver1
```


Feature Information for Secure Storage

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|----------------|---|
| Cisco IOS XE Gibraltar 16.11.1 | Secure Storage | Secure Storage feature allows you to secure critical configuration information by encrypting it. It encrypts asymmetric key-pairs, pre-shared secrets, the type 6 password encryption key and certain credentials. An instance-unique encryption key is stored in the hardware trust anchor to prevent it from being compromised. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 17

Conditional Debug and Radioactive Tracing

- [Introduction to Conditional Debugging, on page 221](#)
- [Introduction to Radioactive Tracing, on page 222](#)
- [How to Configure Conditional Debug and Radioactive Tracing, on page 222](#)
- [Monitoring Conditional Debugging, on page 226](#)
- [Configuration Examples for Conditional Debugging, on page 226](#)
- [Additional References for Conditional Debugging and Radioactive Tracing, on page 227](#)
- [Feature History for Conditional Debugging and Radioactive Tracing, on page 227](#)

Introduction to Conditional Debugging

The Conditional Debugging feature allows you to selectively enable debugging and logging for specific features based on the set of conditions you define. This feature is useful in systems where a large number of features are supported.



Note Only Control Plane Tracing is supported.

The Conditional debug allows granular debugging in a network that is operating at a large scale with a large number of features. It allows you to observe detailed debugs for granular instances within the system. This is very useful when we need to debug only a particular session among thousands of sessions. It is also possible to specify multiple conditions.

A condition refers to a feature or identity, where identity could be an interface, IP Address, or a MAC address and so on.



Note MAC address is the only supported condition.

This is in contrast to the general debug command, that produces its output without discriminating on the feature objects that are being processed. General debug command consumes a lot of system resources and impacts the system performance.

Introduction to Radioactive Tracing

Radioactive tracing provides the ability to stitch together a chain of execution for operations of interest across the system, at an increased verbosity level. This provides a way to conditionally print debug information (up to DEBUG Level or a specified level) across threads, processes and function calls.



Note The default level is **DEBUG**. The users cannot change this to another level.

The following features are enabled for Radioactive Tracing:

- IGMP Snooping
- Layer 2 Multicast

How to Configure Conditional Debug and Radioactive Tracing

Conditional Debugging and Radioactive Tracing

Radioactive Tracing when coupled with Conditional Debugging, enable us to have a single debug CLI to debug all execution contexts related to the condition. This can be done without being aware of the various control flow processes of the feature within the box and without having to issue debugs at these processes individually.

Location of Tracefiles

By default the tracefile logs will be generated for each process and saved into either the **/tmp/rp/trace** or **/tmp/fp/trace** directory. In this temp directory, the trace logs are written to files, which are of 1 MB size each. The directory can hold up to a maximum of 25 such files for a given process. When a tracefile in the **/tmp** directory reaches its 1MB limit or whatever size was configured for it during the boot time, it is rotated out to an archive location in the **/crashinfo** partition under **tracelogs** directory.

The **/tmp** directory holds only a single tracefile for a given process. Once the file reaches its file size limit it is rotated out to **/crashinfo/tracelogs**. In the archive directory, up to 25 files are accumulated, after which the oldest one is replaced by the newly rotated file from **/tmp**.

The tracefiles in the crashinfo directory are located in the following formats:

1. Process-name_Process-ID_running-counter.timestamp.gz
Example: IOSRP_R0-0.bin_0.14239.20151101234827.gz
2. Process-name_pmanlog_Process-ID_running-counter.timestamp.bin.gz
Example: wcm_pmanlog_R0-0.30360_0.20151028233007.bin.gz

Configuring Conditional Debugging

To configure conditional debugging, follow the steps given below:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | debug platform condition mac {mac-address} Example: <pre>Device# debug platform condition mac bc16.6509.3314</pre> | Configures conditional debugging for the MAC Address specified. |
| Step 3 | debug platform condition start Example: <pre>Device# debug platform condition start</pre> | Starts conditional debugging (this will start radioactive tracing if there is a match on one of the conditions above). |
| Step 4 | show platform condition OR show debug Example: <pre>Device# show platform condition Device# show debug</pre> | Displays the current conditions set. |
| Step 5 | debug platform condition stop Example: <pre>Device# debug platform condition stop</pre> | Stops conditional debugging (this will stop radioactive tracing). |
| Step 6 | request platform software trace archive [last {number} days] [target {crashinfo: flashinfo:}] Example: <pre># request platform software trace archive last 2 days</pre> | (Optional) Displays historical logs of merged tracefiles on the system. Filter on any combination of number of days or location. |
| Step 7 | show platform software trace [filter-binary level message] Example: <pre>Device# show platform software trace message</pre> | (Optional) Displays logs merged from the latest tracefile. Filter on any combination of application condition, trace module name, and trace level. <ul style="list-style-type: none"> • filter-binary - Filter the modules to be collated • level - Show trace levels • message - Show trace message ring contents |

| | Command or Action | Purpose |
|---------------|---|--|
| | | Note On the device: <ul style="list-style-type: none"> • Available from IOS console in addition to linux shell. • Generates a file with merged logs. • Displays merged logs only from staging area |
| Step 8 | clear platform condition all Example: Device# <code>clear platform condition all</code> | Clears all conditions. |

What to do next



Note The commands **request platform software trace filter-binary** and **show platform software trace filter-binary** work in a similar way. The only difference is:

- **request platform software trace filter-binary** - Sources the data from historical logs.
- **show platform software trace filter-binary** – Sources the data from the flash Temp directory.

Of these, *mac_log <..date..>* is the most important file, as it gives the messages for the MAC we are debugging. The command **show platform software trace filter-binary** also generates the same flash files, and also prints the *mac_log* on the screen.

Radioactive Tracing for L2 Multicast

To identify a specific multicast receiver, specify the MAC address of the joiner or the receiver client, Group Multicast IP address and Snooping VLAN. Additionally, enable the trace level for the debug. The debug level will provide detailed traces and better visibility into the system.

debug platform condition feature multicast controlplane mac client MAC address ip Group IP address vlan id level debug level

Recommended Workflow for Trace files

The Recommended Workflow for Trace files is listed below:

1. To request the tracelogs for a specific time period.

EXAMPLE 1 day.

Use the command:

Device#**request platform software trace archive last 1 day**

2. The system generates a tar ball (.gz file) of the tracelogs in the location /flash:
3. Copy the file off the switch. By copying the file, the tracelogs can be used to work offline. For more details on copying files, see section below.
4. Delete the tracelog file (.gz) file from /flash: location. This will ensure enough space on the switch for other operations.

Copying tracefiles off the box

An example of the tracefile is shown below:

```
Device# dir crashinfo:/tracelogs
Directory of crashinfo:/tracelogs/

50664 -rwx 760 Sep 22 2015 11:12:21 +00:00 plogd_F0-0.bin_0.gz
50603 -rwx 991 Sep 22 2015 11:12:08 +00:00 fed_pmanlog_F0-0.bin_0.9558.20150922111208.gz
50610 -rw- 11 Nov 2 2015 00:15:59 +00:00 timestamp
50611 -rwx 1443 Sep 22 2015 11:11:31 +00:00
auto_upgrade_client_sh_pmanlog_R0-.bin_0.3817.20150922111130.gz
50669 -rwx 589 Sep 30 2015 03:59:04 +00:00 cfgwr-8021_R0-0.bin_0.gz
50612 -rwx 1136 Sep 22 2015 11:11:46 +00:00 reflector_803_R0-0.bin_0.1312.20150922111116.gz
50794 -rwx 4239 Nov 2 2015 00:04:32 +00:00 IOSRP_R0-0.bin_0.14239.20151101234827.gz
50615 -rwx 131072 Nov 2 2015 00:19:59 +00:00 linux_iosd_image_pmanlog_R0-0.bin_0
--More--
```

The trace files can be copied using one of the various options shown below:

```
Device# copy crashinfo:/tracelogs ?
crashinfo: Copy to crashinfo: file system
flash: Copy to flash: file system
ftp: Copy to ftp: file system
http: Copy to http: file system
https: Copy to https: file system
null: Copy to null: file system
nvram: Copy to nvram: file system
rcp: Copy to rcp: file system
running-config Update (merge with) current system configuration
scp: Copy to scp: file system
startup-config Copy to startup configuration
syslog: Copy to syslog: file system
system: Copy to system: file system
tftp: Copy to tftp: file system
tmpsys: Copy to tmpsys: file system
```

The general syntax for copying onto a TFTP server is as follows:

```
Device# copy source: tftp:
Device# copy crashinfo:/tracelogs/IOSRP_R0-0.bin_0.14239.20151101234827.gz tftp:
Address or name of remote host []? 2.2.2.2
Destination filename [IOSRP_R0-0.bin_0.14239.20151101234827.gz]?
```



Note It is important to clear the generated report or archive files off the switch in order to have flash space available for tracelog and other purposes.

Monitoring Conditional Debugging

The table shown below lists the various commands that can be used to monitor conditional debugging.

| Command | Purpose |
|--|--|
| show platform condition | Displays the current conditions set. |
| show debug | Displays the current debug conditions set. |
| show platform software trace filter-binary | Displays logs merged from the latest tracefile. |
| request platform software trace filter-binary | Displays historical logs of merged tracefiles on the system. |

Configuration Examples for Conditional Debugging

The following is an output example of the *show platform condition* command.

```
Device# show platform condition
Conditional Debug Global State: Stop
Conditions Direction
```

```
-----|-----
MAC Address 0024.D7C7.0054 N/A
```

```
Feature Condition Type Value
```

```
-----|-----
Device#
```

The following is an output example of the *show debug* command.

```
Device# show debug
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Start
Conditions Direction
```

```
-----|-----
MAC Address 0024.D7C7.0054 N/A
```

```
Feature Condition Type Value
```

```
-----|-----
Packet Infra debugs:
```

```
Ip Address Port
```

```
-----|-----
Device#
```

The following is a sample of the *debug platform condition stop* command.

```
Device# debug platform condition stop
Conditional Debug Global State: Stop
```


Additional References for Conditional Debugging and Radioactive Tracing

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

Feature History for Conditional Debugging and Radioactive Tracing

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | Conditional Debugging and Radioactive Tracing | The Conditional Debugging feature allows you to selectively enable debugging and logging for specific features based on the set of conditions you define. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 18

Consent Token

- [Restrictions for Consent Token, on page 229](#)
- [Information About Consent Token, on page 229](#)
- [Consent Token Authorization Process for System Shell Access, on page 230](#)
- [Feature History for Consent Token, on page 231](#)

Restrictions for Consent Token

- Consent Token is enabled by default and cannot be disabled.
- After the challenge has been sent from the device, the response needs to be entered within 30 minutes. If it is not entered, the challenge expires and a new challenge must be requested.
- A single response is valid only for one time for a corresponding challenge.
- The maximum authorization timeout for root-shell access is seven days.
- After a switchover event, all the existing Consent Token based authorizations would be treated as expired. You must then restart a fresh authentication sequence for service access.
- Only Cisco authorized personnel have access to Consent Token response generation on Cisco's challenge signing server.
- In System Shell access scenario, exiting the shell does not terminate authorization until the authorization timeout occurs or the shell authorization is explicitly terminated by the consent token terminate authorization command.

We recommend that you force terminate System Shell authorization by explicitly issuing the Consent Token terminate command once the purpose of System Shell access is complete.

Information About Consent Token

Consent Token is a security feature that is used to authenticate the network administrator of an organization to access system shell with mutual consent from the network administrator and Cisco Technical Assistance Centre (Cisco TAC).

In some debugging scenarios, the Cisco TAC engineer may have to collect certain debug information or perform live debug on a production system. In such cases, the Cisco TAC engineer will ask you (the network

administrator) to access system shell on your device. Consent Token is a lock, unlock and re-lock mechanism that provides you with privileged, restricted, and secure access to the system shell.

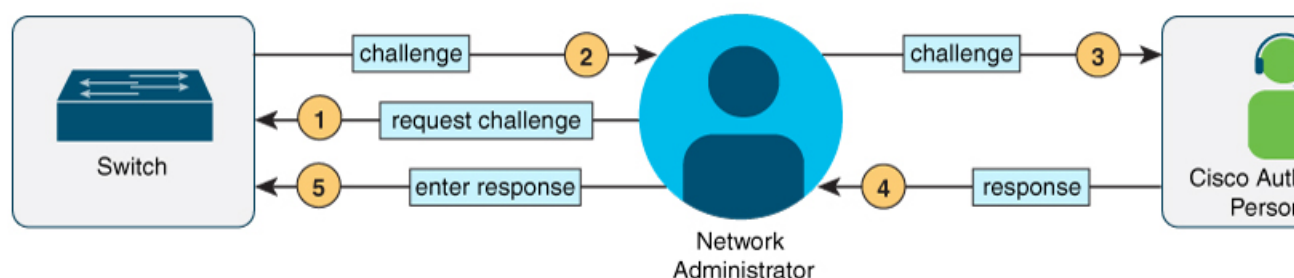
When you request access to system shell, you need to be authorized. You must first run the command to generate a challenge using the Consent Token feature on your device. The device generates a unique challenge as output. You must then copy this challenge string and send it to a Cisco Authorized Personnel through e-mail or Instant Message.

The Cisco Authorized Personnel processes the unique challenge string and generates a response that is unique. The Cisco Authorized Personnel copies this response string and sends it to you through e-mail or Instant Message.

You must then input this response string into your device. If the challenge-response pair match, you are authorized to access system shell. If not, an error is displayed and you are required to repeat the authentication process.

Once you gain access to system shell, collect the debug information required by the Cisco TAC engineer. After you are done accessing system shell, terminate the session and continue the debugging process.

Figure 5: Consent Token



Consent Token Authorization Process for System Shell Access

This section describes the process of Consent Token authorization to access system shell:

Procedure

Step 1 Generate a challenge requesting for access to system shell for the specified time period.

Example:

```

Device# request consent-token generate-challenge shell-access auth-timeout 900
%Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation attempt: Shell access 0).
Device#
  
```

Send a request for a challenge using the **request consent-token generate-challenge shell-access time-validity-slot** command. The duration in minutes for which you are requesting access to system shell is the time-slot-period.

In this example, the time period is 900 minutes after which the session expires.

The device generates a unique challenge as output. This challenge is a base-64 format string.

Step 2 Send the challenge string to a Cisco Authorized Personnel.

Send the challenge string generated by the device to a Cisco Authorized Personnel through e-mail or Instant Message.

The Cisco Authorized Personnel processes the unique challenge string and generates a response. The response is also a base-64 string that is unique. The Cisco Authorized Personnel copies this response string and sends it to you through e-mail or Instant Message.

Step 3 Input the response string onto your device.**Example:**

```
Device# request consent-token accept-response shell-access
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success:
  Shell access 0).

Device# request platform software system shell
Activity within this shell can jeopardize the functioning of the system.
Are you sure you want to continue? [y/n] y
Device#
*Jan 18 02:56:59.714: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authorization for Shell
  access 0 will expire in 10 min).
```

Input the response string sent to you by the Cisco Authorized Personnel using the **request consent-token accept-response shell-access response-string** command.

If the challenge-response pair match, you are authorized to access system shell. If the challenge-response pair do not match, an error is displayed and you are required to repeat steps 1 to 3.

After you are authorized, you can access system shell for the requested time-slot.

The device sends a message when there is ten minutes remaining of the authorization session.

Step 4 Terminate the session.**Example:**

```
Device# request consent-token terminate-auth
% Consent token authorization termination success

Device#
*Jan 18 23:33:02.937: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication:
  Shell access 0).
Device#
```

When you finish accessing system shell, you can end the session using the **request consent-token terminate-auth** command. You can also force terminate the session prior to the authorization timeout using this command. The session also gets terminated automatically when the requested time slot expires.

Feature History for Consent Token

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|---------------|--|
| Cisco IOS XE Gibraltar 16.11.1 | Consent Token | Consent Token is a security feature that is used to authenticate the network administrator of an organization to access system shell with mutual consent from the network administrator and Cisco Technical Assistance Centre (Cisco TAC). |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 19

Troubleshooting the Software Configuration

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the switch. Depending on the nature of the problem, you can use the command-line interface (CLI), Device Manager, or Network Assistant to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

- [Information About Troubleshooting the Software Configuration, on page 233](#)
- [How to Troubleshoot the Software Configuration, on page 239](#)
- [Verifying Troubleshooting of the Software Configuration, on page 247](#)
- [Configuration Examples for Troubleshooting Software, on page 249](#)
- [Additional References for Troubleshooting Software Configuration, on page 250](#)
- [Feature History for Troubleshooting Software Configuration, on page 250](#)

Information About Troubleshooting the Software Configuration

Software Failure on a Switch

Switch software can be corrupted during an upgrade by downloading the incorrect file to the switch, and by deleting the image file. In all of these cases, there is no connectivity.

Lost or Forgotten Password on a Device

The default configuration for the device allows an end user with physical access to the device to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the device.



Note

On these devices, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message reminds you to return to the default configuration during the recovery process.



Note You cannot recover encryption password key, when Cisco WLC configuration is copied from one Cisco WLC to another (in case of an RMA).

Follow the steps described in the section [Recovering from a Lost or Forgotten Password, on page 239](#) to recover from a lost or forgotten password.

Ping

The device supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- Normal response—The normal response (*hostname* is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a *no-answer* message is returned.
- Unknown host—If the host does not exist, an *unknown host* message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a *destination-unreachable* message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a *network or host unreachable* message is returned.

Refer to the section [Executing Ping, on page 245](#) to understand how **ping** works.

Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. Traceroute finds the path by using the MAC address tables of the devices in the path. When the Device detects a device in the path that does not support Layer 2 traceroute, the Device continues to send Layer 2 trace queries and lets them time out.

The Device can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Layer 2 Traceroute Guidelines

- Cisco Discovery Protocol (CDP) must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP.

If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.

- A device is reachable from another device when you can test connectivity by using the **ping** privileged EXEC command. All devices in the physical path must be reachable from each other.
- The maximum number of hops identified in the path is ten.

- You can enter the **traceroute mac** or the **traceroute mac ip** privileged EXEC command on a device that is not in the physical path from the source device to the destination device. All devices in the path must be reachable from this switch.
- The **traceroute mac** command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.
- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.
- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.
- The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the device uses the Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.
 - If an ARP entry exists for the specified IP address, the device uses the associated MAC address and identifies the physical path.
 - If an ARP entry does not exist, the device sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.
- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.
- This feature is not supported in Token Ring VLANs.
- Layer 2 traceroute opens a listening socket on the User Datagram Protocol (UDP) port 2228 that can be accessed remotely with any IPv4 address, and does not require any authentication. This UDP socket allows to read VLAN information, links, presence of particular MAC addresses, and CDP neighbor information, from the device. This information can be used to eventually build a complete picture of the Layer 2 network topology.
- Layer 2 traceroute is enabled by default and can be disabled by running the **no l2 traceroute** command in global configuration mode. To re-enable Layer 2 traceroute, use the **l2 traceroute** command in global configuration mode.

IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your Device can participate as the source or destination of the **traceroute** privileged EXEC command and might or might not appear as a hop in the **traceroute** command output. If the Device is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate devices do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate Device is a multilayer Device that is routing a particular packet, this device shows up as a hop in the traceroute output.

The **tracert** privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute finds the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To learn when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP *port-unreachable* error to the source. Because all errors except port-unreachable errors come from intermediate hops, the receipt of a port-unreachable error means that this message was sent by the destination port.

Go to [Example: Performing a Traceroute to an IP Host, on page 249](#) to see an example of IP traceroute process.

Debug Commands



Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments.

System Report

System reports or crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). It is necessary to quickly and reliably collect critical crash information with high fidelity and integrity. Further, it is necessary to collect this information and bundle it in a way that it can be associated or identified with a specific crash occurrence.

System reports are generated in case of a switchover: System reports are generated only on high availability (HA) member switches. Reports are not generated for non-HA members.

The system does not generate reports in case of a reload.

During a process crash, the following is collected locally from the switch:

1. Full process core
2. Tracelogs
3. IOS syslogs (not guaranteed in case of non-active crashes)
4. System process information

5. Bootup logs
6. Reload logs
7. Certain types of /proc information

This information is stored in separate files which are then archived and compressed into one bundle. This makes it convenient to get a crash snapshot in one place, and can be then moved off the box for analysis. This report is generated before the switch goes down to rommon/bootloader.

Except for the full core and tracelogs, everything else is a text file.

Use the **request platform software process core fed switch active** command to generate the core dump.

```
Device# request platform software process core fed switch active
SUCCESS: Core file generated.

Device# dir bootflash:/core
Directory of bootflash:/core/
16430  -rw-          10941657   Apr  6 2022 00:15:20 +00:00
Switch_1_RP_0_fed_18469_20220406-001511-UTC.core.gz
16812  -rw-           1   Apr  6 2022 00:01:48 +00:00  .callhome
16810  drwx           4096   Jan 18 2022 21:10:35 +00:00  modules
```

Crashinfo Files

By default the system report file will be generated and saved into the /crashinfo directory. If it cannot be saved to the crashinfo partition for lack of space, then it will be saved to the /flash directory.

To display the files, enter the **dir crashinfo:** command. The following is sample output of a crashinfo directory:

System reports are located in the crashinfo directory in the following format:

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

After a switch crashes, check for a system report file. The name of the most recently generated system report file is stored in the last_systemreport file under the crashinfo directory. The system report and crashinfo files assist TAC while troubleshooting the issue.

The system report generated can be further copied using TFTP, HTTP and few other options.

```
Device# copy crashinfo: ?
crashinfo: Copy to crashinfo: file system
flash: Copy to flash: file system
ftp: Copy to ftp: file system
http: Copy to http: file system
https: Copy to https: file system
null: Copy to null: file system
nvram: Copy to nvram: file system
rcp: Copy to rcp: file system
running-config Update (merge with) current system configuration
scp: Copy to scp: file system
startup-config Copy to startup configuration
syslog: Copy to syslog: file system
system: Copy to system: file system
tftp: Copy to tftp: file system
tmpsys: Copy to tmpsys: file system
```

The general syntax for copying onto TFTP server is as follows:

```
Device# copy crashinfo: tftp:
Source filename [system-report_1_20150909-092728-UTC.gz]?
Address or name of remote host []? 1.1.1.1
Destination filename [system-report_1_20150909-092728-UTC.gz]?
```

The tracelogs can be collected by issuing a trace archive command. This command provides time period options. The command syntax is as follows:

```
Device# request platform software trace archive ?
last      Archive trace files of last x days
target    Location and name for the archive file
```

The tracelogs stored in crashinfo: or flash: directory from within the last 3650 days can be collected.

```
Device# request platform software trace archive last ?
<1-3650> Number of days (1-3650)
Switch#request platform software trace archive last 3650 days target ?
crashinfo: Archive file name and location
flash:     Archive file name and location
```



Note It is important to clear the system reports or trace archives from flash or crashinfo directory once they are copied out, in order to have space available for tracelogs and other purposes.

Onboard Failure Logging on the Switch

You can use the onboard failure logging (OBFL) feature to collect information about the device. The information includes uptime, temperature, and voltage information and helps Cisco technical support representatives to troubleshoot device problems. We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

By default, OBFL is enabled. It collects information about the device and small form-factor pluggable (SFP) modules. The device stores this information in the flash memory:

- CLI commands—Record of the OBFL CLI commands that are entered on a standalone device.
- Message—Record of the hardware-related system messages generated by a standalone device .
- Power over Ethernet (PoE)—Record of the power consumption of PoE ports on a standalone device .
- Temperature—Temperature of a standalone device .
- Uptime data—Time when a standalone device starts, the reason the device restarts, and the length of time the device has been running since it last restarted.
- Voltage—System voltages of a standalone device .

You should manually set the system clock or configure it by using Network Time Protocol (NTP).

When the device is running, you can retrieve the OBFL data by using the **show logging onboard** privileged EXEC commands. If the device fails, contact your Cisco technical support representative to find out how to retrieve the data.

When an OBFL-enabled device is restarted, there is a 10-minute delay before logging of new data begins.

Fan Failures

By default, the feature is disabled. When more than one of the fans fails in a field-replaceable unit (FRU) or in a power supply, the device does not shut down, and this error message appears:

The device might overheat and shut down.

To restart the device, it must be power cycled.

Possible Symptoms of High CPU Utilization

Excessive CPU utilization might result in these symptoms, but the symptoms might also result from other causes, some of which are the following:

- Spanning tree topology changes
- EtherChannel links brought down due to loss of communication
- Failure to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions)
- UDLD flapping
- IP SLAs failures because of SLAs responses beyond an acceptable threshold
- DHCP or IEEE 802.1x failures if the switch does not forward or respond to requests

How to Troubleshoot the Software Configuration

Recovering from a Lost or Forgotten Password

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.



Note On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

Procedure

-
- Step 1** Connect a terminal or PC to the switch.
- Connect a terminal or a PC with terminal-emulation software to the switch console port. If you are recovering the password for a switch stack, connect to the console port of the active switch.
 - Connect a PC to the Ethernet management port. If you are recovering the password for a switch stack, connect to the Ethernet management port of a stack member.
- Step 2** Set the line speed on the emulation software to 9600 baud.
- Step 3** Power off the standalone switch or the entire switch stack.
- Step 4** Reconnect the power cord to the switch or the active switch. For a device with dual supervisor module, remove the standby supervisor from the chassis before the password recovery procedure. Reconnect the power

cord to the switch or the active supervisor module. Press Ctrl-C to prevent autoboot and to get into ROMMON mode while the switch or the active supervisor module is booting up.

Proceed to the *Procedure with Password Recovery Enabled* section, and follow the steps.

Step 5 After recovering the password, reload the switch or the active switch.

On a switch:

```
Switch> reload
Proceed with reload? [confirm] y
```

On the active switch:

```
Switch> reload slot <stack-active-member-number>
Proceed with reload? [confirm] y
```

Step 6 Power on the remaining switches in the stack.

Procedure with Password Recovery Enabled

Procedure

Step 1 Ignore the startup configuration with the following command:

```
Device: SWITCH_IGNORE_STARTUP_CFG=1
```

Step 2 Boot the switch with the *packages.conf* file from flash.

```
Device: boot flash:packages.conf
```

Step 3 Terminate the initial configuration dialog by answering **No**.

```
Would you like to enter the initial configuration dialog? [yes/no]: No
```

Step 4 At the switch prompt, enter privileged EXEC mode.

```
Device> enable
Device#
```

Step 5 Copy the startup configuration to running configuration.

```
Device# copy startup-config running-config Destination filename [running-config]?
```

Press Return in response to the confirmation prompts. The configuration file is now reloaded, and you can change the password.

Step 6 Enter global configuration mode and change the **enable** password.

```
Device# configure terminal  
Device(config)# enable secret password
```

Step 7 Return to privileged EXEC mode:

```
Device(config)# exit  
Device#
```

Step 8 Write the running configuration to the startup configuration file.

```
Device# copy running-config startup-config
```

Step 9 Confirm that manual boot mode is enabled.

```
Device# show boot  
  
BOOT variable = flash:packages.conf;  
Manual Boot = yes  
Enable Break = yes
```

Step 10 Reload the device.

```
Device# reload
```

Step 11 Set the SWITCH_IGNORE_STARTUP_CFG parameter to 0.

```
Device(config)# no system ignore startupconfig switch all  
Device(config)# end  
Device# write memory
```

Step 12 Boot the device with the *packages.conf* file from flash.

```
Device: boot flash:packages.conf
```

Step 13 After the device boots up, disable manual boot on the device.

```
Device(config)# no boot manual
```

Procedure with Password Recovery Disabled

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but  
is currently disabled. Access to the boot loader prompt  
through the password-recovery mechanism is disallowed at  
this point. However, if you agree to let the system be
```

```
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```



Caution Returning the device to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup device and VLAN configuration files.

- If you enter **n** (no), the normal boot process continues as if the **Mode** button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:

```
Press Enter to continue.....
```

- If you enter **y** (yes), the configuration file in flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

Procedure

Step 1 Choose to continue with password recovery and delete the existing configuration:

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

Step 2 Display the contents of flash memory:

```
Device: dir flash:
```

The device file system appears.

Step 3 Boot up the system:

```
Device: boot
```

You are prompted to start the setup program. To continue with password recovery, enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

Step 4 At the device prompt, enter privileged EXEC mode:

```
Device> enable
```

Step 5 Enter global configuration mode:

```
Device# configure terminal
```

Step 6 Change the password:


```
Device(config)# enable secret password
```

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 7 Return to privileged EXEC mode:

```
Device(config)# exit
Device#
```

Note Before continuing to Step 9, power on any connected stack members and wait until they have completely initialized.

Step 8 Write the running configuration to the startup configuration file:

```
Device# copy running-config startup-config
```

The new password is now in the startup configuration.

Step 9 You must now reconfigure the device. If the system administrator has the backup device and VLAN configuration files available, you should use those.

Preventing Switch Stack Problems

To prevent switch stack problems, you should do the following:

- Make sure that the device that you add to or remove from the switch stack are powered off. For all powering considerations in switch stacks, see the “Switch Installation” chapter in the hardware installation guide.
- Press the **Mode** button on a stack member until the Stack mode LED is on. The last two port LEDs on the device should be green. Depending on the device model, the last two ports are either 10/100/1000 ports or small form-factor pluggable (SFP) module. If one or both of the last two port LEDs are not green, the stack is not operating at full bandwidth.
- We recommend using only one CLI session when managing the switch stack. Be careful when using multiple CLI sessions to the active switch. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible that you might not be able to identify the session from which you entered a command.
- Manually assigning stack member numbers according to the placement of the device in the stack can make it easier to remotely troubleshoot the switch stack. However, you need to remember that the device have manually assigned numbers if you add, remove, or rearrange device later. Use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* global configuration command to manually assign a stack member number.

If you replace a stack member with an identical model, the new device functions with the exact same configuration as the replaced device. This is also assuming the new device is using the same member number as the replaced device.

Removing powered-on stack members causes the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. If you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks. To recover from a partitioned switch stack, follow these steps:

1. Power off the newly created switch stacks.
2. Reconnect them to the original switch stack through their StackWise Plus ports.
3. Power on the device.

For the commands that you can use to monitor the switch stack and its members, see the *Displaying Switch Stack Information* section.

Preventing Autonegotiation Mismatches

The IEEE 802.3ab autonegotiation protocol manages the device settings for speed (10 Mb/s, 100 Mb/s, and 1000 Mb/s, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize the device performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.



Note If a remote device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate.

Troubleshooting SFP Module Security and Identification

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the device, the device software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.



Note The security error message references the GBIC_SECURITY facility. The device supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces.

If you are using a non-Cisco SFP module, remove the SFP module from the device, and replace it with a Cisco module. After inserting a Cisco SFP module, use the **errdisable recovery cause gbic-invalid** global configuration command to verify the port status, and enter a time interval for recovering from the error-disabled state. After the elapsed interval, the device brings the interface out of the error-disabled state and retries the

operation. For more information about the **errdisable recovery** command, see the command reference for this release.

If the module is identified as a Cisco SFP module, but the system is unable to read vendor-data information to verify its accuracy, an SFP module error message is generated. In this case, you should remove and reinsert the SFP module. If it continues to fail, the SFP module might be defective.

Executing Ping

If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or have IP routing configured to route between those subnets.

IP routing is disabled by default on all devices.



Note Though other protocol keywords are available with the **ping** command, they are not supported in this release.

Use this command to ping another device on the network from the device:

| Command | Purpose |
|---|---|
| ping ip <i>host</i> <i>address</i> Device# ping 172.20.52.3 | Pings a remote host through IP or by supplying the hostname or network address. |

Monitoring Temperature

The Device monitors the temperature conditions and uses the temperature information to control the fans.

Monitoring the Physical Path

You can monitor the physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:

Table 17: Monitoring the Physical Path

| Command | Purpose |
|--|--|
| tracetroute mac [interface <i>interface-id</i>] { <i>source-mac-address</i> } [interface <i>interface-id</i>] { <i>destination-mac-address</i> } [vlan <i>vlan-id</i>] [detail] | Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address. |
| tracetroute mac ip { <i>source-ip-address</i> <i>source-hostname</i> } { <i>destination-ip-address</i> <i>destination-hostname</i> } [detail] | Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname. |

Executing IP Traceroute



Note Though other protocol keywords are available with the **traceroute** privileged EXEC command, they are not supported in this release.

| Command | Purpose |
|---|--|
| traceroute ip host Device# traceroute ip 192.51.100.1 | Traces the path that packets take through the network. |

Redirecting Debug and Error Message Output

By default, the network server sends the output from **debug** commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port .

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.



Note Be aware that the debugging destination you use affects system overhead. When you log messages to the console, very high overhead occurs. When you log messages to a virtual terminal, less overhead occurs. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

For more information about system message logging, see *Configuring System Message Logging*.

Using the show platform Command

The output from the **show platform** privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

Most of the information in the output from the command is useful mainly for technical support personnel, who have access to detailed information about the device application-specific integrated circuits (ASICs). However, packet forwarding information can also be helpful in troubleshooting.

Using the show debug command

The **show debug** command is entered in privileged EXEC mode. This command displays all debug options available on the switch.

To view all conditional debug options run the command **show debug condition** The commands can be listed by selecting either a condition identifier <1-1000> or *all* conditions.

To disable debugging, use the **no debug all** command.


Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Verifying Troubleshooting of the Software Configuration

Displaying OBFL Information

Table 18: Commands for Displaying OBFL Information - Cisco Catalyst 9600 Series Switches

| Command | Purpose |
|---|---|
| show logging onboard RP active clilog [<i>continuous</i> <i>detail</i> <i>summary</i>] Device# show logging onboard RP active clilog | Displays the OBFL CLI commands that were entered on a module. |
| show logging onboard RP active environment [<i>continuous</i> <i>detail</i> <i>summary</i>] Device# show logging onboard RP active environmentt | Displays the UDI information for a module and for all the connected FRU devices: the PID, the VID, and the serial number. |
| show logging onboard RP active message [<i>continuous</i> <i>detail</i> <i>summary</i>] Device# show logging onboard RP active message | Displays the hardware-related messages generated by a module. |
| show logging onboard RP active counter [<i>continuous</i> <i>detail</i> <i>summary</i>] Device# show logging onboard RP active counter | Displays the counter information on a module. |
| show logging onboard RP active temperature [<i>continuous</i> <i>detail</i> <i>summary</i>] Device# show logging onboard RP active temperature | Displays the temperature information of a module. |
| show logging onboard RP active uptime [<i>continuous</i> <i>detail</i> <i>summary</i>] Device# show logging onboard RP active uptime | Displays the time when a module start, the reason the module restart, and the length of time that the module have been running since they last restarted. |

Example: Verifying the Problem and Cause for High CPU Utilization

| Command | Purpose |
|--|---|
| show logging onboard RP active voltage [<i>continuous</i> <i>detail</i> <i>summary</i>] Device# show logging onboard RP active voltage | Displays the system voltages of a module. |
| show logging onboard RP active status [<i>continuous</i> <i>detail</i> <i>summary</i>] Device# show logging onboard RP active status | Displays the status of each OBFL application of a module. |

Example: Verifying the Problem and Cause for High CPU Utilization

To determine if high CPU utilization is a problem, enter the **show processes cpu sorted** privileged EXEC command. Note the underlined information in the first line of the output example.

```
Device# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

This example shows normal CPU utilization. The output shows that utilization for the last 5 seconds is 8%/0%, which has this meaning:

- The total CPU utilization is 8 percent, including both time running Cisco IOS processes and time spent handling interrupts.
- The time spent handling interrupts is zero percent.

Table 19: Troubleshooting CPU Utilization Problems

| Type of Problem | Cause | Corrective Action |
|--|---|--|
| Interrupt percentage value is almost as high as total CPU utilization value. | The CPU is receiving too many packets from the network. | Determine the source of the network packet. Stop the flow, or change the switch configuration. See the section on “Analyzing Network Traffic.” |
| Total CPU utilization is greater than 50% with minimal time spent on interrupts. | One or more Cisco IOS process is consuming too much CPU time. This is usually triggered by an event that activated the process. | Identify the unusual event, and troubleshoot the root cause. See the section on “Debugging Active Processes.” |

Configuration Examples for Troubleshooting Software

Example: Pinging an IP Host

This example shows how to ping an IP host:

```
Device# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Device#
```

Table 20: Ping Output Display Characters

| Character | Description |
|-----------|---|
| ! | Each exclamation point means receipt of a reply. |
| . | Each period means the network server timed out while waiting for a reply. |
| U | A destination unreachable error PDU was received. |
| C | A congestion experienced packet was received. |
| I | User interrupted test. |
| ? | Unknown packet type. |
| & | Packet lifetime exceeded. |

To end a ping session, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key.

Example: Performing a Traceroute to an IP Host

This example shows how to perform a **traceroute** to an IP host:

```
Device# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

 0 192.0.2.1 0 msec 0 msec 4 msec
 1 192.0.2.203 12 msec 8 msec 0 msec
 2 192.0.2.100 4 msec 0 msec 0 msec
 3 192.0.2.10 0 msec 4 msec 0 msec
```

The display shows the hop count, the IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent.

Table 21: Traceroute Output Display Characters

| Character | Description |
|-----------|---|
| * | The probe timed out. |
| ? | Unknown packet type. |
| A | Administratively unreachable. Usually, this output means that an access list is blocking traffic. |
| H | Host unreachable. |
| N | Network unreachable. |
| P | Protocol unreachable. |
| Q | Source quench. |
| U | Port unreachable. |

To end a trace in progress, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key.

Additional References for Troubleshooting Software Configuration

Related Documents

| Related Topic | Document Title |
|--|--|
| For complete syntax and usage information for the commands used in this chapter. | <i>Command Reference (Catalyst 9600 Series Switches)</i> |

Feature History for Troubleshooting Software Configuration

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------------|--|---|
| Cisco IOS XE Gibraltar 16.11.1 | Troubleshooting Software Configuration | Troubleshooting software configuration describes how to identify and resolve software problems related to the Cisco IOS software on the switch. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.