



## **System Management Configuration Guide, Cisco IOS XE Release 3.6E (Catalyst 3650 Switches)**

**First Published:** 2013-10-10

### **Americas Headquarters**

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

Text Part Number: OL-32634-01





## CONTENTS

---

### Preface

#### Preface **xix**

Document Conventions **xix**

Related Documentation **xxi**

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

---

### CHAPTER 1

#### Using the Command-Line Interface **1**

Information About Using the Command-Line Interface **1**

Command Modes **1**

Understanding Abbreviated Commands **3**

No and Default Forms of Commands **3**

CLI Error Messages **4**

Configuration Logging **4**

Using the Help System **4**

How to Use the CLI to Configure Features **6**

Configuring the Command History **6**

    Changing the Command History Buffer Size **6**

    Recalling Commands **6**

    Disabling the Command History Feature **7**

Enabling and Disabling Editing Features **7**

    Editing Commands Through Keystrokes **8**

    Editing Command Lines That Wrap **9**

Searching and Filtering Output of show and more Commands **10**

Accessing the CLI on a Switch Stack **11**

Accessing the CLI Through a Console Connection or Through Telnet **11**

---

### CHAPTER 2

#### Using the Web Graphical User Interface **13**

Prerequisites for Using the Web GUI **13**

Information About Using The Web GUI	14
Web GUI Features	14
Connecting the Console Port of the Switch	15
Logging On to the GUI	16
Enabling Web and Secure Web Modes	16
Configuring the Switch Web GUI	17

---

**CHAPTER 3**

<b>Administering the System</b>	<b>21</b>
Finding Feature Information	21
Information About Administering the Switch	21
System Time and Date Management	21
System Clock	22
Network Time Protocol	22
NTP Stratum	24
NTP Associations	24
NTP Security	24
NTP Implementation	24
NTP Version 4	25
System Name and Prompt	26
Stack System Name and Prompt	26
Default System Name and Prompt Configuration	26
DNS	26
Default DNS Settings	27
Login Banners	27
Default Banner Configuration	27
MAC Address Table	27
MAC Address Table Creation	28
MAC Addresses and VLANs	28
MAC Addresses and Switch Stacks	28
Default MAC Address Table Settings	28
ARP Table Management	29
How to Administer the Switch	29
Configuring the Time and Date Manually	29
Setting the System Clock	29
Configuring the Time Zone	30

Configuring Summer Time (Daylight Saving Time)	31
	33
Configuring a System Name	35
Setting Up DNS	36
Configuring a Message-of-the-Day Login Banner	38
Configuring a Login Banner	39
Managing the MAC Address Table	41
Changing the Address Aging Time	41
Configuring MAC Address Change Notification Traps	42
Configuring MAC Address Move Notification Traps	44
Configuring MAC Threshold Notification Traps	46
Adding and Removing Static Address Entries	49
Configuring Unicast MAC Address Filtering	50
Monitoring and Maintaining Administration of the Switch	51
Configuration Examples for Switch Administration	53
Example: Setting the System Clock	53
Examples: Configuring Summer Time	53
Example: Configuring a MOTD Banner	53
Example: Configuring a Login Banner	54
Example: Configuring MAC Address Change Notification Traps	54
Example: Configuring MAC Threshold Notification Traps	54
Example: Adding the Static Address to the MAC Address Table	54
Example: Configuring Unicast MAC Address Filtering	55
Additional References for Switch Administration	55
Feature History and Information for Switch Administration	56

---

**CHAPTER 4**
**Performing Switch Setup Configuration 57**

Finding Feature Information	57
Information About Performing Switch Setup Configuration	57
Switch Boot Process	58
Software Installer Features	58
Software Boot Modes	59
Installed Boot Mode	59
Bundle Boot Mode	59
Boot Mode for a Switch Stack	60

Switches Information Assignment	61
Default Switch Information	61
DHCP-Based Autoconfiguration Overview	61
DHCP Client Request Process	62
DHCP-based Autoconfiguration and Image Update	63
Restrictions for DHCP-based Autoconfiguration	63
DHCP Autoconfiguration	64
DHCP Auto-Image Update	64
DHCP Server Configuration Guidelines	64
Purpose of the TFTP Server	65
Purpose of the DNS Server	65
How to Obtain Configuration Files	66
How to Control Environment Variables	66
Common Environment Variables	67
Environment Variables for TFTP	69
Scheduled Reload of the Software Image	69
How to Perform Switch Setup Configuration	70
Configuring DHCP Autoconfiguration (Only Configuration File)	70
Configuring DHCP Auto-Image Update (Configuration File and Image)	72
Configuring the Client to Download Files from DHCP Server	76
Manually Assigning IP Information to Multiple SVIs	77
Modifying the Switch Startup Configuration	79
Specifying the Filename to Read and Write the System Configuration	79
Manually Booting the Switch	80
Booting the Switch in Installed Mode	81
Booting the Switch in Bundle Mode	83
Booting a Specific Software Image On a Switch Stack	83
Configuring a Scheduled Software Image Reload	85
Monitoring Switch Setup Configuration	86
Example: Verifying the Switch Running Configuration	86
Examples: Displaying Software Bootup in Install Mode	86
Example: Emergency Installation	88
Configuration Examples for Performing Switch Setup	89
Example: Configuring a Switch as a DHCP Server	89
Example: Configuring DHCP Auto-Image Update	90

Example: Configuring a Switch to Download Configurations from a DHCP Server	90
Examples: Scheduling Software Image Reload	90
Additional References For Performing Switch Setup	91
Feature History and Information For Performing Switch Setup Configuration	92

**CHAPTER 5****Configuring Right-To-Use Licenses 93**

Finding Feature Information	93
Restrictions for Configuring RTU Licenses	93
Information About Configuring RTU Licenses	94
Right-To-Use Licensing	94
Right-To-Use Image-Based Licenses	94
Right-To-Use License States	95
License Activation for Switch Stacks	95
Mobility Controller Mode	96
Right-To-Use AP-Count Licensing	96
Right-to-Use AP-Count Evaluation Licenses	97
Right-To-Use Adder AP-Count Rehosting Licenses	97
How to Configure RTU Licenses	97
Activating an Image Based License	97
Activating an AP-Count License	99
Obtaining an Upgrade or Capacity Adder License	100
Rehosting a License	100
Changing Mobility Mode	101
Monitoring and Maintaining RTU Licenses	103
Configuration Examples for RTU Licensing	103
Examples: Activating RTU Image Based Licenses	103
Examples: Displaying RTU Licensing Information	104
Example: Displaying RTU License Details	105
Example: Displaying RTU License Mismatch	105
Example: Displaying RTU Licensing Usage	106
Additional References for RTU Licensing	107
Feature History and Information for RTU Licensing	108

**CHAPTER 6****Configuring Administrator Usernames and Passwords 109**

Finding Feature Information	109
-----------------------------	-----

Information About Configuring Administrator Usernames and Passwords	109
Configuring Administrator Usernames and Passwords	111
Examples: Administrator Usernames and Passwords Configuration	112
Additional References for Administrator Usernames and Passwords	113
Feature History and Information For Performing Administrator Usernames and Passwords Configuration	114

**CHAPTER 7****Configuring 802.11 parameters and Band Selection 115**

Finding Feature Information	115
Restrictions on Band Selection, 802.11 Bands, and Parameters	115
Information About Configuring Band Selection, 802.11 Bands, and Parameters	116
Band Selection	116
Band Selection Algorithm	116
802.11 Bands	117
802.11n Parameter	117
802.11h Parameter	117
How to Configure 802.11 Bands and Parameters	118
Configuring Band Selection (CLI)	118
Configuring the 802.11 Bands (CLI)	119
Configuring 802.11n Parameters (CLI)	122
Configuring 802.11h Parameters (CLI)	125
Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters	126
Monitoring Configuration Settings Using Band Selection and 802.11 Bands Commands	126
Example: Viewing the Configuration Settings for 5-GHz Band	126
Example: Viewing the Configuration Settings for 24-GHz Band	128
Example: Viewing the status of 802.11h Parameters	129
Example: Verifying the Band Selection Settings	129
Configuration Examples for Band Selection, 802.11 Bands, and Parameters	130
Examples: Band Selection Configuration	130
Examples: 802.11 Bands Configuration	130
Examples: 802.11n Configuration	131
Examples: 802.11h Configuration	131
Additional References for 802.11 Parameters and Band Selection	132
Feature History and Information For Performing 802.11 parameters and Band Selection Configuration	133



---

**CHAPTER 8****Configuring Aggressive Load Balancing 135**

- Finding Feature Information 135
- Restrictions for Aggressive Load Balancing 135
- Information for Configuring Aggressive Load Balancing Parameters 136
  - Aggressive Load Balancing 136
- How to Configure Aggressive Load Balancing 137
  - Configuring Aggressive Load Balancing 137
- Monitoring Aggressive Load Balancing 138
- Examples: Aggressive Load Balancing Configuration 139
- Additional References for Aggressive Load Balancing 139
- Feature History and Information For Performing Aggressive Load Balancing Configuration 140

---

**CHAPTER 9****Configuring Client Roaming 141**

- Finding Feature Information 141
- Restrictions for Configuring Client Roaming 141
- Information About Client Roaming 142
  - Inter-Subnet Roaming 143
  - Voice-over-IP Telephone Roaming 143
  - CCX Layer 2 Client Roaming 143
- How to Configure Layer 2 or Layer 3 Roaming 144
  - Configuring Layer 2 or Layer 3 Roaming 144
  - Configuring CCX Client Roaming Parameters (CLI) 145
  - Configuring Mobility Oracle 147
  - Configuring Mobility Controller 148
  - Configuring Mobility Agent 150
- Monitoring Client Roaming Parameters 151
- Monitoring Mobility Configurations 151
- Additional References for Configuring Client Roaming 153
- Feature History and Information For Performing Client Roaming Configuration 154

---

**CHAPTER 10****Configuring Application Visibility and Control 155**

- Finding Feature Information 155
- Information About Application Visibility and Control 155
- Restrictions for Application Visibility and Control 156

How to Configure Application Visibility and Control	157
Configuring Application Visibility and Control (GUI)	157
Configuring Application Visibility (GUI)	157
Monitoring Application Visibility and Control	158
Monitoring Application Visibility and Control (CLI)	158
Monitoring Application Visibility and Control (GUI)	159
Examples: Application Visibility and Control	160
Examples: Application Visibility Configuration	160
Additional References for Application Visibility and Control	161
Feature History and Information For Application Visibility and Control	162

---

**CHAPTER 11**

<b>Configuring Voice and Video Parameters</b>	<b>163</b>
Finding Feature Information	163
Prerequisites for Voice and Video Parameters	163
Restrictions for Voice and Video Parameters	164
Information About Configuring Voice and Video Parameters	164
Call Admission Control	164
Static-Based CAC	165
Load-Based CAC	165
IOSd Call Admission Control	165
Expedited Bandwidth Requests	166
U-APSD	167
Traffic Stream Metrics	167
Information About Configuring Voice Prioritization Using Preferred Call Numbers	168
Information About EDCA Parameters	169
How to Configure Voice and Video Parameters	169
Configuring Voice Parameters (CLI)	169
Configuring Video Parameters (CLI)	173
Configuring SIP-Based CAC (CLI)	175
Configuring a Preferred Call Number (CLI)	177
Configuring EDCA Parameters (CLI)	178
Monitoring Voice and Video Parameters	180
Configuration Examples for Voice and Video Parameters	182
Example: Configuring Voice and Video	182
Additional References for Voice and Video Parameters	184

Feature History and Information For Performing Voice and Video Parameters Configuration 185

---

**CHAPTER 12**

**Configuring RFID Tag Tracking 187**

Finding Feature Information 187

Information About Configuring RFID Tag Tracking 187

How to Configure RFID Tag Tracking 188

    Configuring RFID Tag Tracking (CLI) 188

Monitoring RFID Tag Tracking Information 189

Additional References RFID Tag Tracking 189

Feature History and Information For Performing RFID Tag Tracking Configuration 190

---

**CHAPTER 13**

**Configuring Location Settings 191**

Finding Feature Information 191

Information About Configuring Location Settings 191

How to Configure Location Settings 192

    Configuring Location Settings (CLI) 192

    Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI) 194

    Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues (CLI) 195

Monitoring Location Settings and NMSP Settings 196

    Monitoring Location Settings (CLI) 196

    Monitoring NMSP Settings (CLI) 196

Examples: Location Settings Configuration 197

Examples: NMSP Settings Configuration 197

Additional References for Location Settings 198

Feature History and Information For Performing Location Settings Configuration 199

---

**CHAPTER 14**

**Monitoring Flow Control 201**

Finding Feature Information 201

Information About Flow Control 201

Monitoring Flow Control 201

Examples: Monitoring Flow Control 202

Additional References for Monitoring Flow Control 203

Feature History and Information For Monitoring Flow Control 204

---

**CHAPTER 15**

**Configuring SDM Templates 205**

Finding Feature Information	205
Information About Configuring SDM Templates	205
SDM Templates	205
SDM Templates and Switch Stacks	207
How to Configure SDM Templates	207
Configuring SDM Templates	207
Configuring the Switch SDM Template	207
Setting the SDM Template	207
Monitoring and Maintaining SDM Templates	209
Configuration Examples for SDM Templates	209
Examples: Configuring SDM Templates	209
Examples: Displaying SDM Templates	209
Feature History and Information for Configuring SDM Templates	210

**CHAPTER 16**

<b>Configuring System Message Logs</b>	<b>211</b>
Finding Feature Information	211
Restrictions for Configuring System Message Logs	211
Information About Configuring System Message Logs	212
System Message Logging	212
System Log Message Format	212
Default System Message Logging Settings	213
Syslog Message Limits	214
Enabling Syslog Trap Messages	214
How to Configure System Message Logs	215
Setting the Message Display Destination Device	215
Synchronizing Log Messages	216
Disabling Message Logging	218
Enabling and Disabling Time Stamps on Log Messages	218
Enabling and Disabling Sequence Numbers in Log Messages	219
Defining the Message Severity Level	220
Limiting Syslog Messages Sent to the History Table and to SNMP	221
Logging Messages to a UNIX Syslog Daemon	222
Monitoring and Maintaining System Message Logs	223
Monitoring Configuration Archive Logs	223
Configuration Examples for System Message Logs	224

Example: Stacking System Message	224
Example: Switch System Message	224
Additional References for System Message Logs	224
Feature History and Information For System Message Logs	226

**CHAPTER 17**

<b>Configuring Online Diagnostics</b>	<b>227</b>
Finding Feature Information	227
Information About Configuring Online Diagnostics	227
Online Diagnostics	227
How to Configure Online Diagnostics	228
Starting Online Diagnostic Tests	228
Configuring Online Diagnostics	229
Scheduling Online Diagnostics	229
Configuring Health-Monitoring Diagnostics	230
Monitoring and Maintaining Online Diagnostics	233
Displaying Online Diagnostic Tests and Test Results	233
Configuration Examples for Online Diagnostic Tests	234
Examples: Start Diagnostic Tests	234
Example: Configure a Health Monitoring Test	234
Examples: Schedule Diagnostic Test	234
Examples: Displaying Online Diagnostics	235
Additional References for Online Diagnostics	236
Feature History and Information for Configuring Online Diagnostics	237

**CHAPTER 18**

<b>Managing Configuration Files</b>	<b>239</b>
Prerequisites for Managing Configuration Files	239
Restrictions for Managing Configuration Files	239
Information About Managing Configuration Files	240
Types of Configuration Files	240
Configuration Mode and Selecting a Configuration Source	240
Configuration File Changes Using the CLI	240
Location of Configuration Files	241
Copy Configuration Files from a Network Server to the Switch	241
Copying a Configuration File from the Switch to a TFTP Server	242
Copying a Configuration File from the Switch to an RCP Server	242

Restrictions	242
Requirements for the RCP Username	243
Copying a Configuration File from the Switch to an FTP Server	243
Understanding the FTP Username and Password	244
Copy Configuration Files from a Switch to Another Switch	244
Configuration Files Larger than NVRAM	244
Compressing the Configuration File	245
Storing the Configuration in Flash Memory on Class A Flash File Systems	245
Loading the Configuration Commands from the Network	245
Configuring the Switch to Download Configuration Files	245
Network Versus Host Configuration Files	246
How to Manage Configuration File Information	246
Displaying Configuration File Information (CLI)	246
Modifying the Configuration File (CLI)	247
Copying a Configuration File from the Switch to a TFTP Server (CLI)	249
What to Do Next	250
Copying a Configuration File from the Switch to an RCP Server (CLI)	250
Examples	251
Storing a Running Configuration File on an RCP Server	251
Storing a Startup Configuration File on an RCP Server	252
What to Do Next	252
Copying a Configuration File from the Switch to the FTP Server (CLI)	252
Examples	254
Storing a Running Configuration File on an FTP Server	254
Storing a Startup Configuration File on an FTP Server	254
What to Do Next	254
Copying a Configuration File from a TFTP Server to the Switch (CLI)	254
What to Do Next	255
Copying a Configuration File from the rcp Server to the Switch (CLI)	256
Examples	257
Copy RCP Running-Config	257
Copy RCP Startup-Config	257
What to Do Next	257
Copying a Configuration File from an FTP Server to the Switch (CLI)	258
Examples	259

Copy FTP Running-Config	259
Copy FTP Startup-Config	259
What to Do Next	260
Maintaining Configuration Files Larger than NVRAM	260
Compressing the Configuration File (CLI)	260
Storing the Configuration in Flash Memory on Class A Flash File Systems (CLI)	262
Loading the Configuration Commands from the Network (CLI)	263
Copying Configuration Files from Flash Memory to the Startup or Running Configuration (CLI)	265
Copying Configuration Files Between Flash Memory File Systems (CLI)	266
Copying a Configuration File from an FTP Server to Flash Memory Devices (CLI)	267
What to Do Next	269
Copying a Configuration File from an RCP Server to Flash Memory Devices (CLI)	269
Copying a Configuration File from a TFTP Server to Flash Memory Devices (CLI)	270
Re-executing the Configuration Commands in the Startup Configuration File (CLI)	271
Clearing the Startup Configuration (CLI)	271
Deleting a Specified Configuration File (CLI)	272
Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems (CLI)	273
What to Do Next	275
Configuring the Switch to Download Configuration Files	275
Configuring the Switch to Download the Network Configuration File (CLI)	275
Configuring the Switch to Download the Host Configuration File (CLI)	277
Additional References	279

---

**CHAPTER 19**
**Configuration Replace and Configuration Rollback 281**

Prerequisites for Configuration Replace and Configuration Rollback	281
Restrictions for Configuration Replace and Configuration Rollback	282
Information About Configuration Replace and Configuration Rollback	282
Configuration Archive	282
Configuration Replace	283
Configuration Rollback	284
Configuration Rollback Confirmed Change	284
Benefits of Configuration Replace and Configuration Rollback	284
How to Use Configuration Replace and Configuration Rollback	285
Creating a Configuration Archive (CLI)	285

Performing a Configuration Replace or Configuration Rollback Operation (CLI)	286
Monitoring and Troubleshooting the Feature (CLI)	288
Configuration Examples for Configuration Replace and Configuration Rollback	291
Creating a Configuration Archive	291
Replacing the Current Running Configuration with a Saved Cisco IOS Configuration File	291
Reverting to the Startup Configuration File	292
Performing a Configuration Replace Operation with the configure confirm Command	292
Performing a Configuration Rollback Operation	292
Additional References	293

---

**CHAPTER 20**

<b>Working with the Flash File System</b>	<b>297</b>
Information About the Flash File System	297
Displaying Available File Systems	298
Setting the Default File System	300
Displaying Information About Files on a File System	300
Changing Directories and Displaying the Working Directory (CLI)	301
Creating Directories (CLI)	302
Removing Directories	303
Copying Files	303
Copying Files from One Switch in a Stack to Another Switch in the Same Stack	304
Deleting Files	305
Creating, Displaying and Extracting Files (CLI)	305
Additional References	307

---

**CHAPTER 21**

<b>Working with Cisco IOS XE Software Bundles</b>	<b>311</b>
About Software Bundles and Packages	311
Bundle and Package File Location on the Switch	311
Upgrading Cisco IOS XE Software	312
Upgrading Cisco IOS XE Software: Install Mode	312
Upgrading Cisco IOS XE Software Install Mode Example	312
Upgrading Cisco IOS XE Software: Bundle Mode	313
Upgrading Cisco IOS XE Software Bundle Mode Example	313
Converting from the Bundle Running Mode to the Install Running Mode	314
Converting from the Bundle Running Mode to the Install Running Mode Example	314



Copying IOS XE Package and Bundle Files from One Stack Member to Another	315
Copying IOS XE Package and Bundle Files from One Stack Member to Another Example	315
Upgrading a Switch Running Incompatible Software	316
Upgrading a Switch Running Incompatible Software Example	317
Upgrading a Switch Running in Incompatible Running Mode	318
Upgrading a Switch Running in Incompatible Running Mode Example	318
Additional References	320

**CHAPTER 22**

<b>Troubleshooting the Software Configuration</b>	<b>323</b>
Finding Feature Information	323
Information About Troubleshooting the Software Configuration	324
Software Failure on a Switch	324
Lost or Forgotten Password on a Switch	324
Power over Ethernet Ports	324
Disabled Port Caused by Power Loss	325
Disabled Port Caused by False Link-Up	325
Ping	325
Layer 2 Traceroute	326
Layer 2 Traceroute Guidelines	326
IP Traceroute	327
Time Domain Reflector Guidelines	327
Debug Commands	328
Crashinfo Files	329
System Reports	330
Onboard Failure Logging on the Switch	330
Fan Failures	331
Possible Symptoms of High CPU Utilization	331
How to Troubleshoot the Software Configuration	331
Recovering from a Software Failure	331
Recovering from a Lost or Forgotten Password	333
Procedure with Password Recovery Enabled	335
Procedure with Password Recovery Disabled	336
Preventing Switch Stack Problems	338
Preventing Autonegotiation Mismatches	339

Troubleshooting SFP Module Security and Identification	339
Monitoring SFP Module Status	340
Executing Ping	340
Monitoring Temperature	340
Monitoring the Physical Path	341
Executing IP Traceroute	341
Running TDR and Displaying the Results	341
Redirecting Debug and Error Message Output	342
Using the show platform forward Command	342
Using the show debug command	342
Configuring OBFL	343
WSMA Configuration for WebUI	343
Verifying Troubleshooting of the Software Configuration	344
Displaying OBFL Information	344
Example: Verifying the Problem and Cause for High CPU Utilization	345
Scenarios for Troubleshooting the Software Configuration	346
Scenarios to Troubleshoot Power over Ethernet (PoE)	346
Configuration Examples for Troubleshooting Software	349
Example: Pinging an IP Host	349
Example: Performing a Traceroute to an IP Host	349
Example: Enabling All System Diagnostics	350
Additional References for Troubleshooting Software Configuration	351
Feature History and Information for Troubleshooting Software Configuration	352



## Preface

- [Document Conventions](#), page xix
- [Related Documentation](#), page xxi
- [Obtaining Documentation and Submitting a Service Request](#), page xxi

## Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <i>courier font</i> .
<b>Bold Courier font</b>	<b>Bold Courier font</b> indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x   y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
{x   y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y   z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



#### Note

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



#### Tip

Means *the following information will help you solve a problem*.



#### Caution

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



#### Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



#### Warning

### IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

## Related Documentation

**Note**

---

Before installing or upgrading the switch, refer to the switch release notes.

---

- Cisco Catalyst 3650 Series Switches documentation, located at:  
[http://www.cisco.com/go/cat3650\\_docs](http://www.cisco.com/go/cat3650_docs)
- Cisco SFP, SFP+, and QSFP+ modules documentation, including compatibility matrixes, located at:  
[http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html)

## Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

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





# Using the Command-Line Interface

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 6](#)

## Information About Using the Command-Line Interface

### Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, an SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode .

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	Switch>	Enter <b>logout</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display system information.</li> </ul>
Privileged EXEC	While in user EXEC mode, enter the <b>enable</b> command.	Switch#	Enter <b>disable</b> to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	Switch(config)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> .	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the <b>vlan <i>vlan-id</i></b> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the <b>exit</b> command.  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the <b>interface</b> command (with a specific interface).	Switch(config-if)#		Use this mode to configure parameters for the Ethernet ports.



Mode	Access Method	Prompt	Exit Method	About This Mode
			To exit to global configuration mode, enter <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	
Line configuration	While in global configuration mode, specify a line with the <b>line vty</b> or <b>line console</b> command.	Switch(config-line)#	To exit to global configuration mode, enter <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure parameters for the terminal line.

## Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Switch# show conf
```

## No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenab a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

## CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.

**Table 2: Common CLI Error Messages**

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your switch to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode.  The possible keywords that you can enter with the command appear.

## Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.




---

**Note** Only CLI or HTTP changes are logged.

---

## Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

## SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry ?*
3. *abbreviated-command-entry <Tab>*
4. **?**
5. *command ?*
6. *command keyword ?*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>help</b>  <b>Example:</b> Switch# <b>help</b>	Obtains a brief description of the help system in any command mode.
Step 2	<i>abbreviated-command-entry ?</i>  <b>Example:</b> Switch# <b>di?</b> dir disable disconnect	Obtains a list of commands that begin with a particular character string.
Step 3	<i>abbreviated-command-entry &lt;Tab&gt;</i>  <b>Example:</b> Switch# <b>sh conf&lt;tab&gt;</b> Switch# <b>show configuration</b>	Completes a partial command name.
Step 4	<b>?</b>  <b>Example:</b> Switch> <b>?</b>	Lists all commands available for a particular command mode.
Step 5	<i>command ?</i>  <b>Example:</b> Switch> <b>show ?</b>	Lists the associated keywords for a command.
Step 6	<i>command keyword ?</i>  <b>Example:</b> Switch(config)# <b>cdp holdtime ?</b> <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

# How to Use the CLI to Configure Features

## Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

### Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

#### SUMMARY STEPS

1. `terminal history [size number-of-lines]`

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>terminal history [size number-of-lines]</code>  <b>Example:</b> Switch# <code>terminal history size 200</code>	Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

## Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.



#### Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

#### SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. `show history`

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>Ctrl-P</b> or use the <b>up arrow</b> key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
<b>Step 2</b>	<b>Ctrl-N</b> or use the <b>down arrow</b> key	Returns to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the up arrow key. Repeat the key sequence to recall successively more recent commands.
<b>Step 3</b>	<b>show history</b>  <b>Example:</b> Switch# <b>show history</b>	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the <b>terminal history</b> global configuration command and the <b>history</b> line configuration command.

**Disabling the Command History Feature**

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

**SUMMARY STEPS**

1. **terminal no history**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal no history</b>  <b>Example:</b> Switch# <b>terminal no history</b>	Disables the feature during the current terminal session in privileged EXEC mode.

**Enabling and Disabling Editing Features**

Although enhanced editing mode is automatically enabled, you can disable it and reenable it.

**SUMMARY STEPS**

1. **terminal editing**
2. **terminal no editing**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal editing</b>  <b>Example:</b> Switch# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
<b>Step 2</b>	<b>terminal no editing</b>  <b>Example:</b> Switch# <code>terminal no editing</code>	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

## Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.

**Note**

The arrow keys function only on ANSI-compatible terminals such as VT100s.

**Table 3: Editing Commands**

Editing Commands	Description
<b>Ctrl-B</b> or use the <b>left arrow</b> key	Moves the cursor back one character.
<b>Ctrl-F</b> or use the <b>right arrow</b> key	Moves the cursor forward one character.
<b>Ctrl-A</b>	Moves the cursor to the beginning of the command line.
<b>Ctrl-E</b>	Moves the cursor to the end of the command line.
<b>Esc B</b>	Moves the cursor back one word.
<b>Esc F</b>	Moves the cursor forward one word.
<b>Ctrl-T</b>	Transposes the character to the left of the cursor with the character located at the cursor.
<b>Delete</b> or <b>Backspace</b> key	Erases the character to the left of the cursor.
<b>Ctrl-D</b>	Deletes the character at the cursor.

<b>Ctrl-K</b>	Deletes all characters from the cursor to the end of the command line.
<b>Ctrl-U</b> or <b>Ctrl-X</b>	Deletes all characters from the cursor to the beginning of the command line.
<b>Ctrl-W</b>	Deletes the word to the left of the cursor.
<b>Esc D</b>	Deletes from the cursor to the end of the word.
<b>Esc C</b>	Capitalizes at the cursor.
<b>Esc L</b>	Changes the word at the cursor to lowercase.
<b>Esc U</b>	Capitalizes letters from the cursor to the end of the word.
<b>Ctrl-V</b> or <b>Esc Q</b>	Designates a particular keystroke as an executable command, perhaps as a shortcut.
<b>Return</b> key	Scrolls down a line or screen on displays that are longer than the terminal screen can display.  <b>Note</b> The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including <b>show</b> command output. You can use the <b>Return</b> and <b>Space</b> bar keystrokes whenever you see the More prompt.
<b>Space</b> bar	Scrolls down one screen.
<b>Ctrl-L</b> or <b>Ctrl-R</b>	Redisplays the current command line if the switch suddenly sends a message to your screen.

## Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.



**Note**

The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

**SUMMARY STEPS**

1. **access-list**
2. **Ctrl-A**
3. **Return key**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<p><b>access-list</b></p> <p><b>Example:</b></p> <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Switch(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Switch(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	<p>Displays the global configuration command entry that extends beyond one line.</p> <p>When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.</p>
<b>Step 2</b>	<p><b>Ctrl-A</b></p> <p><b>Example:</b></p> <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2\$</pre>	<p>Checks the complete syntax.</p> <p>The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.</p>
<b>Step 3</b>	<p><b>Return key</b></p>	<p>Execute the commands.</p> <p>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the <b>terminal width</b> privileged EXEC command to set the width of your terminal.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

**Searching and Filtering Output of show and more Commands**

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

**SUMMARY STEPS**

1. **{show | more} command | {begin | include | exclude} regular-expression**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>{<b>show</b>   <b>more</b>} <i>command</i>   {<b>begin</b>   <b>include</b>   <b>exclude</b>} <i>regular-expression</i></p> <p><b>Example:</b>  Switch# <b>show interfaces   include protocol</b>  Vlan1 is up, line protocol is up  Vlan10 is up, line protocol is down  GigabitEthernet1/0/1 is up, line protocol is down  GigabitEthernet1/0/2 is up, line protocol is up</p>	<p>Searches and filters the output.</p> <p>Expressions are case sensitive. For example, if you enter   <b>exclude output</b>, the lines that contain <b>output</b> are not displayed, but the lines that contain <b>output</b> appear.</p>

## Accessing the CLI on a Switch Stack

You can access the CLI through a console connection, through Telnet, a SSH, or by using the browser.

You manage the switch stack and the stack member interfaces through the active switch. You cannot manage stack members on an individual switch basis. You can connect to the active switch through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the active switch. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.


**Note**

We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

To debug the standby switch, use the **session standby ios** privileged EXEC command from the active switch to access the IOS console of the standby switch. To debug a specific stack member, use the **session switch stack-member-number** privileged EXEC command from the active switch to access the diagnostic shell of the stack member. For more information about these commands, see the switch command reference.

To debug a specific stack member, you can start a CLI session from the stack master by using the **session stack-member-number** privileged EXEC command. The stack member number is appended to the system prompt. For example, *Switch-2#* is the prompt for stack member 2 where the system prompt for the stack master is *Switch*. Only the **show** and **debug** commands are available in a CLI session to a specific stack member. You can also use the **remote command stack-member-number LINE** privileged EXEC command on the stack master to enable debugging on a member switch without first starting a session.

## Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

If your switch is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your switch must first be configured for this type of access.

You can use one of these methods to establish a connection with the switch:

- Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.
  - The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
  - The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.



## CHAPTER

# 2

## Using the Web Graphical User Interface

- [Prerequisites for Using the Web GUI](#), page 13
- [Information About Using The Web GUI](#), page 14
- [Connecting the Console Port of the Switch](#) , page 15
- [Logging On to the GUI](#), page 16
- [Enabling Web and Secure Web Modes](#) , page 16
- [Configuring the Switch Web GUI](#), page 17

## Prerequisites for Using the Web GUI

### Wired Web UI (Device Manager) System Requirements

#### Hardware Requirements

**Table 4: Minimum Hardware Requirements**

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum <a href="#">1</a>	512 MB <a href="#">2</a>	256	1024 x 768	Small

<sup>1</sup> We recommend 1 GHz.

<sup>2</sup> We recommend 1 GB DRAM.

#### Software Requirements

- – Windows 7, Windows Vista, Windows XP, Windows 2003, or Windows 2000
- – Microsoft Internet Explorer 6.0 and 7.0, and Mozilla Firefox up to version 26.0, with JavaScript enabled.

### Wireless Web UI Software Requirements

- Operating Systems
  - Windows 7
  - Windows 8
  - Mac OS X 10.8
- Browsers:
  - Google Chrome, version 35
  - Microsoft Internet Explorer, versions 10 or 11
  - Mozilla Firefox, version 30 or later
  - Safari, version 6.1

## Information About Using The Web GUI

A web browser, or graphical user interface (GUI), is built into each switch.

You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface. Click Help at the top of any page in the GUI to display online help. You might need to disable your browser's pop-up blocker to view the online help.

**Note**

---

The following special characters are not supported in the GUI: ampersand (&), semicolon (;), and lesser than (<).

---

## Web GUI Features

The switch web GUI supports the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:

- Admin Users
- SNMP System Summary
- Management Port
- Wireless Management
- RF Mobility and Country code
- Mobility configuration
- WLANs

- 802.11 Configuration
- Set Time

The Monitor tab:

- Displays summary details of switch, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification-friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:

- Enables you to configure the switch for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the switch, WLAN, and radios.
- Enables you to configure and set security policies on your switch.
- Enables you to access the switch operating system software management commands.

The Administration tab enables you to configure system logs.

## Connecting the Console Port of the Switch

### Before You Begin

Before you can configure the switch for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).

- 
- Step 1** Connect one end of a null-modem serial cable to the switch's RJ-45 console port and the other end to your PC's serial port.
- Step 2** Plug the AC power cord into the switch and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet. Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self-test verification) and basic configuration. If the switch passes the power-on self-test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.
- Step 3** Enter **yes**. Proceed with basic initial setup configuration parameters in the CLI setup wizard. Specify the IP address for the service port which is the gigabitethernet 0/0 interface.  
After entering the configuration parameters in the configuration wizard, you can access the Web GUI. Now, the switch is configured with the IP address for service port.
-

## Logging On to the GUI



**Note** Do not configure TACACS authentication when the controller is set to use local authentication.

---

Enter the switch IP address in your browser's address bar. For a secure connection, enter **https://ip-address**. For a less secure connection, enter **http://ip-address**.

---

## Enabling Web and Secure Web Modes

- 
- Step 1** Choose **Configuration > Switch > Management > Protocol Management > HTTP-HTTPS**.  
The **HTTP-HTTPS Configuration** page appears.
- Step 2** To enable web mode, which allows users to access the switch GUI using "http://ip-address," choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled. Web mode (HTTP) is not a secure connection.
- Step 3** To enable secure web mode, which allows users to access the switch GUI using "https://ip-address," choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled. Secure web mode (HTTPS) is a secure connection.
- Step 4** Choose to track the device in the IP Device Tracking check box.
- Step 5** Choose to enable the trust point in the Enable check box.
- Step 6** Choose the trustpoints from the Trustpoints drop-down list.
- Step 7** Enter the amount of time, in seconds, before the web session times out due to inactivity in the HTTP Timeout-policy (1 to 600 sec) text box.  
The valid range is from 1 to 600 seconds.
- Step 8** Enter the server life time in the Server Life Time (1 to 86400 sec) text box.  
The valid range is from 1 to 86400 seconds.
- Step 9** Enter the maximum number of connection requests that the server can accept in the Maximum number of Requests (1 to 86400) text box.  
The valid range is from 1 to 86400 connections.
- Step 10** Click **Apply**.
- Step 11** Click **Save Configuration**.
-

# Configuring the Switch Web GUI

The configuration wizard enables you to configure basic settings on the switch. You can run the wizard after you receive the switch from the factory or after the switch has been reset to factory defaults. The configuration wizard is available in both GUI and CLI formats.

- 
- Step 1** Connect your PC to the service port and configure an IPv4 address to use the same subnet as the switch. The switch is loaded with IOS XE image and the service port interface is configured as gigabitethernet 0/0.
- Step 2** Start Internet Explorer 10 (or later), Firefox 2.0.0.11 (or later), or Google Chrome on your PC and enter the management interface IP address on the browser window. The management interface IP address is same as the gigabitethernet 0/0 (also known as service port interface). When you log in for the first time, you need to enter HTTP username and password. By default, the username is **admin** and the password is **cisco**. You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.
- When you log in for the first time, the **Accessing Cisco Switch <Model Number> <Hostname>** page appears.
- Step 3** On the **Accessing Cisco Switch** page, click the **Wireless Web GUI** link to access switch web GUI **Home** page.
- Step 4** Choose **Configuration > Wizard** to perform all steps that you need to configure the switch initially. The **Admin Users** page appears.
- Step 5** On the **Admin Users** page, enter the administrative username to be assigned to this switch in the User Name text box and the administrative password to be assigned to this switch in the Password and Confirm Password text boxes. Click **Next**. The default username is **admin** and the default password is **cisco**. You can also create a new administrator user for the switch. You can enter up to 24 ASCII characters for username and password.
- The **SNMP System Summary** page appears.
- Step 6** On the **SNMP System Summary** page, enter the following SNMP system parameters for the switch, and click **Next**:
- Customer-definable switch location in the Location text box.
  - Customer-definable contact details such as phone number with names in the Contact text box.
  - Choose **enabled** to send SNMP notifications for various SNMP traps or **disabled** not to send SNMP notifications for various SNMP traps from the SNMP Global Trap drop-down list.
  - Choose **enabled** to send system log messages or **disabled** not to send system log messages from the SNMP Logging drop-down list.
- Note** The SNMP trap server, must be reachable through the distribution ports (and not through the gigabitethernet0/0 service or management interface).
- The **Management Port** page appears.
- Step 7** In the **Management Port** page, enter the following parameters for the management port interface (gigabitethernet 0/0) and click **Next**.
- Interface IP address that you assigned for the service port in the IP Address text box.
  - Network mask address of the management port interface in the Netmask text box.

- The IPv4 Dynamic Host Configuration Protocol (DHCP) address for the selected port in the IPv4 DHCP Server text box.

The **Wireless Management** page appears.

**Step 8** In the **Wireless Management** page, enter the following wireless interface management details, and click **Next**.

- Choose the interface—VLAN, or Ten Gigabit Ethernet from the Select Interface drop-down list.
- VLAN tag identifier, or 0 for no VLAN tag in the VLAN id text box.
- IP address of wireless management interface where access points are connected in the IP Address text box.
- Network mask address of the wireless management interface in the Netmask text box.
- DHCP IPv4 IP address in the IPv4 DHCP Server text box.

When selecting VLAN as interface, you can specify the ports as –Trunk or Access ports from the selected list displayed in the Switch Port Configuration text box.

The **RF Mobility and Country Code** page appears.

**Step 9** In the **RF Mobility and Country Code** page, enter the RF mobility domain name in the RF Mobility text box, choose current country code from the Country Code drop-down list, and click **Next**. From the GUI, you can select only one country code.

**Note** Before configuring RF grouping parameters and mobility configuration, ensure that you refer to the relevant conceptual content and then proceed with the configuration.

The **Mobility Configuration** page with mobility global configuration settings appears.

**Step 10** In the **Mobility Configuration** page, view and enter the following mobility global configuration settings, and click **Next**.

- Choose **Mobility Controller** or **Mobility Agent** from the Mobility Role drop-down list:
  - If Mobility Agent is chosen, enter the mobility controller IP address in the Mobility Controller IP Address text box and mobility controller IP address in the Mobility Controller Public IP Address text box.
  - If Mobility Controller is chosen, then the mobility controller IP address and mobility controller public IP address are displayed in the respective text boxes.
- Displays mobility protocol port number in the Mobility Protocol Port text box.
- Displays the mobility switch peer group name in the Mobility Switch Peer Group Name text box.
- Displays whether DTLS is enabled in the DTLS Mode text box.
 

DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS.
- Displays mobility domain identifier for 802.11 radios in the Mobility Domain ID for 802.11 radios text box.
- The amount of time (in seconds) between each ping request sent to an peer switch in the Mobility Keepalive Interval (1-30)sec text box.
 

Valid range is from 1 to 30 seconds, and the default value is 10 seconds.
- Number of times a ping request is sent to an peer switch before the peer is considered to be unreachable in the Mobility Keepalive Count (3-20) text box.
 

The valid range is from 3 to 20, and the default value is 3.



- The DSCP value that you can set for the mobility switch in the Mobility Control Message DSCP Value (0-63) text box.

The valid range is 0 to 63, and the default value is 0.

- Displays the number of mobility switch peer group member configured in the Switch Peer Group Members Configured text box.

The **WLANs** page appears.

**Step 11** In the **WLANs** page, enter the following WLAN configuration parameters, and click **Next**.

- WLAN identifier in the WLAN ID text box.
- SSID of the WLAN that the client is associated with in the SSID text box.
- Name of the WLAN used by the client in the Profile Name text box.

The **802.11 Configuration** page appears.

**Step 12** In the **802.11 Configuration** page, check either one or both 802.11a/n/ac and 802.11b/g/n check boxes to enable the 802.11 radios, and click **Next**.

The **Set Time** page appears.

**Step 13** In the **Set Time** page, you can configure the time and date on the switch based on the following parameters, and click **Next**.

- Displays current timestamp on the switch in the Current Time text box.
- Choose either Manual or NTP from the Mode drop-down list.  
On using the NTP server, all access points connected to the switch, synchronizes its time based on the NTP server settings available.
- Choose date on the switch from the Year, Month, and Day drop-down list.
- Choose time from the Hours, Minutes, and Seconds drop-down list.
- Enter the time zone in the Zone text box and select the off setting required when compared to the current time configured on the switch from the Offset drop-down list.

The **Save Wizard** page appears.

**Step 14** In the **Save Wizard** page, you can review the configuration settings performed on the switch using these steps, and if you wish to change any configuration value, click **Previous** and navigate to that page. You can save the switch configuration created using the wizard only if a success message is displayed for all the wizards. If the **Save Wizard** page displays errors, you must recreate the wizard for initial configuration of the switch.

---





## Administering the System

---

- [Finding Feature Information, page 21](#)
- [Information About Administering the Switch, page 21](#)
- [How to Administer the Switch, page 29](#)
- [Monitoring and Maintaining Administration of the Switch, page 51](#)
- [Configuration Examples for Switch Administration, page 53](#)
- [Additional References for Switch Administration, page 55](#)
- [Feature History and Information for Switch Administration, page 56](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

#### Related Topics

[Feature History and Information for Troubleshooting Software Configuration, on page 352](#)

### Information About Administering the Switch

#### System Time and Date Management

You can manage the system time and date on your switch 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](http://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:

- 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

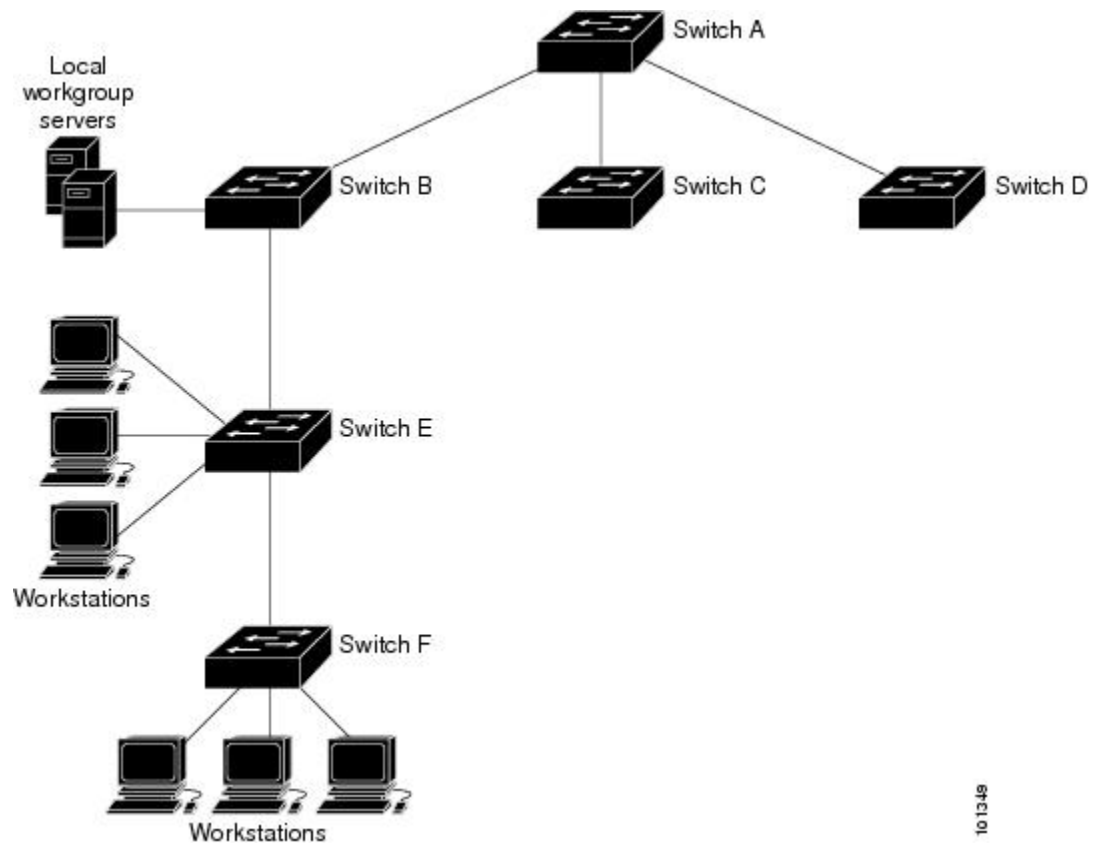
LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

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 below shows a typical network example using NTP. Switch A is the NTP master, 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 Switch, Switch B and Switch 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.

## NTP Security

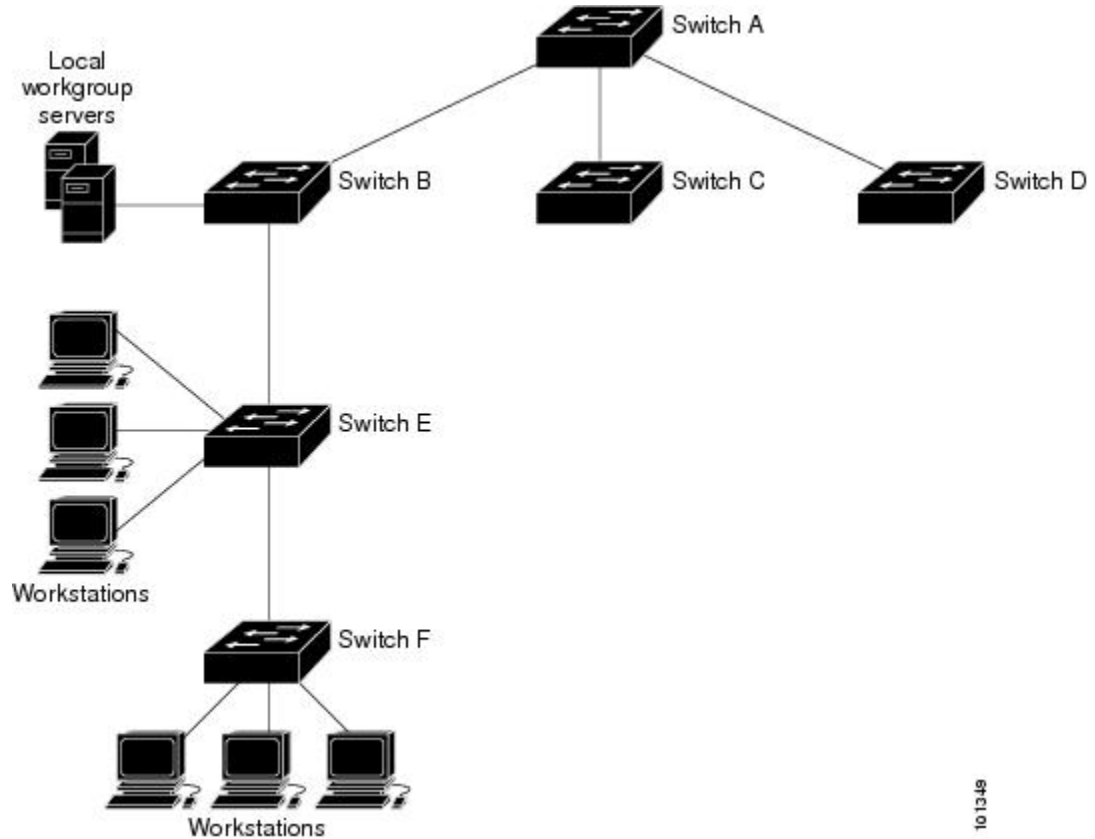
The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

## 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.

The following figure shows a typical network example using NTP. Switch A is the NTP master, 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.

**Figure 2: Typical NTP Network Configuration**



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.

## NTP Version 4

NTP version 4 is implemented on the switch. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6.

- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

For details about configuring NTPv4, see the *Implementing NTPv4 in IPv6* chapter of the *Cisco IOS IPv6 Configuration Guide, Release 12.4T*.

## System Name and Prompt

You configure the system name on the Switch 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 switch, 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 5: 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 switch 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 switch 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 switch 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 switch to other network devices. The switch 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 switch 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 switch maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch 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 switch 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 Switch 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 Switch joins a switch stack, that Switch 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 6: Default Settings for the MAC Address**

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned

Feature	Default Setting
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 Switch

### 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 switch can synchronize, you do not need to manually set the system clock.

#### 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:

#### SUMMARY STEPS

1. **enable**
2. Use one of the following:
  - **clock set** *hh:mm:ss day month year*
  - **clock set** *hh:mm:ss month day year*

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	Use one of the following: <ul style="list-style-type: none"> <li>• <b>clock set</b> <i>hh:mm:ss day month year</i></li> <li>• <b>clock set</b> <i>hh:mm:ss month day year</i></li> </ul> <b>Example:</b> Switch# <b>clock set 13:32:00 23 March 2013</b>	Manually set the system clock using one of these formats: <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>day</i>—Specifies the day by date in the month.</li> <li>• <i>month</i>—Specifies the month by name.</li> <li>• <i>year</i>—Specifies the year (no abbreviation).</li> </ul>

## Configuring the Time Zone

Follow these steps to manually configure the time zone:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock timezone zone hours-offset [minutes-offset]**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 3</b>	<b>clock timezone zone hours-offset</b> [minutes-offset]  <b>Example:</b> Switch(config)# <b>clock timezone AST -3 30</b>	Sets the time zone.  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. <ul style="list-style-type: none"> <li>• <i>zone</i>—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC.</li> <li>• <i>hours-offset</i>—Enters the hours offset from UTC.</li> <li>• (Optional) <i>minutes-offset</i>—Enters the minutes offset from UTC. This available where the local time zone is a percentage of an hour different from UTC.</li> </ul>
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b>  <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(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:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock summer-time zone date date month year hh:mm date month year hh:mm [offset]**
4. **clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 3</b>	<b>clock summer-time zone date date month year hh:mm date month year hh:mm [offset]</b>  <b>Example:</b> Switch(config)# <b>clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00</b>	Configures summer time to start and end on specified days every year.
<b>Step 4</b>	<b>clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]</b>  <b>Example:</b> Switch(config)# <b>clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00</b>	<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 <b>clock summer-time zone recurring</b> 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"> <li>• <i>zone</i>—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect.</li> <li>• (Optional) <i>week</i>— Specifies the week of the month (1 to 4, <b>first</b>, or <b>last</b>).</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• (Optional) <i>day</i>—Specifies the day of the week (Sunday, Monday...).</li> <li>• (Optional) <i>month</i>—Specifies the month (January, February...).</li> <li>• (Optional) <i>hh:mm</i>—Specifies the time (24-hour format) in hours and minutes.</li> <li>• (Optional) <i>offset</i>—Specifies the number of minutes to add during summer time. The default is 60.</li> </ul>
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show running-config</b>  <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
<b>Step 7</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

Follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock summer-time zone date** [ *month date year hh:mm month date year hh:mm [offset]* ] or **clock summer-time zone date** [ *date month year hh:mm date month year hh:mm [offset]* ]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p><b>clock summer-time zone date</b> [ <i>month date year hh:mm month date year hh:mm [offset]</i> ] or <b>clock summer-time zone date</b> [ <i>date month year hh:mm date month year hh:mm [offset]</i> ]</p>	<p>Configures summer time to start on the first date and end on the second date.</p> <p>Summer time is disabled by default.</p> <ul style="list-style-type: none"> <li>• For <i>zone</i>, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect.</li> <li>• (Optional) For <i>week</i>, specify the week of the month (1 to 5 or last).</li> <li>• (Optional) For <i>day</i>, specify the day of the week (Sunday, Monday...).</li> <li>• (Optional) For <i>month</i>, specify the month (January, February...).</li> <li>• (Optional) For <i>hh:mm</i>, specify the time (24-hour format) in hours and minutes.</li> <li>• (Optional) For <i>offset</i>, specify the number of minutes to add during summer time. The default is 60.</li> </ul>
Step 4	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Switch# show running-config</pre>	Verifies your entries.



	Command or Action	Purpose
Step 6	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## Configuring a System Name

Follow these steps to manually configure a system name:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `hostname name`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Switch> <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters the global configuration mode.
Step 3	<b>hostname name</b>  <b>Example:</b> Switch(config)# <code>hostname remote-users</code>	Configures a system name. When you set the system name, it is also used as the system prompt.  The default setting is Switch.  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.

	Command or Action	Purpose
<b>Step 4</b>	<b>end</b>  <b>Example:</b> remote-users (config) # <b>end</b> remote-users#	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b>  <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Setting Up DNS

If you use the switch 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** global configuration command. 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:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip domain-name** *name*
4. **ip name-server** *server-address1* [*server-address2* ... *server-address6*]
5. **ip domain-lookup** [**nsap** | **source-interface** *interface*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p><b>ip domain-name <i>name</i></b></p> <p><b>Example:</b></p> <pre>Switch(config)# ip domain-name Cisco.com</pre>	<p>Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).</p> <p>Do not include the initial period that separates an unqualified name from the domain name.</p> <p>At boot time, no domain name is configured; however, if the switch 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).</p>
Step 4	<p><b>ip name-server <i>server-address1</i> [<i>server-address2 ... server-address6</i>]</b></p> <p><b>Example:</b></p> <pre>Switch(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300</pre>	<p>Specifies the address of one or more name servers to use for name and address resolution.</p> <p>You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.</p>
Step 5	<p><b>ip domain-lookup [<i>nsap</i>   <i>source-interface interface</i>]</b></p> <p><b>Example:</b></p> <pre>Switch(config)# ip domain-lookup</pre>	<p>(Optional) Enables DNS-based hostname-to-address translation on your switch. This feature is enabled by default.</p> <p>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).</p>
Step 6	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.

	Command or Action	Purpose
<b>Step 7</b>	<b>show running-config</b>  <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
<b>Step 8</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

### What to Do Next

## 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 switch

Follow these steps to configure a MOTD login banner:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner motd *c message c***
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 3</b>	<b>banner motd c message c</b>  <b>Example:</b> Switch(config)# <b>banner motd #</b> 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 <b>Return</b> key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.  <i>message</i> —Enters a banner message up to 255 characters. You cannot use the delimiting character in the message.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b>  <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(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:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **banner login *c message c***
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 3</b>	<b>banner login <i>c message c</i></b>  <b>Example:</b> Switch(config)# <b>banner login \$</b> Access for authorized users only. Please enter your username and password. \$	Specifies the login message.  <i>c</i> — Enters the delimiting character of your choice, for example, a pound sign (#), and press the <b>Return</b> key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.  <i>message</i> —Enters a login message up to 255 characters. You cannot use the delimiting character in the message.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b>  <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.

	Command or Action	Purpose
<b>Step 6</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <code>copy running-config startup-config</code>	(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:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mac address-table aging-time [0 | 10-1000000] [routed-mac | vlan vlan-id]`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> Switch> <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters the global configuration mode.
<b>Step 3</b>	<code>mac address-table aging-time [0   10-1000000] [routed-mac   vlan <i>vlan-id</i>]</code>	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.

	Command or Action	Purpose
	<b>Example:</b> <pre>Switch(config)# mac address-table aging-time 500 vlan 2</pre>	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.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b>  <b>Example:</b> <pre>Switch# show running-config</pre>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>Switch# 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:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-addr community-string notification-type* { **informs** | **traps** } { **version** { **1** | **2c** | **3** } }  
 { **vrf** *vrf instance name* }
4. **snmp-server enable traps mac-notification change**
5. **mac address-table notification change**
6. **mac address-table notification change** [**interval** *value*] [**history-size** *value*]
7. **interface** *interface-id*
8. **snmp trap mac-notification change** { **added** | **removed** }
9. **end**
10. **show running-config**
11. **copy running-config startup-config**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p><b>snmp-server host</b> <i>host-addr</i> <i>community-string</i> <i>notification-type</i> { <b>informs</b>   <b>traps</b> } { <b>version</b> { <b>1</b>   <b>2c</b>   <b>3</b> } } { <b>vrf</b> <i>vrf instance name</i> }</p> <p><b>Example:</b></p> <pre>Switch(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"> <li>• <i>host-addr</i>—Specifies the name or address of the NMS.</li> <li>• <b>traps</b> (the default)—Sends SNMP traps to the host.</li> <li>• <b>informs</b>—Sends SNMP informs to the host.</li> <li>• <b>version</b>—Specifies the SNMP version to support. Version 1, the default, is not available with informs.</li> <li>• <i>community-string</i>—Specifies the string to send with the notification operation. Though you can set this string by using the <b>snmp-server host</b> command, we recommend that you define this string by using the <b>snmp-server community</b> command before using the <b>snmp-server host</b> command.</li> <li>• <i>notification-type</i>—Uses the <b>mac-notification</b> keyword.</li> <li>• <b>vrf</b> <i>vrf instance name</i>—Specifies the VPN routing/forwarding instance for this host.</li> </ul>
Step 4	<p><b>snmp-server enable traps mac-notification change</b></p> <p><b>Example:</b></p> <pre>Switch(config)# snmp-server enable traps mac-notification change</pre>	Enables the switch to send MAC address change notification traps to the NMS.
Step 5	<p><b>mac address-table notification change</b></p> <p><b>Example:</b></p> <pre>Switch(config)# mac address-table notification change</pre>	Enables the MAC address change notification feature.
Step 6	<p><b>mac address-table notification change</b> [<b>interval</b> <i>value</i>] [<b>history-size</b> <i>value</i>]</p>	Enters the trap interval time and the history table size.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch(config)# mac address-table notification change interval 123 Switch(config)# mac address-table notification change history-size 100</pre>	<ul style="list-style-type: none"> <li>• (Optional) <b>interval value</b>—Specifies the notification trap interval in seconds between each set of traps that are generated to the NMS. The range is 0 to 2147483647 seconds; the default is 1 second.</li> <li>• (Optional) <b>history-size value</b>—Specifies the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1.</li> </ul>
<b>Step 7</b>	<p><b>interface</b> <i>interface-id</i></p> <p><b>Example:</b></p> <pre>Switch(config)# interface gigabitethernet1/0/2</pre>	Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap.
<b>Step 8</b>	<p><b>snmp trap mac-notification change</b> {added   removed}</p> <p><b>Example:</b></p> <pre>Switch(config-if)# snmp trap mac-notification change added</pre>	<p>Enables the MAC address change notification trap on the interface.</p> <ul style="list-style-type: none"> <li>• Enables the trap when a MAC address is <b>added</b> on this interface.</li> <li>• Enables the trap when a MAC address is <b>removed</b> from this interface.</li> </ul>
<b>Step 9</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 10</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Switch# show running-config</pre>	Verifies your entries.
<b>Step 11</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy running-config startup-config</pre>	(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 switch to send MAC address-move notification traps to an NMS host:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-addr* {traps | informs} {version {1 | 2c | 3}} *community-string notification-type*
4. **snmp-server enable traps mac-notification move**
5. **mac address-table notification mac-move**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
<b>Step 3</b>	<p><b>snmp-server host</b> <i>host-addr</i> {traps   informs} {version {1   2c   3}} <i>community-string notification-type</i></p> <p><b>Example:</b></p> <pre>Switch(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"> <li>• <i>host-addr</i>—Specifies the name or address of the NMS.</li> <li>• <b>traps</b> (the default)—Sends SNMP traps to the host.</li> <li>• <b>informs</b>—Sends SNMP informs to the host.</li> <li>• <b>version</b>—Specifies the SNMP version to support. Version 1, the default, is not available with informs.</li> <li>• <i>community-string</i>—Specifies the string to send with the notification operation. Though you can set this string by using the <b>snmp-server host</b> command, we recommend that you define this string by using the <b>snmp-server community</b> command before using the <b>snmp-server host</b> command.</li> <li>• <i>notification-type</i>—Uses the <b>mac-notification</b> keyword.</li> </ul>

	Command or Action	Purpose
<b>Step 4</b>	<b>snmp-server enable traps mac-notification move</b>  <b>Example:</b> <pre>Switch(config)# snmp-server enable traps mac-notification move</pre>	Enables the switch to send MAC address move notification traps to the NMS.
<b>Step 5</b>	<b>mac address-table notification mac-move</b>  <b>Example:</b> <pre>Switch(config)# mac address-table notification mac-move</pre>	Enables the MAC address move notification feature.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show running-config</b>  <b>Example:</b> <pre>Switch# show running-config</pre>	Verifies your entries.
<b>Step 8</b>	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(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:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-addr* {traps | informs} {version {1 | 2c | 3}} *community-string notification-type*
4. **snmp-server enable traps mac-notification threshold**
5. **mac address-table notification threshold**
6. **mac address-table notification threshold** [*limit percentage*] | [*interval time*]
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

## DETAILED STEPS

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

	Command or Action	Purpose
Step 4	<p><b>snmp-server enable traps mac-notification threshold</b></p> <p><b>Example:</b></p> <pre>Switch(config)# snmp-server enable traps mac-notification threshold</pre>	Enables MAC threshold notification traps to the NMS.
Step 5	<p><b>mac address-table notification threshold</b></p> <p><b>Example:</b></p> <pre>Switch(config)# mac address-table notification threshold</pre>	Enables the MAC address threshold notification feature.
Step 6	<p><b>mac address-table notification threshold [limit percentage]   [interval time]</b></p> <p><b>Example:</b></p> <pre>Switch(config)# mac address-table notification threshold interval 123 Switch(config)# mac address-table notification threshold limit 78</pre>	<p>Enters the threshold value for the MAC address threshold usage monitoring.</p> <ul style="list-style-type: none"> <li>• (Optional) <b>limit percentage</b>—Specifies the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent.</li> <li>• (Optional) <b>interval time</b>—Specifies the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.</li> </ul>
Step 7	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 8	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Switch# show running-config</pre>	Verifies your entries.
Step 9	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## What to Do Next

### Adding and Removing Static Address Entries

Follow these steps to add a static address:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mac address-table static mac-addr vlan vlan-id interface interface-id`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p><code>mac address-table static mac-addr vlan vlan-id interface interface-id</code></p> <p><b>Example:</b></p> <pre>Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1</pre>	<p>Adds a static address to the MAC address table.</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> </ul>

	Command or Action	Purpose
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 5</b>	<b>show running-config</b>  <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring Unicast MAC Address Filtering

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac address-table static *mac-addr* vlan *vlan-id* drop**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.



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

## Monitoring and Maintaining Administration of the Switch

Command	Purpose
<b>clear mac address-table dynamic</b>	Removes all dynamic entries.
<b>clear mac address-table dynamic address mac-address</b>	Removes a specific MAC address.

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

# Configuration Examples for Switch Administration

## Example: Setting the System Clock

This example shows how to manually set the system clock:

```
Switch# 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:

```
Switch(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:

```
Switch(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:

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

```
Switch(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
Switch(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:

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet1/2/1
Switch(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:

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

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet1/1/1
```

## 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:

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

## Additional References for Switch Administration

### Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference (Catalyst 3650 Switches)</i>
Network management configuration	<i>Network Management Configuration Guide (Catalyst 3650 Switches)</i>
Layer 2 configuration	<i>Layer 2/3 Configuration Guide (Catalyst 3650 Switches)</i>
VLAN configuration	<i>VLAN Configuration Guide (Catalyst 3650 Switches)</i>
Platform-independent command references	<i>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>
Platform-independent configuration information	<i>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>  <i>IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>

**Standards and RFCs**

Standard/RFC	Title
None	—

**MIBs**

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information for Switch Administration

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



## CHAPTER

# 4

## Performing Switch Setup Configuration

---

- [Finding Feature Information, page 57](#)
- [Information About Performing Switch Setup Configuration, page 57](#)
- [How to Perform Switch Setup Configuration, page 70](#)
- [Monitoring Switch Setup Configuration, page 86](#)
- [Configuration Examples for Performing Switch Setup, page 89](#)
- [Additional References For Performing Switch Setup, page 91](#)
- [Feature History and Information For Performing Switch Setup Configuration, page 92](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

#### Related Topics

[Feature History and Information for Troubleshooting Software Configuration, on page 352](#)

### Information About Performing Switch Setup Configuration

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

## Switch Boot Process

To start your switch, you need to follow the procedures in the hardware installation guide for installing and powering on the switch and setting up the initial switch configuration (IP address, subnet mask, default gateway, secret and Telnet passwords, and so forth).

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 switch.

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.

The boot loader also provides trap-door access into the system if the operating system has problems serious enough that it cannot be used. The trap-door mechanism provides enough access to the system so that if it is necessary, you can reinstall the operating system software image by using the Xmodem Protocol, recover from a lost or forgotten password, and finally restart the operating system.

Before you can assign switch 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 switch 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.

## Software Installer Features

The following software installer features are supported on your switch:

- Software bundle installation on a standalone switch, a switch stack, or a subset of switches in a stack. The default is installation on all the switches if a switch stack is configured.
- Software rollback to a previously installed package set.
- Emergency installation in the event that no valid installed packages reside on the boot flash.
- Auto-upgrade of a switch that joins the switch stack with incompatible software.



- Installation using packages on one switch as the source for installing packages on another switch in the switch stack.



---

**Note**

---

## Software Boot Modes

Your switch supports two modes to boot the software packages:

- Installed mode
- Bundle mode

### Related Topics

[Examples: Displaying Software Bootup in Install Mode, on page 86](#)

[Example: Emergency Installation, on page 88](#)

## Installed Boot Mode

You can boot your switch in installed mode by booting the software package provisioning file that resides in flash:

```
Switch: boot flash:packages.conf
```

The provisioning file contains a list of software packages to boot, mount, and run. The ISO file system in each installed package is mounted to the root file system directly from flash.



---

**Note**

---

The packages and provisioning file used to boot in installed mode must reside in flash. Booting in installed mode from usbflash0: or tftp: is not supported.

---

### Related Topics

[Examples: Displaying Software Bootup in Install Mode, on page 86](#)

[Example: Emergency Installation, on page 88](#)

## Bundle Boot Mode

You can boot your switch in bundle boot mode by booting the bundle (.bin) file:

```
switch: boot flash:cat3850-universalk9.SSA.03.08.83.EMD.150-8.83.EMD.bin
```

The provisioning file contained in a bundle is used to decide which packages to boot, mount, and run. Packages are extracted from the bundle and copied to RAM. The ISO file system in each package is mounted to the root file system.

Unlike install boot mode, additional memory that is equivalent to the size of the bundle is used when booting in bundle mode.

Unlike install boot mode, bundle boot mode is available from several locations:

- flash:
- usbflash0:
- tftp:




---

**Note** Auto install and smart install functionality is not supported in bundle boot mode.

---




---

**Note** The AP image pre-download feature is not supported in bundle boot mode. For more information about the pre-download feature see the Cisco WLC 5700 Series *Preloading an Image to Access Points* chapter.

---

### Related Topics

[Examples: Displaying Software Bootup in Install Mode, on page 86](#)

[Example: Emergency Installation, on page 88](#)

## Boot Mode for a Switch Stack

All the switches in a stack must be running in installed mode or bundle boot mode. A mixed mode stack is not supported. If a new switch tries to join the stack in a different boot mode than the active switch, the new switch is given a V-mismatch state.

If a mixed mode switch stack is booted at the same time, then only those switches that boot up in a different mode than the active go to the V-mismatch state. If the boot mode does not support auto-upgrade, then the switch stack members must be re-booted in the same boot mode as the active switch.

If the stack is running in installed mode, the auto-upgrade feature can be used to automatically upgrade the new switch that is attempting to join the switch stack.

The auto-upgrade feature changes the boot mode of the new switch to installed mode. If the stack is running in bundle boot mode, the auto-upgrade feature is not available. You will be required to use the bundle mode to boot the new switch so that it can join the switch stack.

This is an example of the state of a switch that attempts to join the switch stack when the boot mode is not compatible with the active switch:

```
Switch# show switch

Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch#   Role   Mac Address      Priority Version   State
-----
  1       Member 6400 f125.1a00   1         0         V-Mismatch
 *2       Active 6400.f125.1100  1         V01       Ready
Switch
```

## Switches Information Assignment

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

Use the switch 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 switch receives the dynamically assigned IP address and reads the configuration file.

If you are an experienced user familiar with the switch configuration steps, manually configure the switch. Otherwise, use the setup program described in the *Boot Process* section.

## Default Switch Information

**Table 7: 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 Switch.
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 switch can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your switch (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 switch. 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 switch can be on the same LAN or on a different LAN than the switch. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your switch 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 switch.

## DHCP Client Request Process

When you boot up your switch, the DHCP client is invoked and requests configuration information from a DHCP server when the configuration file is not present on the switch. 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, Switch 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 switch 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 DHCP DECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCP NAK 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 switch accepts replies from a BOOTP server and configures itself, the switch broadcasts, instead of unicasts, TFTP requests to obtain the switch configuration file.

The DHCP hostname option allows a group of switches to obtain hostnames and a standard configuration from the central management DHCP server. A client (switch) includes in its DHCP DISCOVER 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.

If a client has a default hostname (the `hostname name` global configuration command is not configured or the `no hostname` global configuration command is entered to remove the hostname), the DHCP hostname option is not included in the packet when you enter the `ip address dhcp` interface configuration command. In this case, if the client receives the DHCP hostname option from the DHCP interaction while acquiring an IP address for an interface, the client accepts the DHCP hostname option and sets the flag to show that the system now has a hostname configured.

## 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 switches in a network. Simultaneous image and configuration upgrade for all switches in the network helps ensure that each new switch 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 switches in your network from a DHCP server. The downloaded configuration file becomes the running configuration of the switch. It does not over write the bootstrap configuration saved in the flash, until you reload the switch.

## 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 switches in your network. The switch (or switches) 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 switch, 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 switch in your network, the auto-image update feature starts. The downloaded configuration file is saved in the running configuration of the switch, and the new image is downloaded and installed on the switch. When you reboot the switch, the configuration is stored in the saved configuration on the switch.

## 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 switch by the switch hardware address.
- If you want the switch 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 switch) (required)
- If you want the switch 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 switch 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 switch is not configured. If the router IP address or the TFTP server name are not found, the switch might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.
- The switch can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your switch but are not configured. (These features are not operational.)

## Purpose of the TFTP Server

Based on the DHCP server configuration, the switch attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the switch 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 switch 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 switch 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 switch'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 switch 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 switch 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 switches. 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 switch, or if it is to be accessed by the switch 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 switch.

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 switch. If it is on a different LAN, the switch 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 switch obtains its configuration information in these ways:

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

The switch receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. The switch 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 switch, but the TFTP server address is not provided in the DHCP reply (one-file read method).

The switch receives its IP address, subnet mask, and the configuration filename from the DHCP server. The switch 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 switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

The switch receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The switch 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 switch reads the cisco.net.cfg file.)

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

After obtaining its hostname from the default configuration file or the DHCP reply, the switch 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 switch cannot read the network-config, cisco.net.cfg, or the hostname file, it reads the router-config file. If the switch cannot read the router-config file, it reads the ciscotr.cfg file.



### Note

The switch 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 switch, you enter the boot loader mode only through the console connection configured for 9600 bps. Unplug the switch power cord, and press the **Mode** button while reconnecting the power cord. You can release the **Mode** button after all the amber system LEDs turn on and remain solid. The boot loader switch prompt then appears.



The switch 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 8: Common Environment Variables**

Variable	Boot Loader Command	Cisco IOS Global Configuration Command
BOOT	<p><b>set BOOT</b> <i>filesystem :/file-url ...</i></p> <p>A semicolon-separated list of executable files to try to load and execute when automatically booting.</p>	<p><b>boot system</b> <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"> <li>• When booting in installed mode, the package provisioning file specified in the <b>boot</b> command is used to determine which packages to activate. For example <b>boot flash:packages.conf</b>.</li> <li>• 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, <b>boot flash:image.bin</b>.</li> </ul>

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

## 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 9: Environment Variables for TFTP**

Variable	Description
MAC_ADDR	Specifies the MAC address of the switch.  <b>Note</b> 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_ROUTER	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 switch at a later time (for example, late at night or during the weekend when the switch is used less), or you can synchronize a reload network-wide (for example, to perform a software upgrade on all switches 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 switch is configured for manual booting, do not reload it from a virtual terminal. This restriction prevents the switch from entering the boot loader mode and then taking it from the remote user's control.

If you modify your configuration file, the switch 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 Switch Setup Configuration

Using DHCP to download a new image and a new configuration to a switch requires that you configure at least two switches. One switch acts as a DHCP and TFTP server and the second switch (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 switch in the network so that it can support the autoconfiguration of a new switch.

#### SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp pool** *poolname*
3. **boot** *filename*
4. **network** *network-number mask prefix-length*
5. **default-router** *address*
6. **option 150** *address*
7. **exit**
8. **tftp-server flash:***filename.text*
9. **interface** *interface-id*
10. **no switchport**
11. **ip address** *address mask*
12. **end**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<p><b>ip dhcp pool</b> <i>poolname</i></p> <p><b>Example:</b></p> <pre>Switch(config)# ip dhcp pool pool</pre>	Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.
<b>Step 3</b>	<p><b>boot</b> <i>filename</i></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# boot config-boot.text</pre>	Specifies the name of the configuration file that is used as a boot image.
<b>Step 4</b>	<p><b>network</b> <i>network-number mask prefix-length</i></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# network 10.10.10.0 255.255.255.0</pre>	<p>Specifies the subnet network number and mask of the DHCP address pool.</p> <p><b>Note</b> 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 (/).</p>
<b>Step 5</b>	<p><b>default-router</b> <i>address</i></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# default-router 10.10.10.1</pre>	Specifies the IP address of the default router for a DHCP client.
<b>Step 6</b>	<p><b>option 150</b> <i>address</i></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# option 150 10.10.10.1</pre>	Specifies the IP address of the TFTP server.
<b>Step 7</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# exit</pre>	Returns to global configuration mode.
<b>Step 8</b>	<p><b>tftp-server flash:</b><i>filename.text</i></p> <p><b>Example:</b></p> <pre>Switch(config)# tftp-server flash:config-boot.text</pre>	Specifies the configuration file on the TFTP server.

	Command or Action	Purpose
<b>Step 9</b>	<b>interface</b> <i>interface-id</i>  <b>Example:</b> Switch(config)# <b>interface</b> gigabitethernet1/0/4	Specifies the address of the client that will receive the configuration file.
<b>Step 10</b>	<b>no switchport</b>  <b>Example:</b> Switch(config-if)# <b>no switchport</b>	Puts the interface into Layer 3 mode.
<b>Step 11</b>	<b>ip address</b> <i>address mask</i>  <b>Example:</b> Switch(config-if)# <b>ip address</b> 10.10.10.1 255.255.255.0	Specifies the IP address and mask for the interface.
<b>Step 12</b>	<b>end</b>  <b>Example:</b> Switch(config-if)# <b>end</b>	Returns to privileged EXEC mode.

### Related Topics

[Example: Configuring a Switch as a DHCP Server, on page 89](#)

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

This task describes DHCP autoconfiguration to configure TFTP and DHCP settings on an existing switch 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 switch. In the text file, put the name of the image that you want to download (forexample, `c3750e-ipservices-mz.122-44.3.SE.tar``c3750x-ipservices-mz.122-53.3.SE2.tar`). This image must be a tar and not a bin file.

## SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp pool** *poolname*
3. **boot** *filename*
4. **network** *network-number mask prefix-length*
5. **default-router** *address*
6. **option 150** *address*
7. **option 125** *hex*
8. **copy tftp flash** *filename.txt*
9. **copy tftp flash** *imagename.bin*
10. **exit**
11. **tftp-server flash:** *config.txt*
12. **tftp-server flash:** *imagename.bin*
13. **tftp-server flash:** *filename.txt*
14. **interface** *interface-id*
15. **no switchport**
16. **ip address** *address mask*
17. **end**
18. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>ip dhcp pool</b> <i>poolname</i>  <b>Example:</b> Switch(config)# <b>ip dhcp pool pool1</b>	Creates a name for the DHCP server address pool and enter DHCP pool configuration mode.
<b>Step 3</b>	<b>boot</b> <i>filename</i>  <b>Example:</b> Switch(dhcp-config)# <b>boot config-boot.txt</b>	Specifies the name of the file that is used as a boot image.

	Command or Action	Purpose
<b>Step 4</b>	<p><b>network</b> <i>network-number mask prefix-length</i></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# network 10.10.10.0 255.255.255.0</pre>	<p>Specifies the subnet network number and mask of the DHCP address pool.</p> <p><b>Note</b> 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 (/).</p>
<b>Step 5</b>	<p><b>default-router</b> <i>address</i></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# default-router 10.10.10.1</pre>	Specifies the IP address of the default router for a DHCP client.
<b>Step 6</b>	<p><b>option 150</b> <i>address</i></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# option 150 10.10.10.1</pre>	Specifies the IP address of the TFTP server.
<b>Step 7</b>	<p><b>option 125</b> <i>hex</i></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# option 125 hex 0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370</pre>	Specifies the path to the text file that describes the path to the image file.
<b>Step 8</b>	<p><b>copy tftp flash</b> <i>filename.txt</i></p> <p><b>Example:</b></p> <pre>Switch(config)# copy tftp flash image.bin</pre>	Uploads the text file to the switch.
<b>Step 9</b>	<p><b>copy tftp flash</b> <i>imagenamename.bin</i></p> <p><b>Example:</b></p> <pre>Switch(config)# copy tftp flash image.bin</pre>	Uploads the tar file for the new image to the switch.
<b>Step 10</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Switch(dhcp-config)# exit</pre>	Returns to global configuration mode.



	Command or Action	Purpose
<b>Step 11</b>	<b>tftp-server flash:</b> <i>config.text</i>  <b>Example:</b> Switch(config)# <b>tftp-server flash:config-boot.text</b>	Specifies the Cisco IOS configuration file on the TFTP server.
<b>Step 12</b>	<b>tftp-server flash:</b> <i>imagename.bin</i>  <b>Example:</b> Switch(config)# <b>tftp-server flash:image.bin</b>	Specifies the image name on the TFTP server.
<b>Step 13</b>	<b>tftp-server flash:</b> <i>filename.txt</i>  <b>Example:</b> Switch(config)# <b>tftp-server flash:boot-config.text</b>	Specifies the text file that contains the name of the image file to download
<b>Step 14</b>	<b>interface</b> <i>interface-id</i>  <b>Example:</b> Switch(config)# <b>interface gigabitEthernet1/0/4</b>	Specifies the address of the client that will receive the configuration file.
<b>Step 15</b>	<b>no switchport</b>  <b>Example:</b> Switch(config-if)# <b>no switchport</b>	Puts the interface into Layer 3 mode.
<b>Step 16</b>	<b>ip address</b> <i>address mask</i>  <b>Example:</b> Switch(config-if)# <b>ip address 10.10.10.1 255.255.255.0</b>	Specifies the IP address and mask for the interface.
<b>Step 17</b>	<b>end</b>  <b>Example:</b> Switch(config-if)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 18</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch(config-if)# <b>end</b>	(Optional) Saves your entries in the configuration file.

**Related Topics**

[Example: Configuring DHCP Auto-Image Update, on page 90](#)

**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.

**SUMMARY STEPS**

1. **configure terminal**
2. **boot host dhcp**
3. **boot host retry timeout** *timeout-value*
4. **banner config-save** ^C *warning-message* ^C
5. **end**
6. **show boot**

**DETAILED STEPS**

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

	Command or Action	Purpose
	Download Configuration Files at Reboot^C	
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Switch(config-if) # <b>end</b>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show boot</b>  <b>Example:</b> Switch# <b>show boot</b>	Verifies the configuration.

### Related Topics

[Example: Configuring a Switch to Download Configurations from a DHCP Server, on page 90](#)

## Manually Assigning IP Information to Multiple SVIs

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface vlan** *vlan-id*
3. **ip address** *ip-address subnet-mask*
4. **exit**
5. **ip default-gateway** *ip-address*
6. **end**
7. **show interfaces vlan** *vlan-id*
8. **show ip redirects**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>interface vlan</b> <i>vlan-id</i>  <b>Example:</b> Switch(config)# <b>interface vlan 99</b>	Enters interface configuration mode, and enters the VLAN to which the IP information is assigned. The range is 1 to 4094.
<b>Step 3</b>	<b>ip address</b> <i>ip-address subnet-mask</i>  <b>Example:</b> Switch(config-vlan)# <b>ip address 10.10.10.2 255.255.255.0</b>	Enters the IP address and subnet mask.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> Switch(config-vlan)# <b>exit</b>	Returns to global configuration mode.
<b>Step 5</b>	<b>ip default-gateway</b> <i>ip-address</i>  <b>Example:</b> Switch(config)# <b>ip default-gateway 10.10.10.1</b>	<p>Enters the IP address of the next-hop router interface that is directly connected to the switch where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch.</p> <p>Once the default gateway is configured, the switch has connectivity to the remote networks with which a host needs to communicate.</p> <p><b>Note</b> When your switch is configured to route with IP, it does not need to have a default gateway set.</p> <p><b>Note</b> The switch capwap relays on default-gateway configuration to support routed access point join the switch.</p>
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show interfaces vlan</b> <i>vlan-id</i>  <b>Example:</b> Switch# <b>show interfaces vlan 99</b>	Verifies the configured IP address.
<b>Step 8</b>	<b>show ip redirects</b>  <b>Example:</b> Switch# <b>show ip redirects</b>	Verifies the configured default gateway.

# Modifying the Switch 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 switch for this task.

### SUMMARY STEPS

1. `configure terminal`
2. `boot flash:/file-url`
3. `end`
4. `show boot`
5. `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
Step 2	<b>boot flash:/file-url</b>  <b>Example:</b> Switch(config)# <code>boot flash:config.text</code>	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	<b>end</b>  <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode.
Step 4	<b>show boot</b>  <b>Example:</b> Switch# <code>show boot</code>	Verifies your entries.  The <code>boot</code> global configuration command changes the setting of the <code>CONFIG_FILE</code> environment variable.

	Command or Action	Purpose
<b>Step 5</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <code>copy running-config startup-config</code>	(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.

### SUMMARY STEPS

1. `configure terminal`
2. `boot manual`
3. `end`
4. `show boot`
5. `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>boot manual</b>  <b>Example:</b> Switch(config)# <code>boot manual</code>	Enables the switch to manually boot up during the next boot cycle.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 4</b>	<b>show boot</b>	Verifies your entries.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch# show boot</pre>	<p>The <b>boot manual</b> global command changes the setting of the MANUAL_BOOT environment variable.</p> <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 <b>boot filesystem:/file-url</b> boot loader command.</p> <ul style="list-style-type: none"> <li>• <i>filesystem:</i>—Uses flash: for the system board flash device. Switch: <b>boot flash:</b></li> <li>• For <i>file-url</i>—Specifies the path (directory) and the name of the bootable image.</li> </ul> <p>Filenames and directory names are case-sensitive.</p>
<b>Step 5</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Booting the Switch in Installed Mode

### SUMMARY STEPS

1. **cp source\_file\_path destination\_file\_path**
- 2.
3. **reload**
4. **boot flash:packages.conf**
5. **show version**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<p><b>cp source_file_path destination_file_path</b></p> <p><b>Example:</b></p> <pre>Switch# copy tftp://10.0.0.6/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:</pre>	(Optional) Copies the bin file (image.bin) from the FTP or TFTP server to USB flash.
<b>Step 2</b>	<p><b>Example:</b></p>	Expands the bin file stored in flash, FTP,

	Command or Action	Purpose
	Expanding the bin file from the TFTP server: <pre>Switch# request platform software package expand switch all file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to flash: Preparing expand operation ... [1]: Downloading file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1 [1]: Finished downloading file tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1 [1]: Copying software from active switch 1 to switch 2 [1]: Finished copying software to switch 2 [1 2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin [1 2]: Copying package files [1 2]: Package files copied [1 2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin  18 -rw- 74387812 Dec 7 2012 05:55:43 +00:00 cat3k_caa-base.SSA.03.09.37.EXP.pkg  19 -rw- 2738868 Dec 7 2012 05:55:44 +00:00 cat3k_caa-drivers.SSA.03.09.37.EXP.pkg 20 -rw- 32465772 Dec 7 2012 05:55:44 +00:00 cat3k_caa-infra.SSA.03.09.37.EXP.pkg 21 -rw- 30389036 Dec 7 2012 05:55:44 +00:00 cat3k_caa-iosd-universalk9.SSA.150-9.37.EXP.pkg 22 -rw- 18342624 Dec 7 2012 05:55:44 +00:00 cat3k_caa-platform.SSA.03.09.37.EXP.pkg 23 -rw- 63374028 Dec 7 2012 05:55:44 +00:00 cat3k_caa-wcm.SSA.10.0.10.14.pkg  17 -rw- 1239 Dec 7 2012 05:56:29 +00:00 packages.conf</pre>	TFTP, HTTP, or HTTPS server on the booted switch. <b>Note</b> Ensure that the <code>packages.conf</code> file is available in the expanded list.
<b>Step 3</b>	<b>reload</b>  <b>Example:</b> <pre>Switch# reload</pre>	Reloads the switch.  <b>Note</b> You can boot the switch manually or automatically using the <code>packages.conf</code> file. If you are booting manually, you can proceed to Step 4. Otherwise, the switch boots up automatically.
<b>Step 4</b>	<b>boot flash:packages.conf</b>  <b>Example:</b> <pre>Switch: boot flash:packages.conf</pre>	Boots the switch with the <code>packages.conf</code> file.
<b>Step 5</b>	<b>show version</b>  <b>Example:</b>	Verifies that the switch is in the <b>INSTALL</b> mode.



## Booting the Switch in Bundle Mode

There are several methods by which you can boot the switch—either by copying the bin file from the TFTP server and then boot the switch, or by booting the switch straight from flash or USB flash using the commands **boot flash:<image.bin>** or **boot usbflash0:<image.bin>**.

The following procedure explains how to boot the switch from the TFTP server in the bundle mode.

### SUMMARY STEPS

1. **switch:BOOT=<source path of .bin file>**
2. **boot**
3. **show version**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>switch:BOOT=&lt;source path of .bin file&gt;</b>  <b>Example:</b> switch:BOOT=tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin	Sets the boot parameters.
Step 2	<b>boot</b>  <b>Example:</b> switch: boot	Boots the switch.
Step 3	<b>show version</b>  <b>Example:</b> switch# show version	Verifies that the switch is in the <b>BUNDLE</b> mode.

## Booting a Specific Software Image On a Switch Stack

By default, the switch attempts to automatically boot up the system using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. However, you can specify a specific image to boot up.

## SUMMARY STEPS

1. **configure terminal**
2. **boot system switch** {*number* | **all**}
3. **end**
4. **show boot system**
5. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>boot system switch</b> { <i>number</i>   <b>all</b> }	(Optional) For switches in a stack, specifies the switch members on which the system image is loaded during the next boot cycle: <ul style="list-style-type: none"> <li>• Use <i>number</i> to specify a stack member. (Specify only one stack member.)</li> <li>• Use <b>all</b> to specify all stack members.</li> </ul>
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 4</b>	<b>show boot system</b>  <b>Example:</b> Switch# <b>show boot system</b>	Verifies your entries.  The <b>boot system</b> global command changes the setting of the BOOT environment variable.  During the next boot cycle, the switch attempts to automatically boot up the system using information in the BOOT environment variable.
<b>Step 5</b>	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring a Scheduled Software Image Reload

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

### SUMMARY STEPS

1. **configure terminal**
2. **copy running-config startup-config**
3. **reload in** *[hh:]mm* *[text]*
4. **reload at** *hh: mm* *[month day | day month]* *[text]*
5. **reload cancel**
6. **show reload**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>copy running-config startup-config</b>  <b>Example:</b> copy running-config startup-config	Saves your switch configuration information to the startup configuration before you use the <b>reload</b> command.
<b>Step 3</b>	<b>reload in</b> <i>[hh:]mm</i> <i>[text]</i>  <b>Example:</b> Switch(config)# <b>reload in 12</b>  System configuration has been modified. Save? [yes/no]: <b>y</b>	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.
<b>Step 4</b>	<b>reload at</b> <i>hh: mm</i> <i>[month day   day month]</i> <i>[text]</i>  <b>Example:</b> Switch(config)# <b>reload at 14:00</b>	Specifies the time in hours and minutes for the reload to occur.  <b>Note</b> Use the <b>at</b> keyword only if the switch 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 switch. To schedule reloads across several switches to occur simultaneously, the time on each switch must be synchronized with NTP.
<b>Step 5</b>	<b>reload cancel</b>  <b>Example:</b> Switch(config)# <b>reload cancel</b>	Cancels a previously scheduled reload.

	Command or Action	Purpose
Step 6	<b>show reload</b>  <b>Example:</b> <b>show reload</b>	Displays information about a previously scheduled reload or identifies if a reload has been scheduled on the switch.

## Monitoring Switch Setup Configuration

### Example: Verifying the Switch Running Configuration

```

Switch# show running-config
Building configuration...

Current configuration: 1363 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Stack1
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxEO
!
.<output truncated>
.
interface gigabitethernet6/0/2
mvr type source

<output truncated>

...!
interface VLAN1
 ip address 172.20.137.50 255.255.255.0
 no ip directed-broadcast
!
 ip default-gateway 172.20.137.1 !
!
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12
!
end

```

### Examples: Displaying Software Bootup in Install Mode

This example displays software bootup in install mode:  
switch: **boot flash:packages.conf**



```

Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x900000000].
#####
File "flash:cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin" uncompressed and
installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services
Nov 7 09:45:49 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2 is
starting stack discovery
#####
Nov 7 09:47:50 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has
finished stack discovery
Nov 7 09:47:50 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2 has
been added to the stack
Nov 7 09:47:58 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch 2
has been elected ACTIVE

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 03.09.12.EMD
EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 04-Nov-12 22:53 by gereddy
License level to iosd is ipservices

```

### Related Topics

[Software Boot Modes, on page 59](#)

[Installed Boot Mode, on page 59](#)

[Bundle Boot Mode, on page 59](#)

## Example: Emergency Installation

This sample output is an example when the **emergency-install** boot command is initiated:

```

switch: emergency-install
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin

The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin) ...
Reading full image into memory.....done
Nova Bundle Image
-----

```



```
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

**Related Topics**

[Configuring DHCP Autoconfiguration \(Only Configuration File\), on page 70](#)

## Example: Configuring DHCP Auto-Image Update

**Related Topics**

[Configuring DHCP Auto-Image Update \(Configuration File and Image\), on page 72](#)

## Example: Configuring a Switch 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:

```
Switch# configure terminal
Switch(config)# boot host dhcp
Switch(config)# boot host retry timeout 300
Switch(config)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause
  You to No longer Automatically Download Configuration Files at Reboot^C
Switch(config)# vlan 99
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# 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)
Switch#
```

**Related Topics**

[Configuring the Client to Download Files from DHCP Server, on page 76](#)

## Examples: Scheduling Software Image Reload

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

```
Switch# 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 switch at a future time:

```
Switch# 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 Switch Setup

### Related Documents

Related Topic	Document Title
Switch setup commands Boot loader commands	<i>System Management Command Reference (Catalyst 3650 Switches)</i>
Pre-download feature	<i>System Management Configuration Guide (Cisco WLC 5700 Series)</i>
IOS XE DHCP configuration	<i>IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>
Hardware installation	<i>Catalyst 3650 Switch Hardware Installation Guide</i>
Platform-independent command references	<i>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>
Platform-independent configuration information	<i>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>  <i>IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

**MIBs**

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information For Performing Switch Setup Configuration

**Command History**

Release	Modification
Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE	This feature was introduced.



## Configuring Right-To-Use Licenses

---

- [Finding Feature Information, page 93](#)
- [Restrictions for Configuring RTU Licenses, page 93](#)
- [Information About Configuring RTU Licenses, page 94](#)
- [How to Configure RTU Licenses, page 97](#)
- [Monitoring and Maintaining RTU Licenses, page 103](#)
- [Configuration Examples for RTU Licensing, page 103](#)
- [Additional References for RTU Licensing, page 107](#)
- [Feature History and Information for RTU Licensing, page 108](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

#### Related Topics

[Feature History and Information for Troubleshooting Software Configuration, on page 352](#)

### Restrictions for Configuring RTU Licenses

The following are the restrictions for configuring and using RTU licenses.

- AP count licenses can be ordered and pre-activated on your switch.

- Imaged based licenses can be upgraded. AP count licenses can be deactivated and moved between switches and controllers.
- To activate a license, you must reboot your switch after configuring the new license level. The AP-count license does not require a reboot to activate.
- An expired evaluation license can not be reactivated after reboot.
- Stack members of a switch stack must run the same license level. If the license level is different, the switch will not join the stack until it is changed and rebooted from the active switch of the stack.
- Licenses on mixed switch stacks are not supported.
- Adder AP-count licenses are installed in the factory.

#### Related Topics

[Activating an Image Based License](#), on page 97

[Examples: Activating RTU Image Based Licenses](#), on page 103

## Information About Configuring RTU Licenses

### Right-To-Use Licensing

Right-to-use (RTU) licensing allows you to order and activate a specific license type and level, and then to manage license usage on your switch. The types of licenses available to order by duration are:

- Permanent licenses—Purchased with a specific feature set with no expiration date.
- Evaluation licenses—Pre-installed on the switch and is valid for only a 90 day in-use period.

To activate a permanent or evaluation license, you are required to accept the End-User License Agreement (EULA).

A permanent license can be moved from one device to another. To activate a license, you must reboot your switch.

If you activate the evaluation license, it will expire in 90 days. An evaluation license is a manufacturing image on your switch and is not transferable to another switch. Once activated, this type of license cannot be deactivated until it expires. After your evaluation period expires, at the next reload your switch image will return to its default license and network operations are not impacted.

#### Related Topics

[Activating an Image Based License](#), on page 97

[Examples: Activating RTU Image Based Licenses](#), on page 103

### Right-To-Use Image-Based Licenses

Right-to-use image licenses support a set of features based on a specific image-based license:

- LAN Base—Layer 2 features.

- IP Base—Layer 2 and Layer 3 features.
- IP Services—Layer 2, Layer 3, and IPv6 features. (Applicable only to switches and not controllers.)

## Right-To-Use License States

After you configure a specific license type and level, you can manage your licenses by monitoring the license state.

**Table 10: RTU License States**

License State	Description
Active, In Use	EULA was accepted and the license is in use after device reboot.
Active, Not In Use	EULA was accepted and the switch is ready to use when the license is enabled.
Not Activated	EULA was not accepted.

Guidelines to follow when monitoring your image based license state:

- A purchased permanent license is set to *Active, In Use* state only after a switch reboot.
- If more than one license was purchased, a reboot will activate the license with the highest feature set. For instance, the IP Services license is activated and not the LAN Base license.
- Remaining licenses purchased after switch reboot, stay in **Active, Not In Use** state.



**Note** For the AP count license, to change the state to Active, In Use, you must first make sure that the evaluation AP count license is deactivated.

## License Activation for Switch Stacks

Right-to-use licensing is supported on switch stacks. A switch is a set of up to nine stacking-capable switches connected through their StackWise-160 ports. One switch in the stack is identified as the active switch and the remaining switches are standby switches. The active switch is activated with an RTU license from its active console. The license level for the standby switches in the stack can be activated at the same time.



**Note** A switch stack cannot contain mixed license levels. Also, the switches must be of the same platform.

To change the license level, you do not need to disconnected the new added stack member if the stack cables are connected. Use the active switch console to set the new member's license level same as active switch and reboot the new member to join the stack.

## Mobility Controller Mode

AP-count licenses are used only when the switch is in Mobility Controller mode. The MC is the gatekeeper for tracking the AP-count licenses and allows an access point to join or not.

Management of AP-count licenses is performed by the switch in mobility controller mode configurable through the CLI.

### Related Topics

[Changing Mobility Mode, on page 101](#)

## Right-To-Use AP-Count Licensing

Right-to-use licensing (RTU) allows you to order and activate a specific license type, and then to manage license usage on your switch.

You can order your switch with support for a specific number of adder access point count licenses, but the total number of licenses ordered should not exceed 25. You can also order your adder access point count licenses after receiving the switch.

For example, if you have ordered 25 new adder licenses, you can add only those ordered adder licenses to the switch. The licenses can be added in increments of 1, but the total number of licenses added for the switch should not exceed 25 .

You can configure your switch to manage the access point count licenses and view the number of access points currently in use from the CLI.

The following are two different types of access point licenses:

- 1 Permanent licenses for the access points
  - Adder access point count license—You can purchase the adder license to increase the switch capacity at a later time. You can transfer the adder access point count license from one switch to another.
- 2 Evaluation licenses for the access points
  - You can activate these licenses to evaluate more access points before purchasing the licenses.
  - The maximum number of access points that can be evaluated is 25 .
  - The evaluation period for using the access point licenses is 90 days.
  - You can activate and deactivate the evaluation licenses from the CLI.

### Related Topics

[Activating an AP-Count License, on page 99](#)

[Obtaining an Upgrade or Capacity Adder License, on page 100](#)

[Rehosting a License, on page 100](#)

## Right-to-Use AP-Count Evaluation Licenses

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 10 access-point count and want to try an evaluation license with a 15-access-point count, you can try out the evaluation license for 90 days.

When an evaluation license is activated, the permanent AP-count licenses are ignored. The maximum supported licenses of 25 access points are available for 90 days.

To prevent disruptions in operation, the switch does not change licenses when an evaluation license expires. A warning expiry message is displayed daily starting five days prior to the expiry date. After 90 days, the evaluation license expires with a warning message. You must disable the evaluation license and then purchase the permanent license.

When the switch reboots after the evaluation license expiry, the license defaults to a permanent license.

### Related Topics

[Activating an AP-Count License, on page 99](#)

[Obtaining an Upgrade or Capacity Adder License, on page 100](#)

[Rehosting a License, on page 100](#)

## Right-To-Use Adder AP-Count Rehosting Licenses

Revoking a license from one device and installing it on another is called rehosting. You might want to rehost a license to change the purpose of a device.

To rehost a license, you must deactivate the adder ap-count license from one device and activate the same license on another device.

Evaluation licenses cannot be rehosted.

## How to Configure RTU Licenses

### Activating an Image Based License

#### SUMMARY STEPS

1. `license right-to-use activate`{ipbase | ipservices | lanbase} {all | evaluation all} [slot *slot-number*] [acceptEULA]
2. `reload` [ *LINE* | at | cancel | in | slot *stack-member-number* | standby-cpu ]
3. `show license right-to-use usage` [ slot *slot-number* ]

## DETAILED STEPS

	Command or Action	Purpose																								
<b>Step 1</b>	<p><b>license right-to-use activate</b> {ipbase   ipservices   lanbase} {all   evaluation all } [slot slot-number] [ acceptEULA]</p> <p><b>Example:</b></p> <pre>Switch# license right-to-use activate ipservices all acceptEULA</pre>	<p>Activates the license level. Activation can happen on all switches and also include the EULA acceptance.</p> <p><b>Note</b> If you do not accept EULA, the modified configuration will not take effect after reload. The default license (or a license that was not deactivated) becomes active after reload.</p>																								
<b>Step 2</b>	<p><b>reload</b> [ LINE   at   cancel   in   slot stack-member-number   standby-cpu ]</p> <p><b>Example:</b></p> <pre>Switch# reload slot 1 Proceed with reload? [confirm] y</pre>	<p>Reloads a specific stack member to complete the activation process for the RTU adder AP-count license.</p> <p><b>Note</b> The reminder to accept the EULA is displayed after reload if it was not accepted earlier.</p> <p>When changing license level, you are not required to save the configuration. But, it is a good practice to ensure all the configuration is stored properly before reload. Changing from a higher license level to a lower license level on reboot will remove CLIs that are not applicable. Ensure that all features in the lower license level that are actively used are not removed.</p>																								
<b>Step 3</b>	<p><b>show license right-to-use usage</b> [ slot slot-number ]</p> <p><b>Example:</b></p> <pre>Switch# show license right-to-use usage</pre> <table border="1"> <thead> <tr> <th>Slot#</th> <th>License Name</th> <th>Type</th> <th>usage-duration(y:m:d)</th> <th>In-Use</th> <th>EULA</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ipservices</td> <td>Permanent</td> <td>0 :10:27</td> <td>yes</td> <td>yes</td> </tr> <tr> <td>1</td> <td>ipservices</td> <td>Evaluation</td> <td>0 :0 :0</td> <td>no</td> <td>no</td> </tr> <tr> <td>1</td> <td>ibase</td> <td>Permanent</td> <td>0 :0 :9</td> <td>no</td> <td>yes</td> </tr> </tbody> </table>	Slot#	License Name	Type	usage-duration(y:m:d)	In-Use	EULA	1	ipservices	Permanent	0 :10:27	yes	yes	1	ipservices	Evaluation	0 :0 :0	no	no	1	ibase	Permanent	0 :0 :9	no	yes	<p>Displays detailed usage information.</p>
Slot#	License Name	Type	usage-duration(y:m:d)	In-Use	EULA																					
1	ipservices	Permanent	0 :10:27	yes	yes																					
1	ipservices	Evaluation	0 :0 :0	no	no																					
1	ibase	Permanent	0 :0 :9	no	yes																					



Command or Action	Purpose
<pre> 1          ipbase  Evaluation          0 :0 :0          no          no 1          lanbase  Permanent          0 :11:12         no          yes ----- Switch#                     </pre>	

**Related Topics**

- [Restrictions for Configuring RTU Licenses, on page 93](#)
- [Right-To-Use Licensing, on page 94](#)
- [Monitoring and Maintaining RTU Licenses, on page 103](#)
- [Examples: Activating RTU Image Based Licenses, on page 103](#)

## Activating an AP-Count License

**SUMMARY STEPS**

1. `license right-to-use activate{apcount ap-number slot slot-num} | evaluation} [ acceptEULA]`
2. `show license right-to-use usage [ slot slot-number ]`

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<p><code>license right-to-use activate{apcount <i>ap-number</i> slot <i>slot-num</i>}   evaluation} [ acceptEULA]</code></p> <p><b>Example:</b>  Switch# <code>license right to use activate apcount 5 slot 1 acceptEULA</code></p>	Activates one or more adder AP-count licenses and immediately accepts the EULA.
<b>Step 2</b>	<p><code>show license right-to-use usage [ slot <i>slot-number</i> ]</code></p> <p><b>Example:</b>  Switch# <code>show license right-to-use usage</code></p> <pre> Slot#  License Name      Type      usage-duration(y:m:d)  In-Use  EULA ----- 1      ipservices            permanent  0 :3 :29                yes     yes 1      ipservices            evaluation 0 :0 :0                  no      no 1      ipbase                 permanent  0 :0 :0                  no      no 1      ipbase                 evaluation 0 :0 :0                  no      no 1      lanbase                permanent  0 :0 :0                  no      no 1      apcount                evaluation 0 :3 :11                 no      no 1      apcount                base       0 :0 :0                  no      yes                     </pre>	Displays detailed usage information.

	Command or Action	Purpose
	1      apcount          adder          0 :0 :17                      yes      yes	
	Switch#	

### Related Topics

[Monitoring and Maintaining RTU Licenses](#), on page 103

[Right-To-Use AP-Count Licensing](#), on page 96

[Right-to-Use AP-Count Evaluation Licenses](#), on page 97

## Obtaining an Upgrade or Capacity Adder License

You can use the capacity adder licenses to increase the number of access points supported by the switch.

### SUMMARY STEPS

1. `license right-to-use {activate | deactivate} apcount {ap-number | evaluation} slot slot-num [acceptEULA]`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>license right-to-use {activate   deactivate} apcount {ap-number   evaluation} slot slot-num [acceptEULA]</b>  <b>Example:</b> Switch# <code>license right to use activate apcount 5 slot 2 acceptEULA</code>	Activates one or more adder AP-count licenses and immediately accepts the EULA.

### Related Topics

[Right-to-Use AP-Count Evaluation Licenses](#), on page 97

[Right-To-Use AP-Count Licensing](#), on page 96

## Rehosting a License

To rehost a license, you have to deactivate the license from one switch and then activate the same license on another switch.

**SUMMARY STEPS**

1. `license right-to-use deactivate [license-level] apcount ap-number slot slot-num`
2. `license right-to-use activate [license-level] slot slot-num [ acceptEULA]`

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<p><code>license right-to-use deactivate [license-level] apcount ap-number slot slot-num</code></p> <p><b>Example:</b> Switch# <code>license right-to-use deactivate apcount 1 slot 1</code></p> <p><b>Example:</b> Switch# <code>license right-to-use deactivate ipbase slot 1</code></p>	Deactivates the license on one switch. The "ipbase" license level is considered as the example here.
Step 2	<p><code>license right-to-use activate [license-level] slot slot-num [ acceptEULA]</code></p> <p><b>Example:</b> Switch# <code>license right to use activate ipbase slot 2 acceptEULA</code></p> <p><b>Example:</b> Switch# <code>license right-to-use activate ipbase slot 2 acceptEULA</code></p>	Activates the license on another switch. The "ipbase" license level is considered as the example here.

**Related Topics**

[Right-To-Use AP-Count Licensing, on page 96](#)

[Right-to-Use AP-Count Evaluation Licenses, on page 97](#)

**Changing Mobility Mode****SUMMARY STEPS**

1. `wireless mobility controller`
2. `write memory`
3. `reload [ LINE | at | cancel | in | slot stack-member-number | standby-cpu ]`
4. `no wireless mobility controller`
5. `write memory`
6. `reload [ LINE | at | cancel | in | slot stack-member-number | standby-cpu ]`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>wireless mobility controller</b></p> <p><b>Example:</b>  Switch(config)# <b>wireless mobility controller</b>  %  Mobility role changed to Mobility Controller.  Please save config and reboot the whole stack.</p>	Changes a switch in Mobility Agent mode to Mobility Controller mode.
Step 2	<p><b>write memory</b></p> <p><b>Example:</b>  Switch# <b>write memory</b></p> <p>Building configuration...  Compressed configuration from 13870 bytes to 5390 bytes[OK]  Switch#</p>	
Step 3	<p><b>reload [ LINE   at   cancel   in   slot stack-member-number   standby-cpu ]</b></p> <p><b>Example:</b>  Switch# <b>reload slot 3</b>  Proceed with reload? [confirm] <b>y</b></p>	
Step 4	<p><b>no wireless mobility controller</b></p> <p><b>Example:</b>  Switch(config)# <b>no wireless mobility controller</b>  %  Mobility role changed to Mobility Agent.  Please save config and reboot the whole stack.  Switch(config)#</p>	Changes a switch in Mobility Controller mode to Mobility Agent mode.
Step 5	<p><b>write memory</b></p> <p><b>Example:</b>  Switch# <b>write memory</b></p> <p>Building configuration...  Compressed configuration from 13870 bytes to 5390 bytes[OK]  Switch#</p>	
Step 6	<p><b>reload [ LINE   at   cancel   in   slot stack-member-number   standby-cpu ]</b></p> <p><b>Example:</b>  Switch# <b>reload slot 3</b>  Proceed with reload? [confirm] <b>y</b></p>	

**Related Topics**

[Mobility Controller Mode, on page 96](#)

## Monitoring and Maintaining RTU Licenses

Command	Purpose
<code>show license right-to-use default</code>	Displays the default license information.
<code>show license right-to-use detail</code>	Displays detailed information of all the licenses in the switch stack.
<code>show license right-to-use eula {evaluation   permanent}</code> <code>show license right-to-use eula {evaluation   permanent}</code>	Displays the end user license agreement.
<code>show license right-to-use mismatch</code>	Displays the license information that does not match.
<code>show license right-to-use slot slot-number</code>	Displays the license information for a specific slot in a switch stack.
<code>show license right-to-use summary</code>	Displays a summary of the license information on the entire switch stack.
<code>show license right-to-use usage [ slot slot-number ]</code>	Displays detailed information about usage for all licenses in the switch stack.
<code>show switch</code>	Displays detailed information of every member in a switch stack including the state of the license.

**Related Topics**

[Activating an Image Based License, on page 97](#)

[Examples: Activating RTU Image Based Licenses, on page 103](#)

[Activating an AP-Count License, on page 99](#)

## Configuration Examples for RTU Licensing

### Examples: Activating RTU Image Based Licenses

This example shows how to activate an IP Services image license and accept the EULA for a specific slot:

```
Switch# license right-to-use activate ipservices slot 1 acceptEULA
```

```
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

This example shows how to activate a license for evaluation:

```
Switch# license right-to-use activate ipservices evaluation acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

### Related Topics

[Activating an Image Based License, on page 97](#)

[Restrictions for Configuring RTU Licenses, on page 93](#)

[Right-To-Use Licensing, on page 94](#)

[Monitoring and Maintaining RTU Licenses, on page 103](#)

## Examples: Displaying RTU Licensing Information

This example shows the consolidated RTU licensing information from the active switch on a switch stack. All of the members in the stack have the same license level.

```
Switch# show license right-to-use summary

  License Name      Type      Period left
-----
  ipservices      Permanent      Lifetime
-----
```

```
License Level In Use: ipservices
License Level on Reboot: ipbase
```

This example shows a summary of permanent and adder licenses. The evaluation AP-count license is disabled displaying the total number of activated adder AP-count licenses in the switch stack. AP-count licenses in-use mean that they are connected.

```
Switch# show license right-to-use summary

  License Name      Type      Count      Period left
-----
  ipservices      permanent      N/A      Lifetime
  apcount          base          0
  apcount          adder          25      Lifetime
-----
```

```
License Level In Use: ipservices
License Level on Reboot: ipservices eval
Evaluation AP-Count: Disabled
Total AP Count Licenses: 25
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 15
```

This example shows the RTU default licenses. Default licenses are pre-installed and cannot be removed or transferred. If no license is activated the switch uses the default license, after a reboot.

```
Switch# show license right-to-use default

  Slot#      License Name      Type      Count
-----
  1          ipservices      permanent      N/A
```

1	apcount	base	0
1	apcount	adder	10
Slot#	License Name	Type	Count
-----			
2	ipservices	permanent	N/A
2	apcount	base	0
2	apcount	adder	10
Slot#	License Name	Type	Count
-----			
3	ipservices	permanent	N/A
3	apcount	base	0
3	apcount	adder	10

## Example: Displaying RTU License Details

This example shows all the detailed information for the RTU licenses on slot 1:

```
Switch# show license right-to-use detail slot 1
Index 1
  License Name      : ipservices
  Period left       : Lifetime
  License Type      : Permanent
  License State     : Active, In use
  License Location  : Slot 1
Index 2
  License Name      : ipservices
  Period left       : 90
  License Type      : Evaluation
  License State     : Not Activated
  License Location  : Slot 1
Index 3
  License Name      : ipbase
  Period left       : Lifetime
  License Type      : Permanent
  License State     : Active, Not In use
  License Location  : Slot 1
Index 4
  License Name      : ipbase
  Period left       : 90
  License Type      : Evaluation
  License State     : Not Activated
  License Location  : Slot 1
Index 5
  License Name      : lanbase
  Period left       : Lifetime
  License Type      : Permanent
  License State     : Active, Not In use
  License Location  : Slot 1
```

## Example: Displaying RTU License Mismatch

This example shows the license information of the switches in a stack and a mismatch state of a member switch. The member must match the active.

```
Switch# show switch
```

## Example: Displaying RTU Licensing Usage

```
Switch/Stack Mac Address : 1c1d.8625.7700 - Local Mac Address
Switch#  Role      Mac Address      Priority  H/W  Current State
-----  -
*1      Active  1c1d.8625.7700  15      V02  Ready
2       Standby  bc16.f55c.ab80  7       V04  Ready
3       Member  580a.2095.da00  1       V03  Lic-Mismatch
```



**Note** To resolve the license mismatch, first check the RTU license summary:

```
Switch# show license right-to-use
```

Then change the license level of the mismatched switched so that it is the same license level of the active switch. This example shows that the IP Base license was activated for the member switch to match the active switch.

```
Switch# license right-to-use activate ipbase slot 3 acceptEULA
```

## Example: Displaying RTU Licensing Usage

This example shows the detailed licensing usage on your switch stack. The IP Services license in Slot 1 is permanent and usage is one day. An AP-count license in Slot 2 is ready for evaluation. EULA was accepted and state shows in use, but after reboot the evaluation license will be deactivated.

```
Switch# show license right-to-use usage
```

```
Slot#  License Name      Type      usage-duration(y:m:d)  In-Use  EULA
-----  -
1      ipservices           Permanent  0 :10:27               yes     yes
1      ipservices           Evaluation 0 :0 :0                 no      no
1      ipbase               Permanent 0 :0 :9                 no      yes
1      ipbase               Evaluation 0 :0 :0                 no      no
1      lanbase              Permanent 0 :11:12                no      yes
-----  -
Slot#  License Name      Type      usage-duration(y:m:d)  In-Use  EULA
-----  -
2      ipservices           Permanent 0 :3 :25                yes     yes
2      ipservices           Evaluation 0 :0 :0                 no      no
2      ipbase               Permanent 0 :0 :0                 no      yes
2      ipbase               Evaluation 0 :0 :0                 no      no
2      lanbase              Permanent 0 :7 :2                 no      yes
-----  -
Slot#  License Name      Type      usage-duration(y:m:d)  In-Use  EULA
-----  -
3      ipservices           Permanent 0 :6 :15                yes     yes
3      ipservices           Evaluation 0 :0 :0                 no      no
3      ipbase               Permanent 0 :0 :0                 no      yes
3      ipbase               Evaluation 0 :0 :0                 no      no
3      lanbase              Permanent 0 :8 :11                no      yes
-----  -
```



# Additional References for RTU Licensing

## Related Documents

Related Topic	Document Title
RTU commands	<i>System Management Command Reference (Catalyst 3650 Switches)</i>
RTU AP image preload feature	<i>System Management Configuration Guide (Cisco WLC 5700 Series)</i>

## Standards and RFCs

Standard/RFC	Title
None	—

## MIBs

MIB	MIBs Link
Object ciscoLicenseMIB OID 1.3.6.1.4.1.9.9.359 MIB CISCO-LICENSE-MIB ; - View Supporting Images	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information for RTU Licensing

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.



# Configuring Administrator Usernames and Passwords

---

- [Finding Feature Information, page 109](#)
- [Information About Configuring Administrator Usernames and Passwords, page 109](#)
- [Configuring Administrator Usernames and Passwords, page 111](#)
- [Examples: Administrator Usernames and Passwords Configuration, page 112](#)
- [Additional References for Administrator Usernames and Passwords, page 113](#)
- [Feature History and Information For Performing Administrator Usernames and Passwords Configuration, page 114](#)

## Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Information About Configuring Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the switch and viewing configuration information. This section provides instructions for initial configuration and for password recovery.

You can also set administrator usernames and passwords to manage and configure one or more access points that are associated with the switch.

### Strong Passwords

You can set strong administrator passwords such as encrypted passwords with ASCII keys for the administrator user for managing access points.

Use the following guidelines while creating strong passwords:

- There should be at least three of the following categories—lowercase letters, uppercase letters, and digits, and special characters.



---

**Note** Special characters are not supported for username and password for GUI login.

---

- The new password should not be the same as that of the associated username and the username should not be reversed.
- The characters in the password should not be repeated more than three times consecutively.
- The password should not be **cisco**, **ocsic**, **admin**, **nimda**, or any variant obtained by changing the capitalization of letters therein, or by substituting "1" "l" or "!" for i, and/or substituting "0" for "o", and/or substituting "\$" for "s".
- The maximum number of characters accepted for the username and password is 32.

### Encrypted Passwords

You can set three types of keys for the password:

- Randomly generated key—This key is generated randomly and it is the most secure option. To export the configuration file from one system to another, the key should also be exported.
- Static key—The simplest option is to use a fixed (static) encryption key. By using a fixed key, no key management is required, but if the key is somehow discovered, the data can be decrypted by anyone with the knowledge of that key. This is not a secure option and it is called obfuscation in the CLI.
- User defined key—You can define the key by yourself. To export the configuration file from one system to another, both systems should have the same key configured.

# Configuring Administrator Usernames and Passwords

## SUMMARY STEPS

1. **configure terminal**
2. **wireless security strong-password**
3. **username admin-username password {0 unencrypted\_password | 7 hidden\_password | unencrypted\_text}**
4. **username admin-username secret {0 unencrypted\_secret\_text | 4 SHA256 encrypted\_secret\_text | 5 MD5 encrypted\_secret\_text | LINE}**
5. **ap mgmtuser username username password {0 unencrypted password | 8 AES encrypted password }secret {0 unencrypted password | 8 AES encrypted password }**
6. **ap dot1x username username password {0 unencrypted password | 8 AES encrypted password }**
7. **end**
8. **ap name apname mgmtuser username username password password secret secret\_text**
9. **ap name apname dot1x-user username username password password**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>wireless security strong-password</b>  <b>Example:</b> Switch(config)# <b>wireless security strong-password</b>	Enables strong password policy for the administrator user.
Step 3	<b>username admin-username password {0 unencrypted_password   7 hidden_password   unencrypted_text}</b>  <b>Example:</b> Switch(config)# <b>username adminuser1 password 0 QZsek239@</b>	Specifies a username and password for an administrator.  The administrator can configure the switch and view the configured information.
Step 4	<b>username admin-username secret {0 unencrypted_secret_text   4 SHA256 encrypted_secret_text   5 MD5 encrypted_secret_text   LINE}</b>  <b>Example:</b> Switch(config)# <b>username adminuser1 secret 0 QZsek239@</b>	Specifies the secret for the administrator.
Step 5	<b>ap mgmtuser username username password {0 unencrypted password   8 AES encrypted password }secret {0 unencrypted password   8 AES encrypted password }</b>	Specifies administrator username and password for managing all of the access points configured to the switch.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!</pre>	<p>You can also include the secret text to perform privileged access point management.</p> <p><b>Note</b> If your password is not strong enough to fulfill the strong password policy, then the password is rejected with a valid error message. For example, the following password is rejected because it is not a strong password.</p> <pre>Switch# ap mgmtuser username cisco password 0 abcd secret 0 1234</pre>
<b>Step 6</b>	<p><b>ap dot1x username <i>username</i> password {0 <i>unencrypted password</i>   8 <i>AES encrypted password</i> }</b></p> <p><b>Example:</b></p> <pre>Switch(config)# ap dot1x username cisco password 0 Qwci12@</pre>	Specifies the 802.1X username and password for managing all of the access points configured to the switch.
<b>Step 7</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 8</b>	<p><b>ap name <i>apname</i> mgmtuser username <i>username</i> password <i>password</i> secret <i>secret_text</i></b></p> <p><b>Example:</b></p> <pre>Switch# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qne35! secret Nzep592\$</pre>	Configures the administrator username, password, and secret text for managing a specific access point that is configured to the switch.
<b>Step 9</b>	<p><b>ap name <i>apname</i> dot1x-user <i>username</i> password <i>password</i></b></p> <p><b>Example:</b></p> <pre>Switch# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qne35!</pre>	Configures the 802.1X username and password for a specific access point.

## Examples: Administrator Usernames and Passwords Configuration

This example shows how to configure administrator usernames and passwords with the strong password policy in configuration mode:

```
Switch# configure terminal
Switch(config)# wireless security strong-password
Switch(config)# username adminuser1 password 0 QZsek239@
Switch(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!
Switch(config)# ap dot1x username cisco password 0 Qwci12@
Switch# end
```

This example shows how to configure administrator usernames and passwords for an access point in global EXEC mode:

```
Switch# wireless security strong-password
Switch# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@ secret Qwci14@
Switch# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
Switch# end
```

## Additional References for Administrator Usernames and Passwords

### Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series))</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

## Feature History and Information For Performing Administrator Usernames and Passwords Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.





## Configuring 802.11 parameters and Band Selection

---

- [Finding Feature Information, page 115](#)
- [Restrictions on Band Selection, 802.11 Bands, and Parameters, page 115](#)
- [Information About Configuring Band Selection, 802.11 Bands, and Parameters, page 116](#)
- [How to Configure 802.11 Bands and Parameters, page 118](#)
- [Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters, page 126](#)
- [Configuration Examples for Band Selection, 802.11 Bands, and Parameters, page 130](#)
- [Additional References for 802.11 Parameters and Band Selection, page 132](#)
- [Feature History and Information For Performing 802.11 parameters and Band Selection Configuration, page 133](#)

### Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### Restrictions on Band Selection, 802.11 Bands, and Parameters

- Band-selection enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.
- Band selection can be used only with Cisco Aironet 1140, 1250, 1260, 1550, 1800, 2600, 2800, 3500, 3600, 3800 series access points.
- Mid RSSI is not supported on Cisco Aironet 1600 Series access points.

- Band selection is not supported in Cisco Aironet 1040, OEAP 600 series access points.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

## Information About Configuring Band Selection, 802.11 Bands, and Parameters

### Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three nonoverlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on the switch.

Band selection works by regulating probe responses to clients and it can be enabled on a per-WLAN basis. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. In the access point, the band select table can be viewed by giving `show dot11 band-select` command. It can also be viewed from `show cont d0/d1 | begin Lru`.



#### Note

The WMM default configuration will not be shown in **show running-config** output.

### Band Selection Algorithm

The band selection algorithm affects clients that use 2.4-GHz band. Initially, when a client sends a probe request to the access point, the corresponding client probe's Active and Count values (as seen from the band select table) become 1. The algorithm functions based on the following scenarios:

- Scenario - 1: Client RSSI (as seen from **show cont d0/d1 | begin RSSI**) is greater than both Mid-RSSI and Acceptable Client RSSI.
  - Dual band clients—No 2.4-GHz probe responses are seen at any time; 5-GHz probe responses are seen for all 5-GHz probe requests.

- Single band (2.4-GHz) clients— 2.4-GHz probe responses are seen only after the probe suppression cycle.
  - After the client's probe count reaches the configured probe cycle count, the algorithm waits for the Age Out Suppression time and then marks the client probe's Active value as 0. Then, the algorithm is restarted.
- Scenario - 2: Client RSSI (as seen from **show cont d0/d1 | begin RSSI**) lies between Mid-RSSI and Acceptable Client RSSI.
    - All 2.4-GHz and 5-GHz probe requests are responded without any restrictions.
    - This scenario is similar to the band select disabled.

**Note**

---

The client RSSI value (seen as **sh cont d0 | begin RSSI**) is the average of the client packets received, and the Mid-RSSI feature is the instantaneous RSSI value of the probe packets. As a result, the client RSSI is seen as weaker than the configured Mid-RSSI value (7 dB delta). The 802.11b probes from the client are suppressed to push the client to associate with the 802.11a band.

---

## 802.11 Bands

You can configure the 802.11b/g/n (2.4-GHz) and 802.11a/n (5-GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n are enabled.

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, you must mark 11g rates as mandatory.

## 802.11n Parameter

This section provides instructions for managing 802.11n access points on your network. The 802.11n devices support the 2.4- and 5-GHz bands and offer high-throughput data rates.

The 802.11n high-throughput rates are available on all 802.11n access points for WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

**Note**

---

Some Cisco 802.11n APs may intermittently emit incorrect beacon frames, which can trigger false wIPS alarms. We recommend that you ignore these alarms. The issue is observed in the following Cisco 802.11n APs: 1140, 1250, 2600, 3500, and 3600.

---

## 802.11h Parameter

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

# How to Configure 802.11 Bands and Parameters

## Configuring Band Selection (CLI)

### SUMMARY STEPS

1. **configure terminal**
2. **wireless client band-select cycle-count** *cycle\_count*
3. **wireless client band-select cycle-threshold** *milliseconds*
4. **wireless client band-select expire suppression** *seconds*
5. **wireless client band-select expire dual-band** *seconds*
6. **wireless client band-select client-rssi** *client\_rssi*
7. **end**
8. **wlan wlan\_profile\_name wlan\_ID SSID\_network\_name band-select**
9. **end**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless client band-select cycle-count</b> <i>cycle_count</i>  <b>Example:</b> Switch(config)# <b>wireless client band-select cycle-count 3</b>	Sets the probe cycle count for band select.  You can enter a value between 1 and 10 for the <i>cycle_count</i> parameter.
<b>Step 3</b>	<b>wireless client band-select cycle-threshold</b> <i>milliseconds</i>  <b>Example:</b> Switch(config)# <b>wireless client band-select cycle-threshold 5000</b>	Sets the time threshold for a new scanning cycle period.  You can enter a value for threshold between 1 and 1000 for the <i>milliseconds</i> parameter.
<b>Step 4</b>	<b>wireless client band-select expire suppression</b> <i>seconds</i>  <b>Example:</b> Switch(config)# <b>wireless client band-select expire suppression 100</b>	Sets the suppression expire to the band select.  You can enter a value for suppression between 10 to 200 for the <i>seconds</i> parameter.
<b>Step 5</b>	<b>wireless client band-select expire dual-band</b> <i>seconds</i>	Sets the dual band expire.

	Command or Action	Purpose
	<p><b>Example:</b> Switch(config)# <b>wireless client band-select expire dual-band 100</b></p>	You can enter a value for dual band between 10 and 300 for the <i>seconds</i> parameter.
<b>Step 6</b>	<p><b>wireless client band-select client-rssi <i>client_rssi</i></b></p> <p><b>Example:</b> Switch(config)# <b>wireless client band-select client-rssi 40</b></p>	<p>Sets the client RSSI threshold.</p> <p>You can enter a value for minimum dBm of a client RSSI to respond to a probe between 20 and 90 for the <i>client_rssi</i> parameter.</p>
<b>Step 7</b>	<p><b>end</b></p> <p><b>Example:</b> Switch(config)# <b>end</b></p>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 8</b>	<p><b>wlan <i>wlan_profile_name</i> <i>wlan_ID</i> <i>SSID_network_name</i> band-select</b></p> <p><b>Example:</b> Switch(config)# <b>wlan wlan1 25 ssid12</b> Switch(config-wlan)# <b>band-select</b></p>	<p>Configures band selection on specific WLANs.</p> <p>You can enter a value between 1 and 512 for the <i>wlan_ID</i> parameter.</p> <p>You can enter the up to 32 alphanumeric characters for <i>SSID_network_name</i> parameter.</p>
<b>Step 9</b>	<p><b>end</b></p> <p><b>Example:</b> Switch(config)# <b>end</b></p>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring the 802.11 Bands (CLI)

You can configure 802.11 bands and parameters.

## SUMMARY STEPS

1. `configure terminal`
2. `ap dot11 5ghz shutdown`
3. `ap dot11 24ghz shutdown`
4. `ap dot11 {5ghz | 24ghz} beaconperiod time_unit`
5. `ap dot11 {5ghz | 24ghz} fragmentation threshold`
6. `ap dot11 {5ghz | 24ghz} dtpc`
7. `wireless client association limit number interval milliseconds`
8. `ap dot11 {5ghz | 24ghz} rate rate {disable | mandatory | supported}`
9. `no ap dot11 5ghz shutdown`
10. `no ap dot11 24ghz shutdown`
11. `ap dot11 24ghz dot11g`
12. `end`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code>  <b>Example:</b> <code>Switch# configure terminal</code>	Enters global configuration mode.
Step 2	<code>ap dot11 5ghz shutdown</code>  <b>Example:</b> <code>Switch(config)# ap dot11 5ghz shutdown</code>	Disables the 802.11a band.  <b>Note</b> You must disable the 802.11a band before configuring the 802.11a network parameters.
Step 3	<code>ap dot11 24ghz shutdown</code>  <b>Example:</b> <code>Switch(config)# ap dot11 24ghz shutdown</code>	Disables the 802.11b band.  <b>Note</b> You must disable the 802.11b band before configuring the 802.11b network parameters.
Step 4	<code>ap dot11 {5ghz   24ghz} beaconperiod <i>time_unit</i></code>  <b>Example:</b> <code>Switch(config)# ap dot11 5ghz beaconperiod 500</code>	Specifies the rate at which the SSID is broadcast by the access point.  The beacon interval is measured in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.
Step 5	<code>ap dot11 {5ghz   24ghz} fragmentation <i>threshold</i></code>  <b>Example:</b> <code>Switch(config)# ap dot11 5ghz fragmentation 300</code>	Specifies the size at which packets are fragmented.  The threshold is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

	Command or Action	Purpose
Step 6	<p><b>ap dot11 {5ghz   24ghz} dtpc</b></p> <p><b>Example:</b>  Switch(config)# <b>ap dot11 5ghz dtpc</b></p> <p>Switch(config)# <b>no ap dot11 24ghz dtpc</b></p>	<p>Enables access points to advertise their channels and transmit the power levels in beacons, and probe responses.</p> <p>The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.</p> <p><b>Note</b> On access points that run Cisco IOS software, this feature is called world mode.</p> <p>The <b>no</b> form of the command disables the 802.11a or 802.11b DTTPC setting.</p>
Step 7	<p><b>wireless client association limit <i>number</i> interval <i>milliseconds</i></b></p> <p><b>Example:</b>  Switch(config)# <b>wireless client association limit 50 interval 1000</b></p>	<p>Specifies the maximum allowed clients that can be configured.</p> <p>You can configure a maximum number of association request on a single access point slot at a given interval. The range of association limit that you can configure is from one through 100.</p> <p>The association request limit interval is measured between 100 to 10000 milliseconds.</p>
Step 8	<p><b>ap dot11 {5ghz   24ghz} rate <i>rate</i> {<i>disable</i>   <i>mandatory</i>   <i>supported</i>}</b></p> <p><b>Example:</b>  Switch(config)# <b>ap dot11 5ghz rate 36 mandatory</b></p>	<p>Specifies the rate at which data can be transmitted between the controller and the client.</p> <ul style="list-style-type: none"> <li>• <i>disabled</i>—Defines that the clients specify the data rates used for communication.</li> <li>• <i>mandatory</i>—Defines that the clients support this data rate in order to associate to an access point on the controller.</li> <li>• <i>supported</i>—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.</li> <li>• <i>rate</i>—Specifies the rate at which data is transmitted. For the 802.11a and 802.11b bands, the data is transmitted at the rate of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.</li> </ul>
Step 9	<p><b>no ap dot11 5ghz shutdown</b></p> <p><b>Example:</b>  Switch(config)# <b>no ap dot11 5ghz shutdown</b></p>	<p>Enables the 802.11a band.</p> <p><b>Note</b> The default value is enabled.</p>
Step 10	<p><b>no ap dot11 24ghz shutdown</b></p> <p><b>Example:</b>  Switch(config)# <b>no ap dot11 24ghz shutdown</b></p>	<p>Enables the 802.11b band.</p> <p><b>Note</b> The default value is enabled.</p>
Step 11	<p><b>ap dot11 24ghz dot11g</b></p>	<p>Enables or disables 802.11g network support.</p>

	Command or Action	Purpose
	<b>Example:</b> Switch(config)# <b>ap dot11 24ghz dot11g</b>	The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.
<b>Step 12</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.

## Configuring 802.11n Parameters (CLI)

### SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz} dot11n**
3. **ap dot11 {5ghz | 24ghz} dot11n mcs tx *rtu***
4. **wlanwlan\_profile\_name wlan\_ID SSID\_network\_name wmm require**
5. **ap dot11 {5ghz | 24ghz} shutdown**
6. **{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}**
7. **no ap dot11 {5ghz | 24ghz} shutdown**
8. **ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}**
9. **ap dot11 {5ghz | 24ghz} dot11n rifs rx**
10. **end**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>ap dot11 {5ghz   24ghz} dot11n</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz dot11n</b>	Enables 802.11n support on the network.  The <b>no</b> form of the command disables the 802.11n support on the network.
<b>Step 3</b>	<b>ap dot11 {5ghz   24ghz} dot11n mcs tx <i>rtu</i></b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz dot11n mcs tx 20</b>	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. You can set a value from 0 through 23 for the <b>mcs tx</b> parameter.  The <b>no</b> form of the command disables the MCS rates that is configured.



	Command or Action	Purpose																		
<b>Step 4</b>	<p><code>wlan wlan_profile_name wlan_ID SSID_network_name wmm require</code></p> <p><b>Example:</b>                      Switch(config)# <code>wlan wlan1 25 ssid12</code>                      Switch(config-wlan)# <code>wmm require</code></p>	<p>Enables WMM on the WLAN and uses the 802.11n data rates that you configured.</p> <p>The <b>require</b> parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.</p>																		
<b>Step 5</b>	<p><code>ap dot11 {5ghz   24ghz} shutdown</code></p> <p><b>Example:</b>                      Switch(config)# <code>ap dot11 5ghz shutdown</code></p>	<p>Disables the network.</p>																		
<b>Step 6</b>	<p><code>{ap   no ap} dot11 {5ghz   24 ghz} dot11n a-mpdu tx priority {all   0-7}</code></p> <p><b>Example:</b>                      Switch(config)# <code>ap dot11 5ghz dot11n a-mpdu tx priority all</code></p>	<p>Specifies the aggregation method used for 802.11n packets.</p> <p>Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). Both A-MPDU and A-MSDU are performed in the software.</p> <p>You can specify the aggregation method for various types of traffic from the access point to the clients.</p> <p>The following table defines the priority levels (0-7) assigned per traffic type.</p> <p><b>Table 11: Traffic Type Priority Levels</b></p> <table border="1"> <thead> <tr> <th>User Priority</th> <th>Traffic Type</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Best effort</td> </tr> <tr> <td>1</td> <td>Background</td> </tr> <tr> <td>2</td> <td>Spare</td> </tr> <tr> <td>3</td> <td>Excellent effort</td> </tr> <tr> <td>4</td> <td>Controlled load</td> </tr> <tr> <td>5</td> <td>Video, less than 100-ms latency and jitter</td> </tr> <tr> <td>6</td> <td>Voice, less than 100-ms latency and jitter</td> </tr> <tr> <td>7</td> <td>Network control</td> </tr> </tbody> </table>	User Priority	Traffic Type	0	Best effort	1	Background	2	Spare	3	Excellent effort	4	Controlled load	5	Video, less than 100-ms latency and jitter	6	Voice, less than 100-ms latency and jitter	7	Network control
User Priority	Traffic Type																			
0	Best effort																			
1	Background																			
2	Spare																			
3	Excellent effort																			
4	Controlled load																			
5	Video, less than 100-ms latency and jitter																			
6	Voice, less than 100-ms latency and jitter																			
7	Network control																			

	Command or Action	Purpose
		<p>You can configure each priority level independently, or you can use the all parameter to configure all of the priority levels at once. You can configure priority levels so that the traffic uses either A-MPDU transmission or A-MSDU transmission.</p> <ul style="list-style-type: none"> <li>• When you use the <b>ap</b> command along with the other options, the traffic associated with that priority level uses A-MPDU transmission.</li> <li>• When you use the <b>no ap</b> command along with the other options, the traffic associated with that priority level uses A-MSDU transmission.</li> </ul> <p>Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4 and 5 and the rest are disabled. By default, A-MPDU is enabled for all priorities except 6 and 7.</p>
<b>Step 7</b>	<b>no ap dot11 {5ghz   24ghz} shutdown</b>  <b>Example:</b> Switch(config)# <b>no ap dot11 5ghz shutdown</b>	Reenables the network.
<b>Step 8</b>	<b>ap dot11 {5ghz   24ghz} dot11n guard-interval {any   long}</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz dot11n guard-interval long</b>	Configures the guard interval for the network.
<b>Step 9</b>	<b>ap dot11 {5ghz   24ghz} dot11n rifs rx</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz dot11n rifs rx</b>	Configures the Reduced Interframe Space (RIFS) for the network.
<b>Step 10</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring 802.11h Parameters (CLI)

### SUMMARY STEPS

1. `configure terminal`
2. `ap dot11 5ghz shutdown`
3. `{ap | no ap} dot11 5ghz channelswitch mode switch_mode`
4. `ap dot11 5ghz power-constraint value`
5. `no ap dot11 5ghz shutdown`
6. `end`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code>  <b>Example:</b> <code>Switch# configure terminal</code>	Enters global configuration mode.
Step 2	<code>ap dot11 5ghz shutdown</code>  <b>Example:</b> <code>Switch(config)# ap dot11 5ghz shutdown</code>	Disables the 802.11a network.
Step 3	<code>{ap   no ap} dot11 5ghz channelswitch mode <i>switch_mode</i></code>  <b>Example:</b> <code>Switch(config)# ap dot11 5ghz channelswitch mode 0</code>	Enables or disables the access point to announce when it is switching to a new channel.  You can enter a 0 or 1 for the <b>channelswitch</b> parameter to specify whether transmissions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled.
Step 4	<code>ap dot11 5ghz power-constraint <i>value</i></code>  <b>Example:</b> <code>Switch(config)# ap dot11 5ghz power-constraint 200</code>	Configures the 802.11h power constraint value in a range from zero through 255.  The default value for the value parameter is 3 dB.
Step 5	<code>no ap dot11 5ghz shutdown</code>  <b>Example:</b> <code>Switch(config)# no ap dot11 5ghz shutdown</code>	Reenables the 802.11a network.
Step 6	<code>end</code>  <b>Example:</b> <code>Switch(config)# end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

# Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters

## Monitoring Configuration Settings Using Band Selection and 802.11 Bands Commands

This section describes the new commands for band selection and 802.11 bands.

The following commands can be used to monitor band selection, and 802.11 bands and parameters the switch.

**Table 12: Monitoring Configuration Settings Using Band Selection and 802.11 Bands Commands**

Command	Purpose
<b>show ap dot11 5ghz network</b>	Displays 802.11a bands network parameters, 802.11a operational rates, 802.11n MCS settings, and 802.11n status information.
<b>show ap dot11 24ghz network</b>	Displays 802.11b bands network parameters, 802.11b/g operational rates, 802.11n MCS settings, and 802.11n status information.
<b>show wireless dot11h</b>	Displays 802.11h configuration parameters.
<b>show wireless band-select</b>	Displays band select configuration settings.

### Example: Viewing the Configuration Settings for 5-GHz Band

```
Switch# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
```

```
MCS 4 : Supported
MCS 5 : Supported
MCS 6 : Supported
MCS 7 : Supported
MCS 8 : Supported
MCS 9 : Supported
MCS 10 : Supported
MCS 11 : Supported
MCS 12 : Supported
MCS 13 : Supported
MCS 14 : Supported
MCS 15 : Supported
MCS 16 : Supported
MCS 17 : Supported
MCS 18 : Supported
MCS 19 : Supported
MCS 20 : Supported
MCS 21 : Supported
MCS 22 : Supported
MCS 23 : Supported
802.11n Status:
A-MPDU Tx:
  Priority 0 : Enabled
  Priority 1 : Disabled
  Priority 2 : Disabled
  Priority 3 : Disabled
  Priority 4 : Enabled
  Priority 5 : Enabled
  Priority 6 : Disabled
  Priority 7 : Disabled
A-MSDU Tx:
  Priority 0 : Enabled
  Priority 1 : Enabled
  Priority 2 : Enabled
  Priority 3 : Enabled
  Priority 4 : Enabled
  Priority 5 : Enabled
  Priority 6 : Disabled
  Priority 7 : Disabled
Guard Interval : Any
Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admission Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwidth sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
```

**Example: Viewing the Configuration Settings for 24-GHz Band**

```
Video max RF bandwidth : Infinite
Video reserved roaming bandwidth : 0
```

**Example: Viewing the Configuration Settings for 24-GHz Band**

```
Switch# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

802.11b/g Operational Rates
802.11b 1M : Mandatory
802.11b 2M : Mandatory
802.11b 5.5M : Mandatory
802.11g 6M : Supported
802.11g 9M : Supported
802.11b 11M : Mandatory
802.11g 12M : Supported
802.11g 18M : Supported
802.11g 24M : Supported
802.11g 36M : Supported
802.11g 48M : Supported
802.11g 54M : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported
MCS 6 : Supported
MCS 7 : Supported
MCS 8 : Supported
MCS 9 : Supported
MCS 10 : Supported
MCS 11 : Supported
MCS 12 : Supported
MCS 13 : Supported
MCS 14 : Supported
MCS 15 : Supported
MCS 16 : Supported
MCS 17 : Supported
MCS 18 : Supported
MCS 19 : Supported
MCS 20 : Supported
MCS 21 : Supported
MCS 22 : Supported
MCS 23 : Supported
802.11n Status:
A-MPDU Tx:
Priority 0 : Enabled
Priority 1 : Disabled
Priority 2 : Disabled
Priority 3 : Disabled
Priority 4 : Enabled
Priority 5 : Enabled
Priority 6 : Disabled
Priority 7 : Disabled
A-MSDU Tx:
Priority 0 : Enabled
Priority 1 : Enabled
Priority 2 : Enabled
Priority 3 : Enabled
Priority 4 : Enabled
Priority 5 : Enabled
Priority 6 : Disabled
Priority 7 : Disabled
Guard Interval : Any
Rifs Rx : Enabled
```

```

Beacon Interval : 100
CF Pollable Mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 11
Default Tx Power Level : 1
DTPC Status : true
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admission Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwidth sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0

```

## Example: Viewing the status of 802.11h Parameters

```

Switch# show wireless dot11h
Power Constraint: 0
Channel Switch: 0
Channel Switch Mode: 0

```

## Example: Verifying the Band Selection Settings

The following example displays band select configuration:

```

Switch# show wireless band-select

Band Select Probe Response : per WLAN enabling
Cycle Count                : 2
Cycle Threshold (millisec) : 200
Age Out Suppression (sec)  : 20
Age Out Dual Band (sec)   : 60
Client RSSI (dBm)         : -80
Client Mid RSSI (dBm)     : -80

```

# Configuration Examples for Band Selection, 802.11 Bands, and Parameters

## Examples: Band Selection Configuration

This example shows how to set the probe cycle count and time threshold for a new scanning cycle period for band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select cycle-count 3
Switch(config)# wireless client band-select cycle-threshold 5000
Switch(config)# end
```

This example shows how to set the suppression expire to the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select expire suppression 100
Switch(config)# end
```

This example shows how to set the dual band expire for the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select expire dual-band 100
Switch(config)# end
```

This example shows how to set the client RSSI threshold for the band select:

```
Switch# configure terminal
Switch(config)# wireless client band-select client-rssi 40
Switch(config)# end
```

This example shows how to configure band selection on specific WLANs:

```
Switch# configure terminal
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# band-select
Switch(config)# end
```

## Examples: 802.11 Bands Configuration

This example shows how to configure 802.11 bands using beacon interval, fragmentation, and dynamic transmit power control:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 24ghz shutdown
Switch(config)# ap dot11 5ghz beaconperiod 500
Switch(config)# ap dot11 5ghz fragmentation 300
Switch(config)# ap dot11 5ghz dtpc
Switch(config)# wireless client association limit 50 interval 1000
Switch(config)# ap dot11 5ghz rate 36 mandatory
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# no ap dot11 24ghz shutdown
Switch(config)# ap dot11 24ghz dot11g
Switch(config)# end
```



## Examples: 802.11n Configuration

This example shows how to configure 802.11n parameters for 5-GHz band using aggregation method:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\
Switch(config-wlan)# exit
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)#exit
```

This example shows how to configure the guard interval for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\
Switch(config-wlan)# exit
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n guard-interval long
Switch(config)#end
```

This example shows how to configure the RIFS for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz dot11n
Switch(config)# ap dot11 5ghz dot11n mcs tx 20
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# wmm require\
Switch(config-wlan)# exit
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz dot11n rifs rx
Switch(config)#end
```

## Examples: 802.11h Configuration

This example shows how to configure the access point to announce when it is switching to a new channel using restriction transmission:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz channelswitch mode 0
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)#end
```

This example shows how to configure the 802.11h power constraint for 5-GHz band:

```
Switch# configure terminal
Switch(config)# ap dot11 5ghz shutdown
Switch(config)# ap dot11 5ghz power-constraint 200
Switch(config)# no ap dot11 5ghz shutdown
Switch(config)#end
```

## Additional References for 802.11 Parameters and Band Selection

### Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information For Performing 802.11 parameters and Band Selection Configuration

Release	Feature Information
Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE	This feature was introduced.





## CHAPTER 8

# Configuring Aggressive Load Balancing

- [Finding Feature Information, page 135](#)
- [Restrictions for Aggressive Load Balancing, page 135](#)
- [Information for Configuring Aggressive Load Balancing Parameters, page 136](#)
- [How to Configure Aggressive Load Balancing, page 137](#)
- [Monitoring Aggressive Load Balancing, page 138](#)
- [Examples: Aggressive Load Balancing Configuration, page 139](#)
- [Additional References for Aggressive Load Balancing, page 139](#)
- [Feature History and Information For Performing Aggressive Load Balancing Configuration , page 140](#)

## Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Restrictions for Aggressive Load Balancing

- You can configure aggressive load balancing only from the command-line interface.
- Aggressive load balancing is disabled by default, you must enable it manually.
- You can enable load balancing either separately or together with the band select configurations.
- When the band select is enabled on the dual-band clients, the load balancing parameter selects only the lowest load radio from 5-GHz radios. For the 2.4-GHz clients, there is no information of the client on 5 GHz and therefore the load balancing algorithm can only be selected between radio on 2.4 GHz.
- You can operate load balancing of clients between access points on the same switch but not for the clients between access points on the different switch.

- The load balancing uses an existing association denial mechanism based on the number of client on the radio and the band select is implemented by the distributed probe response suppression on the access point only.

## Information for Configuring Aggressive Load Balancing Parameters

### Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. The code 17 indicates that the AP is busy. The AP does not respond with an association response bearing 'success' if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is exceeded, and another less busy AP heard the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).



#### Note

Voice Client does not authenticate when delay is configured more than 300 ms. To avoid this configure a Central-Auth, Local Switching WLAN with CCKM, configure a Pageant Router between AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN and try associating the voice client

The maximum number of client associations that the access points can support is dependent upon the following factors:

- The maximum number of client associations differs for lightweight and autonomous Cisco IOS access points.
- There may be a limit per radio and an overall limit per AP.
- AP hardware (the 16-MB APs have a lower limit than the 32-MB and higher APs)

The Client Association Limits for Lightweight Access Points are as follows:

- For 16-MB APs, the limit is 128 clients per AP. This limit is applicable to 1100 and 1200 series APs.
- For 32-MB and higher APs, there is no per-AP limit.

The maximum Client Association Limits per-radio for all of the Cisco IOS APs is 200 associations.

**Note**

With 32-MB and higher lightweight Cisco IOS APs, with two radios, up to  $200 + 200 = 400$  associations are supported.

The maximum Client Association Limits per Autonomous Cisco IOS access point is around 80 to 127 clients per AP. This number varies depending on the following factors:

- AP model (whether it is 16 MB or 32 MB or higher)
- Cisco IOS software release
- Hardware configuration (two radios use more memory than one)
- Enabled features (WDS functionality in particular)

The per-radio limit is about 200 associations. One association will likely hit the per-AP limit first. Unlike Cisco Unified Wireless Network, autonomous Cisco IOS supports per-SSID/per-AP association limits. This limit is configured using the max-associations CLI, under dot11 SSID. The maximum number is 255 associations (which is also the default number).

**Note**

For a FlexConnect AP the association is locally handled. The load-balancing decisions are taken at the Cisco WLC. A FlexConnect AP initially responds to the client before knowing the result of calculations at the Cisco WLC. Load-balancing doesn't take effect when the FlexConnect AP is in standalone mode.

FlexConnect AP does not send (re)association response with status 17 for Load-Balancing as Local mode APs do; instead, it first sends (re)association with status 0 (success) and then death with reason 5.

# How to Configure Aggressive Load Balancing

## Configuring Aggressive Load Balancing

### SUMMARY STEPS

1. **configure terminal**
2. **wireless load-balancing window** *client-count*
3. **wireless load-balancing denial** *denial-count*
4. **end**
5. **wlan** *wlan\_profile\_name wlan\_ID SSID\_network\_name* **load-balance**
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
Step 2	<b>wireless load-balancing window <i>client-count</i></b>  <b>Example:</b> Switch(config)# <code>wireless load-balancing window 1</code>	Sets the client window for aggressive load balancing. You can enter a value between 0 and 20 for the <i>client_count</i> parameter.
Step 3	<b>wireless load-balancing denial <i>denial-count</i></b>  <b>Example:</b> Switch(config)# <code>wireless load-balancing denial-count 1</code>	Sets the denial count for load balancing. You can enter a value between 0 and 10 for the <i>denial_count</i> parameter.
Step 4	<b>end</b>  <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
Step 5	<b>wlan <i>wlan_profile_name</i> <i>wlan_ID</i> <i>SSID_network_name</i> load-balance</b>  <b>Example:</b> Switch(config)# <code>wlan wlan1 25 ssid12</code> Switch(config-wlan)# <code>load-balance</code>	Enables or disables aggressive load balancing on specific WLANs. You can enter a value between 1 and 512 for the <i>wlan_ID</i> parameter. You can enter the up to 32 alphanumeric characters for <i>SSID_network_name</i> parameter.
Step 6	<b>end</b>  <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Monitoring Aggressive Load Balancing

This section describes the new command for aggressive load balancing.

The following command can be used to monitor aggressive load balancing on the switch.

**Table 13: Monitoring Aggressive Load Balancing Command**

Command	Purpose
<code>show wireless load-balancing</code>	Displays the status of the load-balancing feature.



## Examples: Aggressive Load Balancing Configuration

This example shows how to configure the load balancing denial count:

```
Switch# configure terminal
Switch(config)# wireless load-balancing denial-count 1
Switch(config)# end
Switch# show wireless load-balancing
```

This example shows how to configure the client window for aggressive load balancing:

```
Switch# configure terminal
Switch(config)# wireless load-balancing window 1
Switch(config)# end
Switch# show wireless load-balancing
```

This example shows how to configure load balancing on specific WLAN:

```
Switch# configure terminal
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# load-balance
Switch(config)# end
Switch# show wireless load-balancing
```

## Additional References for Aggressive Load Balancing

### Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

## Feature History and Information For Performing Aggressive Load Balancing Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.



## Configuring Client Roaming

- [Finding Feature Information, page 141](#)
- [Restrictions for Configuring Client Roaming, page 141](#)
- [Information About Client Roaming, page 142](#)
- [How to Configure Layer 2 or Layer 3 Roaming, page 144](#)
- [Monitoring Client Roaming Parameters, page 151](#)
- [Monitoring Mobility Configurations, page 151](#)
- [Additional References for Configuring Client Roaming, page 153](#)
- [Feature History and Information For Performing Client Roaming Configuration , page 154](#)

### Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### Restrictions for Configuring Client Roaming

The following are the restrictions that you should be aware while configuring client roaming:

- Cisco Compatible Extensions (CCX) support is enabled automatically for every WLAN on the switch and cannot be disabled. The switch stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) to utilize these roaming enhancements.
- Client roaming between 600 Series Access points is not supported.

## Information About Client Roaming

The controllers deliver high-end wireless services to the clients roaming across wireless network. Now, the wireless services are integrated with the switches, thus delivering a value-added Cisco unified new mobility architecture. This unified architecture enables client-roaming services to both wireless and wired clients with seamless, fast- roaming services.

The new mobility architecture supports fast client roaming services using logical categorization of network into Mobility Domains (MDs), Mobility Groups (MGs), Mobility Subdomains (MSDs), and Switch Peer Groups (SPGs) using systems such as Mobility Oracle (MO), Mobility Controller (MC), and Mobility Agent (MA).

- A **Mobility Domain** is the entire domain across which client roaming is supported. It is a collection of mobility groups. For example, a campus network can be considered as a mobility domain.
- A **Mobility Group** is a collection of mobility subdomains across which fast roaming is supported. The mobility group can be one or more buildings within a campus across which frequent roaming is supported.
- A **Mobility Subdomain** is an autonomous portion of the mobility domain network. Each mobility subdomain contains one mobility controller (MC) and a collection of SPGs. A subdomain is equivalent to an 802.11r key domain.
- A **Switch Peer Group** is a collection of mobility agents.
- The **Mobility Oracle** acts as the point of contact for mobility events that occur across mobility subdomains. The mobility oracle also maintains a local database of each client in the entire mobility domain, their home and current subdomain. There is only one MO for an entire mobility domain. The Cisco WLC 5700 Series Controllers or Cisco Unified Wireless Networking Solution controller can act as MO.
- The **Mobility Controller** provides mobility management services for inter-SPG roaming events. The MC sends the configuration like SPG name and SPG peer member list to all of the mobility agents under its subdomain. The Cisco WLC 5700 Series Controllers, Cisco Catalyst 3850 Switch, or Cisco Unified Wireless Networking Solution controller can act as MC. The MC has MC functionality and MA functionality that is running internally into it.
- The **Mobility Agent** is the component that maintains client mobility state machine for a mobile client. All APs are connected to the mobility agent.

The New mobility architecture supports seamless roaming in the following scenarios:

- Intra-switch roaming—The client roaming between APs managed by same mobility agent.
- Intra-SPG roaming—The client roaming between mobility agents in the same SPG.
- Inter-SPG, Intra-subdomain roaming—The client roaming between mobility agents in different SPGs within the same subdomain.
- Inter-subdomain roaming—The client roaming between mobility agents across a subdomain.

### Fast Roaming

New mobility architecture supports fast roaming when clients roam within a mobility group by eliminating the need for full authentication. Security polices should be same across the switches for fast roaming.

### Local, anchor, foreign MAs and MCs

When a client joins an MA initially and its point of attachment has not changed, that MA is referred as local or associated MA. The MC to which this MA is associated is referred as local or associated MC.

When a client roams between two MAs, the MA to which the client was previously associated is the anchor MA (point of attachment) and the MA to which the client is currently associated is the foreign or associated MA (point of presence). The MCs to which these MAs are associated are referred as anchor, foreign, or associated MCs, respectively.

## Inter-Subnet Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.\*.\* client auto-IP address or when the operator-set user timeout is exceeded.

## Voice-over-IP Telephone Roaming

802.11 voice-over-IP (VoIP) telephones actively seek out associations with the strongest RF signal to ensure the best quality of service (QoS) and the maximum throughput. The minimum VoIP telephone requirement of 20-millisecond or shorter latency time for the roaming handover is easily met by the Cisco Wireless solution, which has an average handover latency of 5 or fewer milliseconds when open authentication is used. This short latency period is controlled by controllers rather than allowing independent access points to negotiate roaming handovers.

The Cisco Wireless solution supports 802.11 VoIP telephone roaming across lightweight access points managed by controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone because the session is sustained and a tunnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned IP address as long as the session remains active. The tunnel is torn down, and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP address or a 169.254.\*.\* VoIP telephone auto-IP address or when the operator-set user timeout is exceeded.

## CCX Layer 2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements:

- Access point assisted roaming—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.
- Enhanced neighbor list—This feature focuses on improving a CCXv4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.

- Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.




---

**Note** To see whether a particular client supports E2E, choose **Wireless > Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the E2E Version text box in the Client Properties area.

---

- Roam reason report—This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.
- Directed roam request—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX clients and clients running CCXv3 or below must not take any action. No configuration is required for this feature.

## How to Configure Layer 2 or Layer 3 Roaming

### Configuring Layer 2 or Layer 3 Roaming

#### Before You Begin

To configure the mobility agent for Layer 2 or Layer 3 roaming, the following requisites should be considered:

- SSID and security polices should be same across MAs for Layer 2 and Layer 3 roaming.
- Client VLAN ID should be same for Layer 2 roaming and different for Layer 3 roaming.
- Bridge domain ID and client VLAN IDs should be same for Layer 2 roaming. Either one or both of the bridge domain ID and client VLAN ID should be different for Layer 3 roaming.

#### SUMMARY STEPS

1. **configure terminal**
2. **wlan wlan\_profile\_name wlan\_ID SSID\_network\_name**
3. **no mobility anchor sticky**
4. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>wlan wlan_profile_name wlan_ID SSID_network_name</b>  <b>Example:</b> Switch(config)# <b>wlan wlan1</b>	Enters WLAN configuration mode.
Step 3	<b>no mobility anchor sticky</b>  <b>Example:</b> Switch(config-wlan)# <b>no mobility anchor sticky</b>	(Optional) Disables Layer 2 anchoring.
Step 4	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring CCX Client Roaming Parameters (CLI)

## SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz} l2roam rf-params {default | custom min-rssi roam-hyst scan-thresh trans-time}**
3. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>ap dot11 {5ghz   24ghz} l2roam rf-params {default   custom min-rssi roam-hyst scan-thresh trans-time}</b>	Configures CCX Layer 2 client roaming parameters.  To choose the default RF parameters, enter the <b>default</b> option.  To fine-tune the RF parameters that affect client roaming, enter the <b>custom</b> option and then enter any one of the following options:

	Command or Action	Purpose
	<p><b>Example:</b>  Switch#ap dot11 5ghz  12roam rf-params custom  -80</p>	<ul style="list-style-type: none"> <li data-bbox="544 321 1487 598"> <p>• <b>Minimum RSSI</b>—Indicates minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.</p> <p>If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.</p> <p>You can configure the minimum RSSI range from –50 through –90 dBm and the default value is –85 dBm.</p> </li> <li data-bbox="544 625 1487 808"> <p>• <b>Hysteresis</b>—Indicates how much greater the signal strength of a neighboring access point must be for the client to roam to it.</p> <p>This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.</p> <p>You can configure the hysteresis range from 3 through 20 dB and the default is 3 dB.</p> </li> <li data-bbox="544 835 1487 1144"> <p>• <b>Scan Threshold</b>—Indicates a minimum RSSI that is allowed before the client should roam to a better access point.</p> <p>When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold.</p> <p>You can configure the RSSI range from –50 through –90 dBm and the default value is –72 dBm.</p> </li> <li data-bbox="544 1171 1487 1501"> <p>• <b>Transition Time</b>—Indicates the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.</p> <p>The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.</p> <p>You can configure the time period in the range from 1 through 5 seconds and the default time is 5 seconds.</p> </li> </ul>
<b>Step 3</b>	<p><b>end</b></p> <p><b>Example:</b>  Switch(config)# end</p>	<p>Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>



# Configuring Mobility Oracle

## SUMMARY STEPS

1. `configure terminal`
2. `wireless mobility oracle`
3. `end`

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless mobility oracle</b>  <b>Example:</b> Switch(config)# <code>wireless mobility oracle</code>	Enables mobility oracle on the controller.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

# Configuring Mobility Controller

## SUMMARY STEPS

1. **configure terminal**
2. **wireless mobility controller**
3. **wireless mobility controller peer-group** *switch-peer-group-name*
4. **wireless mobility controller peer-group** *switch-peer-group-name* **member ip** *ip-address* {**public-ip** *public-ip-address*}
5. **wireless mobility controller peer-group** *switch-peer-group-name* **multicast**
6. **wireless mobility controller peer-group** *switch-peer-group-name* **multicast ip** *peer-group-multicast-ip-addr*
7. **wireless mobility controller peer-groups***switch-peer-group-name* **bridge-domain-id** *id*
8. **wireless mobility group member ip** *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*]
9. **wireless mobility dscp** *value*
10. **wireless mobility group keepalive** {*count* | *interval*}
11. **wireless mobility group name** *name*
12. **wireless mobility oracle ip***mo-ip-address*
13. **wireless management interface** *interface-name*
14. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless mobility controller</b>  <b>Example:</b> Switch(config)# <code>wireless mobility controller</code>	Enables wireless mobility controller.
<b>Step 3</b>	<b>wireless mobility controller peer-group</b> <i>switch-peer-group-name</i>  <b>Example:</b> Switch(config)# <code>wireless mobility controller peer-group SPG1</code>	Configures a switch peer group name. You can enter up to 31 case-sensitive ASCII printable characters for the group name. Spaces are not allowed in mobility group.  <b>Note</b> The <b>No</b> form of the command deletes the switch peer group.
<b>Step 4</b>	<b>wireless mobility controller peer-group</b> <i>switch-peer-group-name</i> <b>member ip</b> <i>ip-address</i> { <b>public-ip</b> <i>public-ip-address</i> }	Adds a mobility group member to a switch peer group.  <b>Note</b> The <b>No</b> form of the command deletes the member from the switch peer group.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.0.0.1</pre>	
<b>Step 5</b>	<p><b>wireless mobility controller peer-group</b> <i>switch-peer-group-name</i> <b>multicast</b></p> <p><b>Example:</b></p> <pre>Switch(config)# wireless mobility controller peer-group SPG1 multicast</pre>	Configures the multicast mode within a switch peer group.
<b>Step 6</b>	<p><b>wireless mobility controller peer-group</b> <i>switch-peer-group-name</i> <b>multicast ip</b> <i>peer-group-multicast-ip-addr</i></p> <p><b>Example:</b></p> <pre>Switch(config)# wireless mobility controller peer-group SPG1 multicast ip 10.0.0.4</pre>	Configures the multicast IP address for a switch peer group. <b>Note</b> The <b>No</b> form of the command deletes the multicast IP for the switch peer group.
<b>Step 7</b>	<p><b>wireless mobility controller</b> <b>peer-groups</b><i>switch-peer-group-name</i> <b>bridge-domain-id</b> <i>id</i></p> <p><b>Example:</b></p> <pre>Switch(config)# wireless mobility controller peer-group SPG bridge-domain-id 10.0.0.5</pre>	Configures the bridge domain ID for a switch peer group. The default is zero. <b>Note</b> The <b>No</b> form of command sets the bridge domain ID to the default value.
<b>Step 8</b>	<p><b>wireless mobility group member ip</b> <i>ip-address</i> [<b>public-ip</b> <i>public-ip-address</i>] [<b>group</b> <i>group-name</i>]</p> <p><b>Example:</b></p> <pre>Switch(config)# wireless mobility group member ip 10.0.0.1</pre>	Adds a mobility group member. <b>Note</b> The <b>No</b> form of the command removes the member from the group. The default group name is the group name of MC.
<b>Step 9</b>	<p><b>wireless mobility dscp</b> <i>value</i></p> <p><b>Example:</b></p> <pre>Switch(config)# wireless mobility dscp 46</pre>	Sets the DSCP value for mobility control packet. You can configure the DSCP value in a range from 0 through 63. The default value is 46.
<b>Step 10</b>	<p><b>wireless mobility group keepalive</b> {<i>count</i>   <i>interval</i>}</p> <p><b>Example:</b></p> <pre>Switch(config)# wireless mobility group keepalive count</pre>	Configures the wireless mobility group keepalive count which is the number of keepalive retries before a member status is termed DOWN and keepalive interval which is interval between two keepalives.
<b>Step 11</b>	<p><b>wireless mobility group name</b> <i>name</i></p> <p><b>Example:</b></p> <pre>Switch(config)# wireless mobility group name group1</pre>	Specifies the case sensitive wireless mobility group name which can be ASCII printable string up to 31 characters.

	Command or Action	Purpose
Step 12	<b>wireless mobility oracle ip</b> <i>ip-address</i>  <b>Example:</b> Switch(config)# wireless mobility oracle ip 10.0.0.5	Configures the mobility oracle IP address.
Step 13	<b>wireless management interface</b> <i>interface-name</i>  <b>Example:</b> Switch(config)# wireless management interface Vlan21	Configures the wireless management interface.
Step 14	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Mobility Agent

### SUMMARY STEPS

1. **configure terminal**
2. **wireless mobility controller ip** *ip-address*
3. **wireless mobility load-balance**
4. **wireless mobility load-balance threshold** *threshold -value*
5. **wireless management interface** *interface-name*
6. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>wireless mobility controller ip</b> <i>ip-address</i>  <b>Example:</b> Switch(config)# wireless mobility controller ip 10.10.10.20	Sets the IP address of the mobility controller.
Step 3	<b>wireless mobility load-balance</b>	Configures wireless mobility load balancing.

	Command or Action	Purpose
	<b>Example:</b> Switch(config)# wireless mobility load-balance	
<b>Step 4</b>	<b>wireless mobility load-balance threshold</b> <i>threshold -value</i>  <b>Example:</b> Switch(config)# wireless mobility load-balance threshold 100	Configures the number of clients that can be local or anchored on the MA. You can configure the threshold value in a range from 100 to 2000. The default value is 1000.
<b>Step 5</b>	<b>wireless management interface</b> <i>interface-name</i>  <b>Example:</b> Switch(config)# wireless management interface Vlan21	Configures wireless management interface for the mobility agent.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Monitoring Client Roaming Parameters

This section describes the new commands for the client parameters.

The following commands can be used to monitor the client roaming parameters on the switch.

**Table 14: Monitoring Client Roaming Parameters Commands**

Command	Purpose
<b>show ap dot11 {5ghz   24ghz} l2roam rf-param</b>	Displays the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network.
<b>show ap dot11 {5ghz   24ghz} l2roam statistics</b>	Displays the CCX Layer 2 client roaming statistics for the 802.11a or 802.11b/g network.
<b>show ap dot11 {5ghz   24ghz} l2roam mac-address <i>mac-address</i> statistics</b>	Displays the CCX Layer 2 client roaming statistics for a particular access point.

## Monitoring Mobility Configurations

This section describes the new commands for monitoring mobility configurations.

The following command can be used to monitor mobility configurations on the Mobility Oracle, Mobility Controller, and Mobility Agent.

**Table 15: Monitoring Mobility Configuration Commands on the Mobility Controller and Mobility Agent**

Command	Purpose
<b>show wireless mobility summary</b>	Displays the summary information for the Mobility Controller and Mobility Agent.
<b>show wireless mobility statistics</b>	Displays mobility statistics.
<b>show wireless mobility dtls connections</b>	Displays established DTLS connections.

**Table 16: Monitoring Mobility Configuration Commands on the Mobility Oracle**

Command	Purpose
<b>show wireless mobility oracle summary</b>	Displays the status of the Mobility Controllers known to the Mobility Oracle.
<b>show wireless mobility oracle client summary</b>	Displays the information of a list of clients in the Mobility Oracle database.
<b>show wireless mobility oracle client detail</b> <i>client -mac-address</i>	Displays the detailed information of a particular client in the Mobility Oracle database.
<b>show wireless mobility oracle</b> <i>mc-ip</i>	Displays the information of a list of clients in the Mobility Oracle database that are anchored or associated to a specified Mobility Controller.

**Table 17: Monitoring Mobility Configuration Commands on the Mobility Controller**

Command	Purpose
<b>show wireless mobility controller client summary</b>	Displays a list of clients in the subdomain.
<b>show wireless mobility controller client</b> <i>mac-address detail</i>	Displays detailed information for a client in a subdomain.
<b>show wireless mobility agent</b> <i>ma-ip client summary</i>	Displays a list of clients anchored or associated to a specified Mobility Agent.
<b>show wireless mobility ap-list</b>	Displays the list of Cisco APs known to the mobility group.

**Table 18: Monitoring Mobility Configuration Commands on the Mobility Agent**

Command	Purpose
<code>show wireless mobility load-balance summary</code>	Displays the summary of mobility load-balance properties.

## Additional References for Configuring Client Roaming

### Related Documents

Related Topic	Document Title
Mobility configuration	<i>Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>
Mobility-related commands	<i>Mobility Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

## Feature History and Information For Performing Client Roaming Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.





# CHAPTER 10

## Configuring Application Visibility and Control

- [Finding Feature Information, page 155](#)
- [Information About Application Visibility and Control, page 155](#)
- [Restrictions for Application Visibility and Control, page 156](#)
- [How to Configure Application Visibility and Control, page 157](#)
- [Monitoring Application Visibility and Control, page 158](#)
- [Examples: Application Visibility and Control, page 160](#)
- [Additional References for Application Visibility and Control, page 161](#)
- [Feature History and Information For Application Visibility and Control, page 162](#)

### Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### Information About Application Visibility and Control

Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition engine, and provides application-level visibility and control (QoS) in wireless networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or police the data traffic.

Using AVC, we can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.



**Note**

You can view list of 30 applications in Top Applications in Monitor Summary section of the UI.

**Note**

When you downgrade the controller from 8.0 to any earlier version, the AVC rate limit rules display the action as drop. This action is expected since the AVC rate limit rule is introduced in the controller version 8.0.

Cisco WLC Platform	Flow
Cisco 2504 WLC	26,250
Cisco 5508 WLC	183,750
Cisco WiSM2	393,750
Cisco 8510 WLC	336,000
Cisco 5520 WLC	336,000
Cisco 8540 WLC	336,000

## Restrictions for Application Visibility and Control

- AVC is supported only on the following access points:
  - Cisco Aironet 1260 Series Access Points
  - Cisco Aironet 1600 Series Access Points
  - Cisco Aironet 2600 Series Access Point
  - Cisco Aironet 2600 Series Wireless Access Points
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 3500 Series Access Points
  - Cisco Aironet 3600 Series Access Points
- AVC is not supported on Cisco Aironet 702W, 702I (128 M memory), and 1530 Series Access Points.
- Dropping or marking of the data traffic (control part) is not supported for software Release 3.3.
- Dropping or marking of the data traffic (control part) is supported in software Release 3E.
- Multicast traffic classification is not supported.
- Only the applications that are recognized with App visibility can be used for applying QoS control.
- IPv6 including ICMPv6 traffic classifications are not supported.
- Datalink is not supported for NetFlow fields for AVC.
- The following commands are not supported for AVC flow records:
  - **collect flow username**
  - **collect interface { input | output}**

- **collect wireless client ipv4 address**
  - **match interface { input | output}**
  - **match transport igmp type**
- The template timeout cannot be modified on exporters configured with AVC. Even if the template timeout value is configured to a different value, only the default value of 600 seconds is used.
  - For the username information in the AVC-based record templates, ensure that you configure the options **records** to get the user MAC address to username mapping.
  - The total number of flows for which downstream AVC QoS supported per client is 1000.
  - The maximum number of flows supported for Catalyst 3850 Series Switch is 48 K.
  - Google shares resources among several of their services because of which for some of the traffic it is not possible to say it is unique to one application. Therefore we added google-services for traffic that cannot be distinguished. The behavior you experience is expected.

# How to Configure Application Visibility and Control

## Configuring Application Visibility and Control (GUI)

### Configuring Application Visibility (GUI)

You can apply the default flow record (**wireless avc basic**) to the default flow monitor (**wireless-avc-basic**).

If you are using the flow record and flow monitor you have created, then the record name and monitor name should be same. This is specific only for configuring AVC from GUI and not for the CLI configuration.

You can use the flow monitor you have created either for upstream or downstream, or both, but ensure that you use the same record name while mapping with the flow monitor.

---

**Step 1** Choose **Configuration > Wireless > WLAN**.  
The **WLAN** page appears.

**Step 2** Click on the corresponding WLAN ID to open the **WLAN > Edit** page and click **AVC**.  
The **Application Visibility** page appears.

- a) Select the **Application Visibility Enabled** check box to enable AVC on a WLAN.
- b) In the **Upstream Profile** text box, enter the name of the AVC profile.
- c) In the **Downstream Profile** text box, enter the name of the AVC profile.

To enable AVC, you need to enter the profile names for the upstream and downstream profiles. The profile names are the flow monitor names. By default, the flow monitor names (**wireless-avc-basic**) appear in the **Upstream Profile** and **Downstream Profile** text boxes. For the default flow monitor, the default flow record (**wireless avc basic**) will be taken. The default flow record is generated by the system and is available.

You can change the profile names for the upstream and downstream profiles but ensure that the same flow records are available for the flow monitors.

The upstream and downstream profiles can have different profile names but there should be flow records available for the flow monitors.

**Step 3** Click **Apply** to apply AVC on the WLAN.

**Step 4** To disable AVC on a specific WLAN, perform the following steps:

- Choose **Configuration > Wireless > WLAN** to open the **WLAN** page.
- Click on the corresponding WLAN ID to open the **WLAN > Edit** page.
- Click **AVC** to open the **Application Visibility** page.
- Uncheck the **Application Visibility Enabled** check box.
- Click **Apply** to disable AVC on the specific WLAN.

## Monitoring Application Visibility and Control

### Monitoring Application Visibility and Control (CLI)

This section describes the new commands for application visibility.

The following commands can be used to monitor application visibility on the switch and access points.

**Table 19: Monitoring Application Visibility Commands on the switch**

Command	Purpose
<b>show avc client</b> <i>client-mac</i> <b>top n application</b> [aggregate   upstream   downstream]	Displays information about top "N" applications for the given client MAC.
<b>show avc wlan</b> <i>ssid</i> <b>top n application</b> [aggregate   upstream   downstream]	Displays information about top "N" applications for the given SSID.
<b>avc top user</b> [enable   disable]	Enables or disables the information about top "N" application.
<b>show avc wlan</b> <i>wlan-id</i> <b>application app name top N</b> [aggregate   upstream   downstream]	Displays to know network usage information on a per user basis within an application.  <b>Note</b> On Catalyst 4500E Supervisor Engine 8-E, in the information about top N users that is displayed, the client's MAC address and username are not displayed. This issue occurs only within 90 seconds after the client is disconnected.

<b>show wlan id</b> <i>wlan-id</i>	Displays information whether AVC is enabled or disabled on a particular WLAN.
<b>show flow monitor</b> <i>flow_monitor_name</i> <b>cache</b>	Displays information about flow monitors.
<b>show wireless client mac-address</b> <i>mac-address</i> <b>service-policy</b> { <b>input</b>   <b>output</b> }	Displays information about policy mapped to the wireless clients.

**Table 20: Clearing Application Visibility Statistics Commands**

Command	Purpose
<b>clear avc client</b> <i>mac stats</i>	Clears the statistics per client.
<b>clear avc wlan</b> <i>wlan-name stats</i>	Clears the statistics per WLAN.

## Monitoring Application Visibility and Control (GUI)

You can view AVC information on a WLAN in a single shot using a **AVC on WLAN** pie chart on the **Home** page of the switch. The pie chart displays the AVC data (Aggregate - Application Cumulative usage %) of the first WLAN. In addition, the top 5 WLANs based on clients are displayed first. Click on any one of the WLANs to view the corresponding pie chart information. If AVC is not enabled on the first WLAN, then the **Home** page does not display the AVC pie chart.

- 
- Step 1** Choose **Monitor > Controller > AVC > WLANs**.  
The **WLANs** page appears.
- Step 2** Click the corresponding WLAN profile.  
The **Application Statistics** page appears.
- From the **Top Applications** drop-down list, choose the number of top applications you want to view and click **Apply**. The valid range is between 5 to 30, in multiples of 5.
- a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:
- Application name
  - Packet count
  - Byte count
  - Average packet size
  - usage (%)
- Step 3** Choose **Monitor > Clients > Client Details > Clients**.  
The **Clients** page appears.

**Step 4** Click **Client MAC Address** and then click **AVC Statistics** tab.  
The **Application Visibility** page appears.

- a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:
- Application name
  - Packet count
  - Byte count
  - Average packet size
  - usage (%)

## Examples: Application Visibility and Control

### Examples: Application Visibility Configuration

This example shows how to create a flow record, create a flow monitor, apply the flow record to the flow monitor, and apply the flow monitor on a WLAN:

```
Switch# configure terminal
Switch(config)# flow record fr_v4
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# match flow direction
Switch(config-flow-record)# match application name
Switch(config-flow-record)# match wireless ssid
Switch(config-flow-record)# collect counter bytes long
Switch(config-flow-record)# collect counter packets long
Switch(config-flow-record)# collect wireless ap mac address
Switch(config-flow-record)# collect wireless client mac address
Switch(config)#end
```

```
Switch# configure terminal
Switch# flow monitor fm_v4
Switch(config-flow-monitor)# record fr_v4
Switch(config-flow-monitor)# cache timeout active 1800
Switch(config)#end
```

```
Switch(config)#wlan wlan1
Switch(config-wlan)#ip flow monitor fm_v4 input
Switch(config-wlan)#ip flow mon fm-v4 output
Switch(config)#end
```

# Additional References for Application Visibility and Control

## Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>
Flexible NetFlow configuration	<i>Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>
Flexible NetFlow commands	<i>Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>
QoS configuration	<i>QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)</i>
QoS commands	<i>QoS Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)</i>

## Standards and RFCs

Standard/RFC	Title
None	—

## MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

## Feature History and Information For Application Visibility and Control

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.
Cisco IOS XE 3E	AVC control with QoS was introduced.





## Configuring Voice and Video Parameters

---

- [Finding Feature Information, page 163](#)
- [Prerequisites for Voice and Video Parameters, page 163](#)
- [Restrictions for Voice and Video Parameters, page 164](#)
- [Information About Configuring Voice and Video Parameters, page 164](#)
- [How to Configure Voice and Video Parameters, page 169](#)
- [Monitoring Voice and Video Parameters, page 180](#)
- [Configuration Examples for Voice and Video Parameters, page 182](#)
- [Additional References for Voice and Video Parameters, page 184](#)
- [Feature History and Information For Performing Voice and Video Parameters Configuration, page 185](#)

### Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### Prerequisites for Voice and Video Parameters

You can confirm the following points before configuring voice and video parameters:

- Ensure that the switch has access points connected to it.
- Configure SSID.

## Restrictions for Voice and Video Parameters

The following are the restrictions that you should keep in mind while configuring voice and video parameters:

- SIP CAC can be used for the 9971 Cisco phones that support TSPEC-based admission control. You can also use the phones that support Status code 17.
- SIP snooping is supported for providing voice priority to the non-TSPEC SIP phones.
- TSPEC for video CAC is not supported.
- Cisco 792x IP phones that are admitted as non-WMM devices with 11K enabled will experience audio problems with the phones.




---

**Note** Disable 11K for voice WLAN for all 792x Cisco IP phones that are admitted as non-WMM devices with 11K enabled. Upgrade the firmware on Cisco Unified Call Manager to 1.4.5 to resolve this issue. Refer to the Cisco Unified Call Manager configuration guide for more information.

---

## Information About Configuring Voice and Video Parameters

Three parameters on the switch affect voice and/or video quality:

- Call Admission Control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

Call Admission Control (CAC) and UAPSD are supported on Cisco Compatible Extensions (CCX) v4 and v5; however, these parameters are also supported even without CCX but on any device implementing WMM (that supports 802.1e). Expedited bandwidth requests are supported only on CCXv5.

Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.

## Call Admission Control

Call Admission Control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The WMM protocol deployed in CCXv4 maintains QoS under differing network loads.

Two types of Over The Air (OTA) CAC are available: static-based CAC and load-based CAC.

The switch supports the following QoS policies:

- User-defined policies: You can define your own QoS policies. You can have more control over these policies than the existing metal policies.
- System-defined precious metal policies: To support backward compatibility.
  - Platinum: Used for VoIP clients.

- Gold: Used for video clients.
- Silver: Used for best effort traffic.
- Bronze: Used for NRT traffic.

## Static-Based CAC

Voice over WLAN applications supporting WMM and TSPEC can specify how much bandwidth or shared medium time is required to initiate a call. Bandwidth-based, or static, CAC enables the access point to determine whether it is capable of accommodating a particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

The QoS setting for a WLAN determines the level of bandwidth-based CAC support. To use bandwidth-based CAC with voice applications, the WLAN must be configured for Platinum QoS. With bandwidth-based CAC, the access point bandwidth availability is determined based on the amount of bandwidth currently used by the access point clients, to which the bandwidth requested by the Voice over WLAN applications is added. If this total exceeds a configured bandwidth threshold, the new call is rejected.

**Note**

---

You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly for these CCXv4 clients.

---

## Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types (including that from clients), cochannel access point loads, and coallocated channel interference, for voice and video applications. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point continuously measures and updates the utilization of the RF channel (that is, the mean time of bandwidth that has been exhausted), channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

**Note**

---

If you disable load-based CAC, the access points start using bandwidth-based CAC.

---

# IOSd Call Admission Control

IOSd Call Admission Control (CAC) controls bandwidth availability from switch to access point.

You can configure class-based, unconditional packet marking features on your switch for CAC.

CAC is a concept that applies to voice and video traffic only—not data traffic. If an influx of data traffic oversubscribes a particular link in the network, queuing, buffering, and packet drop decisions resolve the congestion. The extra traffic is simply delayed until the interface becomes available to send the traffic, or, if

traffic is dropped, the protocol or the end user initiates a timeout and requests a retransmission of the information.

Network congestion cannot be resolved in this manner when real-time traffic, sensitive to both latency and packet loss, is present, without jeopardizing the quality of service (QoS) expected by the users of that traffic. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion conditions than to allow traffic onto the network to be dropped and delayed, causing intermittent impaired QoS and resulting in customer dissatisfaction.

CAC is therefore a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call.

Based on the admit CAC CLI configuration in addition to the existing CAC algorithm, switch allows either voice or video with TSPEC or SIP snooping. The **admit cac** CLI is mandatory for the voice call to pass through.

If the BSSID policer is configured for the voice or video traffic, then additional checks are performed on the packets.

## Expedited Bandwidth Requests

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both bandwidth-based and load-based CAC. Expedited bandwidth requests are disabled by default. When this feature is disabled, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

The following table lists examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

Table 21: TSPEC Request Handling Examples

CAC Mode	Reserved bandwidth for voice calls <sup>3</sup>	Usage <sup>4</sup>	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Bandwidth-based CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 85% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 85%	Rejected	Rejected

<sup>3</sup> For bandwidth-based CAC, the voice call bandwidth usage is per access point radio and does not take into account cochannel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.

<sup>4</sup> Bandwidth-based CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

**Note**

Admission control for TSPEC G711-20ms and G711-40 ms codec types are supported.

## U-APSD

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

## Traffic Stream Metrics

In a voice-over-wireless LAN (VoWLAN) deployment, traffic stream metrics (TSM) can be used to monitor voice-related metrics on the client-access point air interface. It reports both packet latency and packet loss. You can isolate poor voice quality issues by studying these reports.

The metrics consist of a collection of uplink (client side) and downlink (access point side) statistics between an access point and a client device that supports CCX v4 or later releases. If the client is not CCX v4 or CCXv5 compliant, only downlink statistics are captured. The client and access point measure these metrics. The access

point also collects the measurements every 5 seconds, prepares 90-second reports, and then sends the reports to the controller. The controller organizes the uplink measurements on a client basis and the downlink measurements on an access point basis and maintains an hour's worth of historical data. To store this data, the controller requires 32 MB of additional memory for uplink metrics and 4.8 MB for downlink metrics.

TSM can be configured through either the GUI or the CLI on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

This table shows the upper limit for TSM entries in different controller series.

TSM Entries	5700
MAX AP TSM entries	100
MAX Client TSM entries	250
MAX TSM entries	100*250=25000

**Note**

Once the upper limit is reached, additional TSM entries cannot be stored and sent to WCS or NCS. If client TSM entries are full and AP TSM entries are available, then only the AP entries are stored, and viceversa. This leads to partial output. TSM cleanup occurs every one hour. Entries are removed only for those APs and clients that are not in the system.

## Information About Configuring Voice Prioritization Using Preferred Call Numbers

You can configure a switch to provide support for SIP calls from VoWLAN clients that do not support TSPEC-based calls. This feature is known as SIP CAC support. If bandwidth is available in the configured voice pool, the SIP call uses the normal flow and the switch allocates the bandwidth to those calls.

You can also prioritize up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the switch does not check the configured maximum voice bandwidth. The switch allocates the bandwidth needed for the call, even if it exceeds the maximum bandwidth for voice configured for voice CAC. The preferred call will be rejected if bandwidth allocation exceeds 85% of the radio bandwidth. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

You must configure the following parameters before configuring voice prioritization:

- Set WLAN QoS to allow voice calls to pass through.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

## Information About EDCA Parameters

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

# How to Configure Voice and Video Parameters

## Configuring Voice Parameters (CLI)

### Before You Begin

Ensure that you have configured SIP-based CAC.

You should have created a class map for CAC before beginning this procedure.

### SUMMARY STEPS

1. **show wlan summary**
2. **show wlan** *wlan\_id*
3. **configure terminal**
4. **policy-map** *policy-map name*
5. **class** {*class-name* | **class-default**}
6. **admit cac wmm-tspec**
7. **service-policy** *policy-map name*
8. **end**
9. **wlan** *wlan\_profile\_name wlan\_ID SSID\_network\_name* **wlan shutdown**
10. **wlan** *wlan\_profile\_name wlan\_ID SSID\_network\_name*
11. **wlan** *wlan\_name* **call-snoop**
12. **wlan** *wlan\_name* **service-policy input** *input\_policy\_name*
13. **wlan** *wlan\_name* **service-policy output** *ouput\_policy\_name*
14. **wlan** *wlan\_name* **service-policy input** *ingress\_policy\_name*
15. **wlan** *wlan\_name* **service-policy output** *egress\_policy\_name*
16. **ap dot11** {*5ghz* | *24ghz*} **shutdown**
17. **ap dot11** {*5ghz* | *24ghz*} **cac voice sip**
18. **ap dot11** {*5ghz* | *24ghz*} **cac voice acm**
19. **ap dot11** {*5ghz* | *24ghz*} **cac voice max-bandwidth** *bandwidth*
20. **ap dot11** {*5ghz* | *24ghz*} **cac voice roam-bandwidth** *bandwidth*
21. **no wlan shutdown**
22. **no ap dot11** {*5ghz* | *24ghz*} **shutdown**
23. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>show wlan summary</b>  <b>Example:</b> Switch# <b>show wlan summary</b>	Specifies all of the WLANs configured on the switch.
Step 2	<b>show wlan wlan_id</b>  <b>Example:</b> Switch# <b>show wlan 25</b>	Specifies the WLAN that you plan to modify. For voice over WLAN, ensure that the WLAN is configured for WMM and the QoS level is set to Platinum.
Step 3	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 4	<b>policy-map policy-map name</b>  <b>Example:</b> Switch(config)# <b>policy-map test_2000</b> Switch(config-pmap)#	Enters policy map configuration mode.  Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.  In WLAN, you need to configure service-policy for these commands to take effect.
Step 5	<b>class {class-name   class-default}</b>  <b>Example:</b> Switch(config-pmap)# <b>class test_1000</b> Switch(config-pmap-c)#	Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.  Specifies the name of the class whose policy you want to create or change.  You can also create a system default class for unclassified packets.
Step 6	<b>admit cac wmm-tspec</b>  <b>Example:</b> Switch(config-pmap-c)# <b>admit cac wmm-tspec</b> Switch(config-pmap-c)#	(Optional) Admits the request for Call Admission Control (CAC) for policy map.
Step 7	<b>service-policy policy-map name</b>  <b>Example:</b> Switch(config-pmap-c)# <b>service-policy test_2000</b> Switch(config-pmap-c)#	Configures the QoS service policy.
Step 8	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
Step 9	<b>wlan wlan_profile_name wlan_ID SSID_network_name wlan shutdown</b>	Disables all WLANs with WMM enabled prior to changing the video parameters.



	Command or Action	Purpose
	<b>Example:</b> Switch(config)# wlan wlan1 Switch(config-wlan)# wlan shutdown	
<b>Step 10</b>	<b>wlan wlan_profile_name wlan_ID SSID_network_name</b>  <b>Example:</b> Switch(config)# wlan wlan1 Switch(config-wlan)# wlan shutdown	Disables all WLANs with WMM enabled prior to changing the voice parameters.
<b>Step 11</b>	<b>wlan wlan_name call-snoop</b>  <b>Example:</b> Switch(config)# wlan wlan1 call-snoop	Enables the call-snooping on a particular WLAN.
<b>Step 12</b>	<b>wlan wlan_name service-policy input input_policy_name</b>  <b>Example:</b> Switch(config)# wlan wlan1 Switch(config-wlan)# service-policy input platinum-up	Configures input SSID policy on a particular WLAN to voice.
<b>Step 13</b>	<b>wlan wlan_name service-policy output output_policy_name</b>  <b>Example:</b> Switch(config)# wlan wlan1 Switch(config-wlan)# service-policy output platinum	Configures output SSID policy on a particular WLAN to voice.
<b>Step 14</b>	<b>wlan wlan_name service-policy input ingress_policy_name</b>  <b>Example:</b> Switch(config)# wlan wlan1 Switch(config-wlan)# service-policy input policy1	Configures ingress SSID policy on a particular WLAN as user-defined policy.
<b>Step 15</b>	<b>wlan wlan_name service-policy output egress_policy_name</b>  <b>Example:</b> Switch(config)# wlan wlan1 Switch(config-wlan)# service-policy output policy2	Configures egress SSID policy on a particular WLAN as user-defined policy.
<b>Step 16</b>	<b>ap dot11 {5ghz   24ghz} shutdown</b>  <b>Example:</b>	Disables the radio network.  Switch(config)# ap dot11 5ghz shutdown

	Command or Action	Purpose
<b>Step 17</b>	<b>ap dot11 {5ghz   24ghz} cac voice sip</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac voice sip</b>	Enables or disables SIP IOSd CAC for the 802.11a or 802.11b/g network.
<b>Step 18</b>	<b>ap dot11 {5ghz   24ghz} cac voice acm</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac voice acm</b>	Enables or disables bandwidth-based voice CAC for the 802.11a or 802.11b/g network.
<b>Step 19</b>	<b>ap dot11 {5ghz   24ghz} cac voice max-bandwidth bandwidth</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac voice max-bandwidth 85</b>	<p>Sets the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network.</p> <p>The bandwidth range is 5 to 85%, and the default value is 75%. Once the client reaches the value specified, the access point rejects new videos on this network.</p>
<b>Step 20</b>	<b>ap dot11 {5ghz   24ghz} cac voice roam-bandwidth bandwidth</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac voice roam-bandwidth 10</b>	<p>Sets the percentage of maximum allocated bandwidth reserved for roaming voice clients.</p> <p>The bandwidth range is 0 to 25%, and the default value is 6%. The switch reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.</p>
<b>Step 21</b>	<b>no wlan shutdown</b>  <b>Example:</b> Switch(config-wlan)# <b>no wlan shutdown</b>	Reenables all WLANs with WMM enabled.
<b>Step 22</b>	<b>no ap dot11 {5ghz   24ghz} shutdown</b>  <b>Example:</b> Switch(config)# <b>no ap dot11 5ghz shutdown</b>	Reenables the radio network.
<b>Step 23</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Video Parameters (CLI)

### SUMMARY STEPS

1. `show wlan summary`
2. `show wlan wlan_id`
3. `configure terminal`
4. `policy-map policy-map name`
5. `class {class-name | class-default}`
6. `admit cac wmm-tspec`
7. `service-policy policy-map name`
8. `end`
9. `wlan wlan_profile_name`
10. `ap dot11 {5ghz | 24ghz} shutdown`
11. `ap dot11 {5ghz | 24ghz} cac video acm`
12. `ap dot11 {5ghz | 24ghz} cac video load-based`
13. `ap dot11 {5ghz | 24ghz} cac video max-bandwidth bandwidth`
14. `ap dot11 {5ghz | 24ghz} cac video roam-bandwidth bandwidth`
15. `no wlan shutdown wlan_id`
16. `no ap dot11 {5ghz | 24ghz} shutdown`
17. `end`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>show wlan summary</code>  <b>Example:</b> Switch# <code>show wlan summary</code>	Specifies all of the WLANs configured on the switch.
Step 2	<code>show wlan <i>wlan_id</i></code>  <b>Example:</b> Switch# <code>show wlan 25</code>	Specifies the WLAN that you plan to modify.
Step 3	<code>configure terminal</code>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
Step 4	<code>policy-map <i>policy-map name</i></code>  <b>Example:</b> Switch(config)# <code>policy-map test_2000</code> Switch(config-pmap)#	Enters policy map configuration mode.  Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.  In WLAN, you need to configure service-policy for these commands to take effect.

	Command or Action	Purpose
<b>Step 5</b>	<b>class</b> <i>{class-name   class-default}</i>  <b>Example:</b> Switch(config-pmap)# <b>class test_1000</b> Switch(config-pmap-c)#	Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.  Specifies the name of the class whose policy you want to create or change.  You can also create a system default class for unclassified packets.
<b>Step 6</b>	<b>admit cac wmm-tspec</b>  <b>Example:</b> Switch(config-pmap-c)# <b>admit cac wmm-tspec</b> Switch(config-pmap-c)#	(Optional) Admits the request for Call Admission Control (CAC) for policy map.
<b>Step 7</b>	<b>service-policy</b> <i>policy-map name</i>  <b>Example:</b> Switch(config-pmap-c)# <b>service-policy test_2000</b> Switch(config-pmap-c)#	Configures the QoS service policy.
<b>Step 8</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
<b>Step 9</b>	<b>wlan</b> <i>wlan_profile_name</i>  <b>Example:</b> Switch(config)# <b>wlan wlan1</b> Switch(config-wlan)# <b>wlan shutdown</b>	Disables all WLANs with WMM enabled prior to changing the video parameters.
<b>Step 10</b>	<b>ap dot11 {5ghz   24ghz} shutdown</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz shutdown</b>	Disables the radio network.
<b>Step 11</b>	<b>ap dot11 {5ghz   24ghz} cac video acm</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac video acm</b>	Enables or disables bandwidth-based video CAC for the 802.11a or 802.11b/g network.
<b>Step 12</b>	<b>ap dot11 {5ghz   24ghz} cac video load-based</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac video load-based</b>	Configures the load-based CAC method.  If you do not enter this command, then the default static CAC is applied.
<b>Step 13</b>	<b>ap dot11 {5ghz   24ghz} cac video max-bandwidth</b> <i>bandwidth</i>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac video max-bandwidth 20</b>	Sets the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network.  The bandwidth range is 5 to 85%, and the default value is 75%. The default value is 0, which means no bandwidth request control. The sum of the voice bandwidth and video bandwidth

	Command or Action	Purpose
		should not exceed 85% or configured maximum media bandwidth.
<b>Step 14</b>	<b>ap dot11 {5ghz   24ghz} cac video roam-bandwidth <i>bandwidth</i></b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac video roam-bandwidth 9</b>	Sets the percentage of maximum allocated bandwidth reserved for roaming clients for video.  The bandwidth range is 0 to 25%, and the default value is 0%.
<b>Step 15</b>	<b>no wlan shutdown <i>wlan_id</i></b>  <b>Example:</b> Switch(config-wlan)# <b>no wlan shutdown 25</b>	Reenables all WLANs with WMM enabled.
<b>Step 16</b>	<b>no ap dot11 {5ghz   24ghz} shutdown</b>  <b>Example:</b> Switch(config)# <b>no ap dot11 5ghz shutdown</b>	Reenables the radio network.
<b>Step 17</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring SIP-Based CAC (CLI)

SIP CAC controls the total number of SIP calls that can be made.

### SUMMARY STEPS

1. **configure terminal**
2. **wlan *wlan-name***
3. **call-snoop**
4. **service-policy [client] input *policy-map name***
5. **service-policy [client] output *policy-map name***
6. **end**
7. **show wlan {*wlan-id* | *wlan-name*}**
8. **configure terminal**
9. **ap dot11 {5ghz | 24ghz} cac {voice | video} acm**
10. **ap dot11 {5ghz | 24ghz} cac voice sip**
11. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>wlan wlan-name</b>  <b>Example:</b> Switch(config)# <b>wlan qos-wlan</b> Switch(config-wlan)#	Enters WLAN configuration submode.
Step 3	<b>call-snoop</b>  <b>Example:</b> Switch(config-wlan)# <b>call-snoop</b>	Enables the call-snooping feature for a particular WLAN.
Step 4	<b>service-policy [client] input policy-map name</b>  <b>Example:</b> Switch(config-wlan)# <b>service-policy input platinum-up</b>	Assigns a policy map to WLAN input traffic. Ensure that you provide QoS policy to voice for input traffic.
Step 5	<b>service-policy [client] output policy-map name</b>  <b>Example:</b> Switch(config-wlan)# <b>service-policy output platinum</b>	Assigns policy map to WLAN output traffic. Ensure that you provide QoS policy to voice for output traffic.
Step 6	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.
Step 7	<b>show wlan {wlan-id   wlan-name}</b>  <b>Example:</b> Switch# <b>show wlan qos-wlan</b>	Verifies the configured QoS policy on the WLAN.
Step 8	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 9	<b>ap dot11 {5ghz   24ghz} cac {voice   video} acm</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac voice acm</b>	Enables the ACM static on the radio.  When enabling SIP snooping, use the static CAC, not the load-based CAC.
Step 10	<b>ap dot11 {5ghz   24ghz} cac voice sip</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac voice sip</b>	Configures SIP-based CAC.

	Command or Action	Purpose
Step 11	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring a Preferred Call Number (CLI)

### Before You Begin

You must set the following parameters before configuring a preferred call number.

- Set WLAN QoS to voice.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.
- Enable SIP-based CAC.

### SUMMARY STEPS

1. **configure terminal**
2. **wlan *wlan-name* qos platinum**
3. **ap dot11 {5ghz | 24ghz} cac {voice | video} acm**
4. **wlan *wlan-name***
5. **wireless sip preferred-call-no *call\_index call\_number***
6. **no wireless sip preferred-call-no *call\_index***
7. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>wlan <i>wlan-name</i> qos platinum</b>  <b>Example:</b> Switch(config)# <b>wlan wlan1</b> Switch(config-wlan)# <b>qos platinum</b>	Sets QoS to voice on a particular WLAN.
Step 3	<b>ap dot11 {5ghz   24ghz} cac {voice   video} acm</b>	Enables the static ACM on the radio.

	Command or Action	Purpose
	<b>Example:</b> Switch(config)# <b>ap dot11 5ghz cac voice acm</b>	When enabling SIP snooping, use the static CAC, not the load-based CAC.
<b>Step 4</b>	<b>wlan wlan-name</b>  <b>Example:</b> Switch(config)# <b>wlan wlan1</b> Switch(config-wlan)# <b>call-snoop</b>	Enables the call-snooping feature for a particular WLAN.
<b>Step 5</b>	<b>wireless sip preferred-call-no call_index call_number</b>  <b>Example:</b> Switch(config)# <b>wireless sip preferred-call-no 1 555333</b>	Adds a new preferred call.
<b>Step 6</b>	<b>no wireless sip preferred-call-no call_index</b>  <b>Example:</b> Switch(config)# <b>no wireless sip preferred-call-no 1</b>	Removes a preferred call.
<b>Step 7</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring EDCA Parameters (CLI)

### SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz} shutdown**
3. **ap dot11 {5ghz | 24ghz} edca-parameters {custom-voice | fastlane | optimized-video-voice | optimized-voice | svp-voice | wmm-default}**
4. **no ap dot11 {5ghz | 24ghz} shutdown**
5. **end**
6. **show ap dot11 {5ghz | 24ghz} network**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>ap dot11 {5ghz   24ghz } shutdown</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz shutdown</b>	Disables the radio network.
Step 3	<b>ap dot11 {5ghz   24ghz} edca-parameters {custom-voice   fastlane   optimized-video-voice   optimized-voice   svp-voice   wmm-default}</b>  <b>Example:</b> Switch(config)# <b>ap dot11 5ghz edca-parameters optimized-voice</b>	Enables a specific EDCA parameters for the 802.11a or 802.11b/g network. <ul style="list-style-type: none"> <li>• custom-voice—Enables custom voice parameters for the 802.11a or 802.11b/g network.</li> <li>• fastlane—Enables fastlane parameters for the 802.11a or 802.11b/g network.</li> <li>• optimized-video-voice—Enables EDCA voice- and video-optimized parameters for the 802.11a or 802.11b/g network. Choose this option when both voice and video services are deployed on your network.</li> <li>• optimized-voice—Enables non-SpectraLink voice-optimized profile parameters for the 802.11a or 802.11b/g network. Choose this option when voice services other than SpectraLink are deployed on your network.</li> <li>• svp-voice—Enables SpectraLink voice priority parameters for the 802.11a or 802.11b/g network. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.</li> <li>• wmm-default—Enables the Wi-Fi Multimedia (WMM) default parameters for the 802.11a or 802.11b/g network. This is the default option. Choose this option when voice or video services are not deployed on your network.</li> </ul>
Step 4	<b>no ap dot11 {5ghz   24ghz} shutdown</b>  <b>Example:</b> Switch(config)# <b>no ap dot11 5ghz shutdown</b>	Re-enables the radio network.
Step 5	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.

	Command or Action	Purpose
<b>Step 6</b>	<b>show ap dot11 {5ghz   24ghz} network</b>  <b>Example:</b> Switch# <b>show ap dot11 5ghz network</b>	Displays the current status of MAC optimization for voice.

## Monitoring Voice and Video Parameters

This section describes the new commands for the voice and video parameters.

The following commands can be used to monitor voice and video parameters.

**Table 22: Monitoring Voice Parameters Commands**

Command	Purpose
<b>show ap dot11 {5ghz   24ghz} network</b>	Displays the radio-based statistics for voice.
<b>show ap name <i>ap_name</i> dot11 24ghz tsm all</b>	Displays the TSM voice metrics and current status of MAC optimization for voice.
<b>show ap name <i>apname</i> cac voice</b>	Displays the information about CAC for a particular access point.
<b>show client detail <i>client_mac</i></b>	Displays the U-APSD status for a particular client.
<b>show policy-map interface wireless client</b>	Displays the video client policy details.
<b>show access-list</b>	Displays the video client dynamic access-list from the switch.
<b>show wireless client voice diag status</b>	<p>Displays information about whether voice diagnostics are enabled or disabled. If enabled, this also displays information about the clients in the watch list and the time remaining for the diagnostics of the voice call.</p> <p><b>Note</b> To work on voice diagnostics CLIs, you need to enter the following command: <b>debug voice-diagnostic mac-addr <i>client_mac_01</i> <i>client_mac_02</i></b></p>
<b>show wireless client voice diag tspec</b>	Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.

<b>show wireless client voice diag qos-map</b>	Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
<b>show wireless client voice diag rssi</b>	Display the client's RSSI values in the last 5 seconds when voice diagnostics is enabled.
<b>show client voice-diag roam-history</b>	Displays information about the last three roaming calls. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, reason for roaming-failure.
<b>show policy-map interface wireless mac</b> <i>mac-address</i>	Displays information about the voice and video data packet statistics.
<b>show wireless media-stream client summary</b>	Displays a summary of the media stream and video client information.
<b>show controllers d0   b queue</b>	Displays which queue the packets are going through on an access point.
<b>show platform qos queue stats</b> <i>interface</i>	Displays which queue packets are going through from the switch.

You can monitor the video parameters using the following commands.

**Table 23: Monitoring Video Parameters Commands**

<b>Command</b>	<b>Purpose</b>
<b>show ap join stats summary</b> <i>ap_mac</i>	Displays the last join error detail for a specific access point.
<b>show ip igmp snooping wireless mgid</b>	Displays the TSM voice metrics and current status of MAC optimization for voice.
<b>show wireless media-stream multicast-direct state</b>	Displays the media stream multicast-direct parameters.
<b>show wireless media-stream group summary</b>	Displays the summary of the media stream and client information.
<b>show wireless media-stream group detail</b> <i>group_name</i>	Displays the details of a specific media-stream group.
<b>show wireless media-stream client summary</b>	Displays the details for a set of media-stream clients.

<b>show wireless media-stream client detail</b> <i>group_name</i>	Displays the details for a set of media-stream clients.
<b>show ap dot11 {5ghz   24ghz} media-stream rrc</b>	Display the details of media stream.
<b>show wireless media-stream message details</b>	Displays information about the message configuration.
<b>show ap name <i>ap-name</i> auto-rf dot11 5ghz   i Util</b>	Displays the details of channel utilization.
<b>show controllers d0   b queue</b>	Displays which queue the packets are going through on an access point based on 2.4- and 5-GHz bands.
<b>show controllers d1   b queue</b>	Displays which queue the packets are going through on an access point based on 2.4- and 5-GHz bands.
<b>show cont d1   b Media</b>	Displays the video metric details on the band A or B.
<b>show capwap mcast mgid all</b>	Displays information about all of the multicast groups and their corresponding multicast group identifications (MGIDs) associated to the access point.
<b>show capwap mcast mgid id <i>id</i></b>	Displays information about all of the video clients joined to the multicast group in a specific MGID.

## Configuration Examples for Voice and Video Parameters

### Example: Configuring Voice and Video

#### Configuring Egress SSID Policy for Voice and Video

The following example shows how to create and configure an egress SSID policy for voice and video:

```

table-map egress_ssid_tb
  map from 24 to 24
  map from 34 to 34
  map from 46 to 46
  default copy

class-map match-any voice
  match dscp ef
class-map match-any video
  match dscp af41

policy-map ssid-cac
class class-default
  shape average 25000000
  set dscp dscp table egress_ssid_tb
  queue-buffers ratio 0
  service-policy ssid-child-cac

policy-map ssid-child-cac
class voice
  priority level 1

```

```
    police 5000000
      conform-action transmit
      exceed-action drop
      admit cac wmm-tspec
      rate 1000
      wlan-up 6 7
  class video
    priority level 2
    police 10000000
      conform-action transmit
      exceed-action drop
      admit cac wmm-tspec
      rate 3000
      wlan-up 4 5
```

### Configuring Ingress SSID Policy for Voice and Video

The following example shows how to create and configure an ingress SSID policy for voice and video:

```
table-map up_to_dscp
  map from 0 to 0
  map from 1 to 8
  map from 2 to 8
  map from 3 to 0
  map from 4 to 34
  map from 5 to 34
  map from 6 to 46
  map from 7 to 48
  default copy

policy-map ingress_ssid
  class class-default
    set dscp wlan user-priority table up_to_dscp
```

### Configuring Egress Port Policy Voice and Video

The following example shows how to create and configure an egress port policy for voice and video:

```
policy-map port_child_policy
  class non-client-nrt-class
    bandwidth remaining ratio 10

  class voice
    priority level 1
    police rate 3000000

  class video
    priority level 2
    police rate 4000000
```

### Applying Ingress and Egress SSID policies for Voice and Video on a WLAN

The following example shows how to apply ingress and egress SSID policies for voice and video on a WLAN:

```
wlan voice_video 1 voice_video
  service-policy input ingress_ssid
  service-policy output ssid-cac
```

## Additional References for Voice and Video Parameters

### Related Documents

Related Topic	Document Title
Multicast configuration	<i>Multicast Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>
VideoStream configuration	<i>VideoStream Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information For Performing Voice and Video Parameters Configuration

Release	Feature Information
Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE	This feature was introduced.







## Configuring RFID Tag Tracking

---

- [Finding Feature Information, page 187](#)
- [Information About Configuring RFID Tag Tracking, page 187](#)
- [How to Configure RFID Tag Tracking, page 188](#)
- [Monitoring RFID Tag Tracking Information, page 189](#)
- [Additional References RFID Tag Tracking, page 189](#)
- [Feature History and Information For Performing RFID Tag Tracking Configuration , page 190](#)

### Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### Information About Configuring RFID Tag Tracking

The Switch enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the location appliance.

# How to Configure RFID Tag Tracking

## Configuring RFID Tag Tracking (CLI)

### SUMMARY STEPS

1. `location rfid status`
2. (Optional) `no location rfid status`
3. `location rfid timeout seconds`
4. `location rfid mobility vendor-name name`
5. (Optional) `no location rfid mobility name`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<code>location rfid status</code>  <b>Example:</b> <code>Switch(config)# location rfid status</code>	Enables RFID tag tracking.  By default, RFID tag tracking is enabled.
<b>Step 2</b>	(Optional) <code>no location rfid status</code>  <b>Example:</b> <code>Switch(config)# no location rfid status</code>	Disables RFID tag tracking.
<b>Step 3</b>	<code>location rfid timeout seconds</code>  <b>Example:</b> <code>Switch(config)# location rfid timeout 1500</code>	Specifies a static timeout value (between 60 and 7200 seconds).  The static timeout value is the amount of time that the switch maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.
<b>Step 4</b>	<code>location rfid mobility vendor-name name</code>  <b>Example:</b> <code>Switch(config)# location rfid mobility vendor-name Aerosct</code>	Enables RFID tag mobility for specific tags. When you enter the <b>location rfid mobility vendor-name</b> command, tags are unable to obtain a DHCP address for client mode when attempting to select and/or download a configuration.  <b>Note</b> These commands can be used only for Pango tags. Therefore, the only valid entry for <b>vendor_name</b> is “pango” in all lowercase letters.
<b>Step 5</b>	(Optional) <code>no location rfid mobility name</code>  <b>Example:</b> <code>Switch(config)# no location rfid mobility test</code>	Disables RFID tag mobility for specific tags. When you enter the <b>no location rfid mobility</b> command, tags can obtain a DHCP address. If a tag roams from one subnet to another, it obtains a new address rather than retaining the anchor state.

## Monitoring RFID Tag Tracking Information

This section describes the new commands for the RFID tag tracking Information.

The following commands can be used to monitor the RFID tag tracking Information on the switch.

**Table 24: Monitoring RFID Tag Tracking Information Commands**

Command	Purpose
<code>show location rfid config</code>	Displays the current configuration for RFID tag tracking.
<code>show location rfid detail mac_address</code>	Displays the detailed information for a specific RFID tag.
<code>show location rfid summary</code>	Displays a list of all RFID tags currently connected to the switch.
<code>show location rfid client</code>	Displays a list of RFID tags that are associated to the switch as clients.

## Additional References RFID Tag Tracking

### Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

**MIBs**

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information For Performing RFID Tag Tracking Configuration

Release	Feature Information
Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE	This feature was introduced.



## Configuring Location Settings

---

- [Finding Feature Information, page 191](#)
- [Information About Configuring Location Settings, page 191](#)
- [How to Configure Location Settings, page 192](#)
- [Monitoring Location Settings and NMSP Settings, page 196](#)
- [Examples: Location Settings Configuration, page 197](#)
- [Examples: NMSP Settings Configuration, page 197](#)
- [Additional References for Location Settings, page 198](#)
- [Feature History and Information For Performing Location Settings Configuration, page 199](#)

### Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### Information About Configuring Location Settings

The switch determines the location of client devices by gathering Received Signal Strength Indication (RSSI) measurements from access points all around the client of interest. The switch can obtain location reports from up to 16 access points for clients, RFID tags, and rogue access points.

You can configure the path loss measurement (S60) request for normal clients or calibrating clients to improve location accuracy.

# How to Configure Location Settings

## Configuring Location Settings (CLI)

### SUMMARY STEPS

1. `configure terminal`
2. `location plm {calibrating [multiband | uniband] | client burst_interval}`
3. `location rssi-half-life {calibrating-client | client | rogue-aps | tags } seconds}`
4. `location expiry {calibrating-client | client | rogue-aps | tags } timeout}`
5. `location algorithm {rssi-average | simple}`
6. `location admin-tag string}`
7. `location civic-location identifier {identifier | host}`
8. `location custom-location identifier {identifier | host}`
9. `location geo-location identifier {identifier | host}`
10. `location prefer {cdp | lldp-med | static} weight priority_value}`
11. `location rfid {status | timeout | vendor-name}`
12. `end`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>configure terminal</code></p> <p><b>Example:</b> Switch# <code>configure terminal</code></p>	Enters global configuration mode.
Step 2	<p><code>location plm {calibrating [multiband   uniband]   client <i>burst_interval</i>}</code></p> <p><b>Example:</b> Switch(config)# <code>location plm client 100</code></p>	<p>Configures the path loss measurement (S60) request for calibrating clients or non-calibrating.</p> <p>The path loss measurement request improves the location accuracy. You can configure the <b>burst_interval</b> parameter for the normal, noncalibrating client from zero through 3600 seconds, and the default value is 60 seconds.</p> <p>You can configure the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a/b/g radio.</p> <p>If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The <b>location plm</b> command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the Switch sends it a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1, 6, and 11 for 2.4-GHz-only access points) at a configurable interval (such as 60 seconds) indefinitely.</p>

	Command or Action	Purpose
Step 3	<p><b>location rssi-half-life</b> {<i>calibrating-client</i>   <i>client</i>   <i>rogue-aps</i>   <i>tags</i>} <i>seconds</i></p> <p><b>Example:</b>  <pre>Switch(config)# location rssi-half-life calibrating-client 60</pre></p>	<p>Configures the RSSI half life for the clients, calibrating clients, RFID tags, and rogue access points.</p> <p>You can enter the <b>location rssi-half-life</b> parameter value for the clients, calibrating clients, RFID tags, and rogue access points as 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.</p> <p>Some client devices transmit at reduced power immediately after changing channels, and RF is variable, so RSSI values might vary considerably from packet to packet. The <b>location rssi-half-life</b> command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or half life).</p> <p><b>Note</b> We recommend that you do not use or modify the <b>location rssi-half-life</b> command.</p>
Step 4	<p><b>location expiry</b> {<i>calibrating-client</i>   <i>client</i>   <i>rogue-aps</i>   <i>tags</i>} <i>timeout</i></p> <p><b>Example:</b>  <pre>Switch(config)# location expiry calibrating-client 50</pre></p>	<p>Configures the RSSI timeout value for the clients, calibrating clients, RFID tags, and rogue access points.</p> <p>You can enter the RSSI timeout value for the clients, RFID tags, and rogue access points from 5 through 3600 seconds, and the default value is 5 seconds.</p> <p>For the calibrating clients, you can enter the RSSI timeout value from 0 through 3600 seconds, and the default value is 5 seconds.</p> <p>Ensuring that recent, strong RSSIs are retained by the CPU is critical to location accuracy. The <b>location expiry</b> command enables you to specify the length of time after which old RSSI averages expire.</p> <p><b>Note</b> We recommend that you do not use or modify the <b>location expiry</b> command.</p>
Step 5	<p><b>location algorithm</b> {<i>rssi-average</i>   <i>simple</i>}</p> <p><b>Example:</b>  <pre>Switch(config)# location algorithm rssi-average</pre></p>	<p>Configures the algorithm used to average RSSI and signal-to-noise ratio (SNR) values.</p> <p>You can enter the <b>location algorithm rssi-average</b> command to specify a more accurate algorithm but requires more CPU overhead or the <b>location algorithm simple</b> command to specify a faster algorithm that requires low CPU overhead but provides less accuracy.</p> <p><b>Note</b> We recommend that you do not use or modify the <b>location algorithm</b> command.</p>
Step 6	<p><b>location admin-tag</b> <i>string</i></p> <p><b>Example:</b>  <pre>Switch(config)# location admin-tag</pre></p>	<p>Sets administrative tag or site information for the location of client devices.</p>
Step 7	<p><b>location civic-location identifier</b> {<i>identifier</i>   <i>host</i>}</p> <p><b>Example:</b>  <pre>Switch(config)# location civic-location identifier host</pre></p>	<p>Specifies civic location information.</p> <p>You can set the civic location identifier either as a string or host.</p>

	Command or Action	Purpose
<b>Step 8</b>	<b>location custom-location identifier</b> <i>{identifier   host}</i>  <b>Example:</b> <pre>Switch(config)# location custom-location identifier host</pre>	Specifies custom location information.  You can set the custom location identifier either as a string or host.
<b>Step 9</b>	<b>location geo-location identifier</b> <i>{identifier   host}</i>  <b>Example:</b> <pre>Switch(config)# location geo-location identifier host</pre>	Specifies geographical location information of the client devices.  You can set the location identifier either as a string or host.
<b>Step 10</b>	<b>location prefer</b> <i>{cdp   lldp-med   static}</i> <b>weight</b> <i>priority_value</i>  <b>Example:</b> <pre>Switch(config)# location prefer weight cdp 50</pre>	Sets location information source priority.  You can enter the priority weight from zero through 255.
<b>Step 11</b>	<b>location rfid</b> <i>{status   timeout   vendor-name}</i>  <b>Example:</b> <pre>Switch(config)# location rfid timeout 100</pre>	Configures RFID tag tracking options such as RFID tag status, RFID timeout value, and RFID tag vendor name.  You can enter the RFID timeout value in a range from 60 and 7200 seconds.
<b>Step 12</b>	<b>end</b>  <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI)

The Network Mobility Services Protocol (NMSP) manages communication between the mobility services engine and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.



### Note

The TCP port (16113) that the controller and mobility services engine communicate over must be open (not blocked) on any firewall that exists between the controller and the mobility services engine for NMSP to function.



**SUMMARY STEPS**

1. **configure terminal**
2. **nmsp notification interval** {attachment *seconds* | location *seconds* | rssi [clients *interval* | rfid *interval* | rogues [ap | client ] *interval*]}
3. **end**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>nmsp notification interval</b> {attachment <i>seconds</i>   location <i>seconds</i>   rssi [clients <i>interval</i>   rfid <i>interval</i>   rogues [ap   client ] <i>interval</i> ]}  <b>Example:</b> Switch(config)# <code>nmsp notification interval rssi rfid 50</code>	Sets the NMSP notification interval value for clients, RFID tags, and rogue clients and access points.  You can enter the NMSP notification interval value for RSSI measurement from 1 through 180 seconds.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

**Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues (CLI)****SUMMARY STEPS**

1. **configure terminal**
2. **location notify-threshold** {clients | rogues ap | tags } *threshold*
3. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
Step 2	<b>location notify-threshold</b> {clients   rogues ap   tags } <i>threshold</i>  <b>Example:</b> Switch(config)# <code>location notify-threshold clients 5</code>	Configures the NMSP notification threshold for clients, RFID tags, and rogue clients and access points.  You can enter the RSSI threshold value from zero through 10 db.
Step 3	<b>end</b>  <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Monitoring Location Settings and NMSP Settings

### Monitoring Location Settings (CLI)

This section describes the new commands for location settings.

The following commands can be used to monitor location settings on the switch.

**Table 25: Monitoring Location Settings Commands**

Command	Purpose
<code>show location summary</code>	Displays the current location configuration values.
<code>show location statistics rfid</code>	Displays the location-based RFID statistics.
<code>show location detail client_mac_addr</code>	Displays the RSSI table for a particular client.

### Monitoring NMSP Settings (CLI)

The following commands can be used to monitor NMSP settings on the switch.

**Table 26: Monitoring NMSP Settings Commands**

Command	Purpose
<b>show nmsp attachment suppress interfaces</b>	Displays the attachment suppress interfaces.
<b>show nmsp capability</b>	Displays the NMSP capabilities.
<b>show nmsp notification interval</b>	Displays the NMSP notification intervals.
<b>show nmsp statistics connection</b>	Displays the connection-specific NMSP counters.
<b>show nmsp statistics summary</b>	Displays the common NMSP counters.
<b>show nmsp status</b>	Displays the status of active NMSP connections.
<b>show nmsp subscription detail</b>	Displays all of the mobility services to which the switch is subscribed.
<b>show nmsp subscription detail <i>ip_addr</i></b>	Displays details only for the mobility services subscribed to by a specific IP address.
<b>show nmsp subscription summary</b>	Displays details for all of the mobility services to which the switch is subscribed.

## Examples: Location Settings Configuration

This example shows how to configure the path loss measurement (S60) request for calibrating client on the associated 802.11a or 802.11b/g radio:

```
Switch# configure terminal
Switch(config)# location plm calibrating uniband
Switch(config)# end
Switch# show location summary
```

This example shows how to configure the RSSI half life for a rouge access point:

```
Switch# configure terminal
Switch(config)# location rssi-half-life rogue-aps 20
Switch(config)# end
Switch# show location summary
```

## Examples: NMSP Settings Configuration

This example shows how to configure the NMSP notification interval for RFID tags:

```
Switch# configure terminal
Switch(config)# nmsp notification interval rssi rfid 50
```

```
Switch(config)# end
Switch# show nmosp notification interval
```

This example shows how to configure the NMSP notification interval for clients:

```
Switch# configure terminal
Switch(config)# nmosp notification interval rssi clients 180
Switch(config)# end
Switch# show nmosp notification interval
```

## Additional References for Location Settings

### Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information For Performing Location Settings Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE This feature was introduced.





## Monitoring Flow Control

---

- [Finding Feature Information, page 201](#)
- [Information About Flow Control, page 201](#)
- [Monitoring Flow Control, page 201](#)
- [Examples: Monitoring Flow Control, page 202](#)
- [Additional References for Monitoring Flow Control, page 203](#)
- [Feature History and Information For Monitoring Flow Control, page 204](#)

### Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### Information About Flow Control

Flow control is enabled by default on the switch.

Flow control provides shim layers between WCM and Cisco IOS for a reliable IPC. Every component in WCM has a dedicated channel. Few of the components in WCM have leveraged flow control in that. There is no configuration of flow control from CLI. You can monitor the flow control for any channel.

### Monitoring Flow Control

This section describes the new commands for flow control.

The following commands can be used to monitor flow control on the switch.

Table 27: Monitoring Flow Control

Command	Purpose
<code>show wireless flow-control channel -id</code>	Displays information about flow control on a particular channel.
<code>show wireless flow-control channel-id statistics</code>	Displays statistical information about flow control on a particular channel.

## Examples: Monitoring Flow Control

This example shows how to view information pertaining to any channel:

```
Switch# show wireless flow-control 3
Switch#

Channel Name       : CAPWAP
FC State           : Disabled
Remote Server State : Enabled
Pass-thru Mode     : Disabled
EnQ Disabled       : Disabled
Queue Depth        : 2048
Max Retries        : 5
Min Retry Gap (mSec) : 3
```

This example shows how to view flow control for a particular channel:

```
Switch# show wireless flow-control 3
Switch#

Channel Name                : CAPWAP
# of times channel went into FC : 0
# of times channel came out of FC : 0
Total msg count received by the FC Infra : 1
Pass-thru msgs send count : 0
Pass-thru msgs fail count : 0
# of msgs successfully queued : 0
# of msgs for which queuing failed : 0
# of msgs sent thru after queuing : 0
# of msgs sent w/o queuing : 1
# of msgs for which send failed : 0
# of invalid EAGAINS received : 0
Highest watermark reached : 0
# of times Q hit max capacity : 0
Avg time channel stays in FC (mSec) : 0
```



# Additional References for Monitoring Flow Control

## Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

## Standards and RFCs

Standard/RFC	Title
None	—

## MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information For Monitoring Flow Control

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.



## Configuring SDM Templates

---

- [Finding Feature Information, page 205](#)
- [Information About Configuring SDM Templates, page 205](#)
- [How to Configure SDM Templates, page 207](#)
- [Monitoring and Maintaining SDM Templates, page 209](#)
- [Configuration Examples for SDM Templates, page 209](#)
- [Feature History and Information for Configuring SDM Templates, page 210](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

#### Related Topics

[Feature History and Information for Troubleshooting Software Configuration, on page 352](#)

### Information About Configuring SDM Templates

#### 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.

These templates are supported on your device:

- **Advanced**—The advanced template is available on all supported images for this release. It maximizes system resources for features like netflow, multicast groups, security ACEs, QoS ACEs, and so on.
- **VLAN**—The VLAN template is available only on the LAN Base license. The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 device.

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.

The default is the advanced template.

**Table 28: Approximate Number of Feature Resources Allowed by Templates**

Resource	Advanced	VLAN
Number of VLANs	4094	4094
Unicast MAC addresses	32 K	32 K
Overflow unicast MAC addresses	512	512
IGMP groups and multicast routes	4 K	4 K
Overflow IGMP groups and multicast routes	512	512
• Directly connected routes	16K	16 K
• Indirectly connected IP hosts	7 K	7 K
Policy-based routing ACEs	1024	0
QoS classification ACEs	3 K	3 K
Security ACEs	1.5 K	1.5 K
Netflow ACEs	1024	1024
Input Microflow policer ACEs:	256 K	0
Output Microflow policer ACEs:	256 K	0
FSPAN ACEs	256	256
Tunnels:	256	0
Control Plane Entries:	512	512

Resource	Advanced	VLAN
Input Netflow flows:	8 K	8 K
Output Netflow flows:	16 K	16 K
SGT/DGT entries:	4 K	4 K
SGT/DGT Overflow entries:	0	512

**Note**

When the switch is used as a Wireless Mobility Agent, the only template allowed is the advanced template.

**Note**

SDM templates do not create VLANs. You must create the VLANs before adding commands to the SDM templates.

The tables represent approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance.

## 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

## Configuring SDM Templates

### Configuring the Switch SDM Template

#### Setting the SDM Template

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

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sdm prefer { advanced | vlan }`
4. `end`
5. `reload`

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<p><code>enable</code></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<p><code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.
<b>Step 3</b>	<p><code>sdm prefer { advanced   vlan }</code></p> <p><b>Example:</b></p> <pre>Switch(config)# sdm prefer advanced</pre>	<p>Specifies the SDM template to be used on the switch. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>advanced</b> —Supports advanced features such as Netflow.</li> <li>• <b>vlan</b> —Maximizes VLAN configuration on the switch with no routing supported in hardware.</li> </ul> <p><b>Note</b> The <code>no sdm prefer</code> command and a default template is not supported.</p>
<b>Step 4</b>	<p><code>end</code></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 5</b>	<p><code>reload</code></p> <p><b>Example:</b></p> <pre>Switch# reload</pre>	Reloads the operating system.

# 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.
no sdm prefer	Sets the default 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: Configuring SDM Templates

### Examples: Displaying SDM Templates

This is an example output showing the advanced template information:

```
Switch# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
Number of VLANs:                4094
Unicast MAC addresses:          32768
Overflow Unicast MAC addresses:  512
IGMP and Multicast groups:      8192
Overflow IGMP and Multicast groups: 512
Directly connected routes:      32768
Indirect routes:                 8192
Security Access Control Entries: 3072
QoS Access Control Entries:      2816
Policy Based Routing ACEs:       1024
Netflow ACEs:                    1024
Input Microflow policer ACEs:    256
Output Microflow policer ACEs:   256
Flow SPAN ACEs:                  256
```

```

Tunnels:                                256
Control Plane Entries:                   512
Input Netflow flows:                     8192
Output Netflow flows:                   16384

```

These numbers are typical for L2 and IPv4 features.  
Some features such as IPv6, use up double the entry size;  
so only half as many entries can be created.

This is an example output showing the VLAN template information:

```

Switch# show sdm prefer vlan

Showing SDM Template Info

This is the VLAN template for a typical Layer 2 network.
Number of VLANs:                                4094
Unicast MAC addresses:                          32768
Overflow Unicast MAC addresses:                  512
IGMP and Multicast groups:                      8192
Overflow IGMP and Multicast groups:              512
Directly connected routes:                      32768
Indirect routes:                                8192
Security Access Control Entries:                 3072
QoS Access Control Entries:                      3072
Policy Based Routing ACEs:                       0
Netflow ACEs:                                    1024
Input Microflow policer ACEs:                    0
Output Microflow policer ACEs:                   0
Flow SPAN ACEs:                                  256
Tunnels:                                          0
Control Plane Entries:                           512
Input Netflow flows:                             16384
Output Netflow flows:                            8192

```

These numbers are typical for L2 and IPv4 features.  
Some features such as IPv6, use up double the entry size;  
so only half as many entries can be created.

## Feature History and Information for Configuring SDM Templates

Release	Modification
Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE	This feature was introduced.





## Configuring System Message Logs

- [Finding Feature Information, page 211](#)
- [Restrictions for Configuring System Message Logs, page 211](#)
- [Information About Configuring System Message Logs, page 212](#)
- [How to Configure System Message Logs, page 215](#)
- [Monitoring and Maintaining System Message Logs, page 223](#)
- [Configuration Examples for System Message Logs, page 224](#)
- [Additional References for System Message Logs, page 224](#)
- [Feature History and Information For System Message Logs, page 226](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

#### Related Topics

[Feature History and Information for Troubleshooting Software Configuration, on page 352](#)

### Restrictions for Configuring System Message Logs

When the **logging discriminator** command is configured, the device may experience memory leak or crash. This usually happens during heavy syslog or debug output. The rate of the memory leak is dependent on the number of logs being produced. In extreme cases, the device may also crash. As a workaround, use the **no logging discriminator** command to disable the logging discriminator.

# 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. 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. If a standalone switch, 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.



### 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 29: System Log Message Elements**

Element	Description
<i>seq no:</i>	Stamps log messages with a sequence number only if the <b>service sequence-numbers</b> 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 <b>service timestamps log [datetime   log]</b> 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.
<i>hostname-n</i>	Hostname of a stack member and its switch number in the stack. Though the active switch is a stack member, it does <i>not</i> append its hostname to system messages.

## Default System Message Logging Settings

**Table 30: 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.

Feature	Default Setting
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.

## Enabling Syslog Trap Messages

You can enable Syslog traps using the **snmp-server enable traps syslog** command.

After enabling Syslog traps, you have to specify the trap message severity. Use the **logging snmp-trap** command to specify the trap level. By default, the command enables severity 0 to 4. To enable all the severity level, configure the **logging snmp-trap 0 7** command.

To enable individual trap levels, configure the following commands:

- **logging snmp-trap emergencies**: Enables only severity 0 traps.
- **logging snmp-trap alert**: Enables only severity 1 traps.

Note that, along with the Syslog traps, the Syslog history should also be applied. Without this configuration, Syslog traps are not sent.

Use the **logging history informational** command to enable the Syslog history.

# 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.

### SUMMARY STEPS

1. **configure terminal**
2. **logging buffered** *[size]*
3. **logging** *host*
4. **logging file flash:** *filename* *[max-file-size [min-file-size]]* *[severity-level-number | type]*
5. **end**
6. **terminal monitor**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging buffered</b> <i>[size]</i>  <b>Example:</b> Switch(config)# <b>logging buffered</b> <b>8192</b>	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.  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.  <b>Note</b> Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the <b>show memory</b> 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.
Step 3	<b>logging</b> <i>host</i>  <b>Example:</b> Switch(config)# <b>logging</b> <b>125.1.1.100</b>	Logs messages to a UNIX syslog server host.  <i>host</i> specifies the name or IP address of the host to be used as the syslog server.  To build a list of syslog servers that receive logging messages, enter this command more than once.

	Command or Action	Purpose
<b>Step 4</b>	<p><b>logging file flash:</b> <i>filename</i>  [<i>max-file-size</i> [<i>min-file-size</i>]]  [<i>severity-level-number</i>   <i>type</i>]</p> <p><b>Example:</b></p> <pre>Switch(config)# logging file flash:log_msg.txt 40960 4096 3</pre>	<p>Stores log messages in a file in flash memory on a standalone switch or, in the case of a switch stack, on the active switch.</p> <ul style="list-style-type: none"> <li>• <i>filename</i>—Enters the log message filename.</li> <li>• (Optional) <b>max-file-size</b> —Specifies the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes.</li> <li>• (Optional) <i>min-file-size</i>—Specifies the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes.</li> <li>• (Optional) <i>severity-level-number</i>   <i>type</i>—Specifies either the logging severity level or the logging type. The severity range is 0 to 7.</li> </ul>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>
<b>Step 6</b>	<p><b>terminal monitor</b></p> <p><b>Example:</b></p> <pre>Switch# terminal monitor</pre>	<p>Logs messages to a nonconsole terminal during the current session.</p> <p>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.</p>

## 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.

### SUMMARY STEPS

1. **configure terminal**
2. **line** [**console** | **vty**] *line-number* [*ending-line-number*]
3. **logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*]
4. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 2	<p><b>line [console   vty] line-number [ending-line-number]</b></p> <p><b>Example:</b></p> <pre>Switch(config)# line console</pre>	<p>Specifies the line to be configured for synchronous logging of messages.</p> <ul style="list-style-type: none"> <li>• <b>console</b>—Specifies configurations that occur through the switch console port or the Ethernet management port.</li> <li>• <b>line vty line-number</b>—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.</li> </ul> <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><b>logging synchronous [level [severity-level   all]   limit number-of-buffers]</b></p> <p><b>Example:</b></p> <pre>Switch(config)# logging synchronous level 3 limit 1000</pre>	<p>Enables synchronous logging of messages.</p> <ul style="list-style-type: none"> <li>• (Optional) <b>level severity-level</b>—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.</li> <li>• (Optional) <b>level all</b>—Specifies that all messages are printed asynchronously regardless of the severity level.</li> <li>• (Optional) <b>limit number-of-buffers</b>—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.</li> </ul>
Step 4	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(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 reenabling message logging after it has been disabled, use the **logging on** global configuration command.

This task is optional.

### SUMMARY STEPS

1. **configure terminal**
2. **no logging console**
3. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>no logging console</b>  <b>Example:</b> Switch(config)# <b>no logging console</b>	Disables message logging.
Step 3	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	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.

## SUMMARY STEPS

1. **configure terminal**
2. Use one of these commands:
  - **service timestamps log uptime**
  - **service timestamps log datetime[msec | localtime | show-timezone]**
3. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Use one of these commands: <ul style="list-style-type: none"> <li>• <b>service timestamps log uptime</b></li> <li>• <b>service timestamps log datetime[msec   localtime   show-timezone]</b></li> </ul> <b>Example:</b> Switch(config)# <b>service timestamps log uptime</b> or Switch(config)# <b>service timestamps log datetime</b>	Enables log time stamps. <ul style="list-style-type: none"> <li>• <b>log uptime</b>—Enables time stamps on log messages, showing the time since the system was rebooted.</li> <li>• <b>log datetime</b>—Enables time stamps on log messages. Depending on the options selected, the time stamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.</li> </ul>
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	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.

## SUMMARY STEPS

1. **configure terminal**
2. **service sequence-numbers**
3. **end**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>service sequence-numbers</b>  <b>Example:</b> Switch(config)# <b>service sequence-numbers</b>	Enables sequence numbers.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	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.

## SUMMARY STEPS

1. **configure terminal**
2. **logging console *level***
3. **logging monitor *level***
4. **logging trap *level***
5. **end**

## DETAILED STEPS

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

## SUMMARY STEPS

1. **configure terminal**
2. **logging history level**
3. **logging history size number**
4. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>logging history level</b>  <b>Example:</b> Switch(config)# <b>logging history 3</b>	Changes the default level of syslog messages stored in the history file and sent to the SNMP server.  By default, <b>warnings, errors, critical, alerts, and emergencies</b> messages are sent.
Step 3	<b>logging history size number</b>  <b>Example:</b> Switch(config)# <b>logging history size 200</b>	Specifies the number of syslog messages that can be stored in the history table.  The default is to store one message. The range is 0 to 500 messages.
Step 4	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	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.

**SUMMARY STEPS**

1. Add a line to the file `/etc/syslog.conf`.
2. Enter these commands at the UNIX shell prompt.
3. Make sure the syslog daemon reads the new changes.

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	Add a line to the file <code>/etc/syslog.conf</code> .  <b>Example:</b>  <code>local7.debug /usr/adm/logs/cisco.log</code>	<ul style="list-style-type: none"> <li>• <b>local7</b>—Specifies the logging facility.</li> <li>• <b>debug</b>—Specifies the syslog level. The file must already exist, and the syslog daemon must have permission to write to it.</li> </ul>
<b>Step 2</b>	Enter these commands at the UNIX shell prompt.  <b>Example:</b>  <code>\$ touch /var/log/cisco.log</code> <code>\$ chmod 666 /var/log/cisco.log</code>	Creates the log file. The syslog daemon sends messages at this level or at a more severe level to this file.
<b>Step 3</b>	Make sure the syslog daemon reads the new changes.  <b>Example:</b>  <code>\$ kill -HUP `cat /etc/syslog.pid`</code>	For more information, see the <b>man syslog.conf</b> and <b>man syslogd</b> commands on your UNIX system.

# Monitoring and Maintaining System Message Logs

## Monitoring Configuration Archive Logs

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

# Configuration Examples for System Message Logs

## Example: Stacking System Message

This example shows a partial switch system message for active switch and a stack member (hostname *Switch-2*):

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, 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 GigabitEthernet1/0/1, 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)

00:00:46: %LINK-3-UPDOWN: Interface Port-channell1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/2, changed state to up (Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
(Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/1, changed
state to down 2 (Switch-2)
```

## Example: Switch System Message

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

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell1, 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
System management commands	<i>System Management Command Reference (Catalyst 3650 Switches)</i>

Related Topic	Document Title
Platform-independent command references	<i>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>
Platform-independent configuration information	<i>IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>  <i>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information For System Message Logs

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.





## Configuring Online Diagnostics

---

- [Finding Feature Information, page 227](#)
- [Information About Configuring Online Diagnostics, page 227](#)
- [How to Configure Online Diagnostics, page 228](#)
- [Monitoring and Maintaining Online Diagnostics, page 233](#)
- [Configuration Examples for Online Diagnostic Tests, page 234](#)
- [Additional References for Online Diagnostics, page 236](#)
- [Feature History and Information for Configuring Online Diagnostics, page 237](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

#### Related Topics

[Feature History and Information for Troubleshooting Software Configuration, on page 352](#)

### Information About Configuring Online Diagnostics

#### Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the Switch while the Switch 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 Switch is connected to a live network; and health-monitoring runs in the background with user-defined intervals. By default, the health-monitoring test runs for every 30 seconds.

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 Switch or switch stack and the diagnostic tests that have already run.

## How to Configure Online Diagnostics

### Starting Online Diagnostic Tests

After you configure diagnostic tests to run on the Switch, 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:

#### SUMMARY STEPS

1. **diagnostic start switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**}

#### DETAILED STEPS

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

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

## Configuring Online Diagnostics

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

## Scheduling Online Diagnostics

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis for a Switch. Use the **no** form of this command to remove the scheduling.

### SUMMARY STEPS

1. **configure terminal**
2. **diagnostic schedule switch** *number test {name | test-id | test-id-range | all | basic | complete | minimal | non-disruptive | per-port} {daily | on mm dd yyyy hh:mm | port inter-port-number port-number-list | weekly day-of-week hh:mm}*

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 2</b>	<b>diagnostic schedule switch</b> <i>number test {name   test-id   test-id-range   all   basic   complete   minimal   non-disruptive   per-port} {daily   on mm dd yyyy hh:mm   port inter-port-number port-number-list   weekly day-of-week hh:mm}</i>	Schedules on-demand diagnostic tests for a specific day and time. The <b>switch number</b> keyword is supported only on stacking switches. The range is from 1 to 4. When specifying the tests to be scheduled, use these options: <ul style="list-style-type: none"> <li>• <b>name</b>—Name of the test that appears in the <b>show diagnostic content</b> command output.</li> </ul>

Command or Action	Purpose
<p><b>Example:</b></p> <pre>Switch(config)# diagnostic schedule switch 3 test 1-5 on July 3 2013 23:10</pre>	<ul style="list-style-type: none"> <li>• <i>test-id</i>—ID number of the test that appears in the <b>show diagnostic content</b> command output.</li> <li>• <i>test-id-range</i>—ID numbers of the tests that appear in the <b>show diagnostic content</b> command output.</li> <li>• <b>all</b>—All test IDs.</li> <li>• <b>basic</b>—Starts the basic on-demand diagnostic tests.</li> <li>• <b>complete</b>—Starts the complete test suite.</li> <li>• <b>minimal</b>—Starts the minimal bootup test suite.</li> <li>• <b>non-disruptive</b>—Starts the non-disruptive test suite.</li> <li>• <b>per-port</b>—Starts the per-port test suite.</li> </ul> <p>You can schedule the tests as follows:</p> <ul style="list-style-type: none"> <li>• <b>Daily</b>—Use the <b>daily</b> <i>hh:mm</i> parameter.</li> <li>• <b>Specific day and time</b>—Use the <b>on</b> <i>mm dd yyyy hh:mm</i> parameter.</li> <li>• <b>Weekly</b>—Use the <b>weekly</b> <i>day-of-week hh:mm</i> parameter.</li> </ul>

## Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing on a Switch while it is connected to a live network. You can configure the execution interval for each health-monitoring test, enable the Switch to generate a syslog message because of a test failure, and enable a specific test. Use the **no** form of this command to disable testing.

By default, health monitoring is disabled, but the Switch generates a syslog message when a test fails.

Follow these steps to configure and enable the health-monitoring diagnostic tests:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **diagnostic monitor interval switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds* *day*
4. **diagnostic monitor syslog**
5. **diagnostic monitor threshold switch** *number number* **test** {*name* | *test-id* | *test-id-range* | **all**} **failure** **count** *count*
6. **diagnostic monitor switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters the global configuration mode.
<b>Step 3</b>	<b>diagnostic monitor interval switch</b> <i>number</i> <b>test</b> { <i>name</i>   <i>test-id</i>   <i>test-id-range</i>   <b>all</b> } <i>hh:mm:ss milliseconds</i> <i>day</i>  <b>Example:</b> Switch(config)# <b>diagnostic monitor interval switch 2 test 1 12:30:00 750 5</b>	Configures the health-monitoring interval of the specified tests. The <b>switch</b> <i>number</i> keyword is supported only on stacking switches. The range is from 1 to 9. When specifying the tests, use one of these parameters: <ul style="list-style-type: none"> <li>• <i>name</i>—Name of the test that appears in the <b>show diagnostic content</b> command output.</li> <li>• <i>test-id</i>—ID number of the test that appears in the <b>show diagnostic content</b> command output.</li> <li>• <i>test-id-range</i>—ID numbers of the tests that appear in the <b>show diagnostic content</b> command output.</li> <li>• <b>all</b>—All of the diagnostic tests.</li> </ul> When specifying the interval, set these parameters:

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <i>hh:mm:ss</i>—Monitoring interval in hours, minutes, and seconds. The range for <i>hh</i> is 0 to 24, and the range for <i>mm</i> and <i>ss</i> is 0 to 60.</li> <li>• <i>milliseconds</i>—Monitoring interval in milliseconds (ms). The range is from 0 to 999.</li> <li>• <i>day</i>—Monitoring interval in the number of days. The range is from 0 to 20.</li> </ul>
<b>Step 4</b>	<b>diagnostic monitor syslog</b>  <b>Example:</b>  <pre>Switch(config)# diagnostic monitor syslog</pre>	(Optional) Configures the switch to generate a syslog message when a health-monitoring test fails.
<b>Step 5</b>	<b>diagnostic monitor threshold switch</b> <i>number number test {name   test-id   test-id-range   all} failure count count</i>  <b>Example:</b>  <pre>Switch(config)# diagnostic monitor threshold switch 2 test 1 failure count 20</pre>	(Optional) Sets the failure threshold for the health-monitoring tests. The <b>switch number</b> keyword is supported only on stacking switches. The range is from 1 to 9.  When specifying the tests, use one of these parameters: <ul style="list-style-type: none"> <li>• <i>name</i>—Name of the test that appears in the <b>show diagnostic content</b> command output.</li> <li>• <i>test-id</i>—ID number of the test that appears in the <b>show diagnostic content</b> command output.</li> <li>• <i>test-id-range</i>—ID numbers of the tests that appear in the <b>show diagnostic content</b> command output.</li> <li>• <b>all</b>—All of the diagnostic tests.</li> </ul> The range for the failure threshold <i>count</i> is 0 to 99.
<b>Step 6</b>	<b>diagnostic monitor switch number test</b> <i>{name   test-id   test-id-range   all}</i>  <b>Example:</b>  <pre>Switch(config)# diagnostic monitor switch 2 test 1</pre>	Enables the specified health-monitoring tests. The <b>switch number</b> keyword is supported only on stacking switches. The range is from 1 to 9.  When specifying the tests, use one of these parameters: <ul style="list-style-type: none"> <li>• <i>name</i>—Name of the test that appears in the <b>show diagnostic content</b> command output.</li> <li>• <i>test-id</i>—ID number of the test that appears in the <b>show diagnostic content</b> command output.</li> <li>• <i>test-id-range</i>—ID numbers of the tests that appear in the <b>show diagnostic content</b> command output.</li> <li>• <b>all</b>—All of the diagnostic tests.</li> </ul>

	Command or Action	Purpose
Step 7	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
Step 8	<b>show running-config</b>  <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
Step 9	<b>copy running-config startup-config</b>  <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

### What to Do Next

Use the **no diagnostic monitor interval test***test-id | test-id-range* } global configuration command to change the interval to the default value or to zero. Use the **no diagnostic monitor syslog** command to disable generation of syslog messages when a health-monitoring test fails. Use the **diagnostic monitor threshold test***test-id | test-id-range* } **failure count** command to remove the failure threshold.

## Monitoring and Maintaining Online Diagnostics

### Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured for the Switch or Switch stack and check the test results by using the privileged EXEC **show** commands in this table:

**Table 31: Commands for Diagnostic Test Configuration and Results**

Command	Purpose
<b>show diagnostic content switch</b> [ <i>number</i>   <b>all</b> ]	Displays the online diagnostics configured for a switch.
<b>show diagnostic status</b>	Displays the currently running diagnostic tests.
<b>show diagnostic result switch</b> [ <i>number</i>   <b>all</b> ] [ <b>detail</b>   <b>test</b> { <i>name</i>   <i>test-id</i>   <i>test-id-range</i>   <b>all</b> } [ <b>detail</b> ]]	Displays the online diagnostics test results.

Command	Purpose
<code>show diagnostic switch [number   all] [detail]</code>	Displays the online diagnostics test results.
<code>show diagnostic schedule switch [number   all]</code>	Displays the online diagnostics test schedule.
<code>show diagnostic post</code>	Displays the POST results. (The output is the same as the <code>show post</code> command output.)

## Configuration Examples for Online Diagnostic Tests

### Examples: Start Diagnostic Tests

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

```
Switch# diagnostic start switch 2 test TestInlinePwrCtrlr
```

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

```
Switch# diagnostic start switch 1 test all
```

### Example: Configure a Health Monitoring Test

This example shows how to configure a health-monitoring test:

```
Switch(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
Switch(config)# diagnostic monitor interval switch 1 test TestPortAsicStackPortLoopback
```

### Examples: Schedule Diagnostic Test

This example shows how to schedule diagnostic testing for a specific day and time on a specific switch:

```
Switch(config)# diagnostic schedule test DiagThermalTest on June 3 2013 22:25
```

This example shows how to schedule diagnostic testing to occur weekly at a certain time on a specific switch:

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly saturday 10:30
```



## Examples: Displaying Online Diagnostics

This example shows how to display on demand diagnostic settings:

```
Switch# show diagnostic ondemand settings

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

This example shows how to display diagnostic events for errors:

```
Switch# 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:

```
Switch# show diagnostic description switch 1 test all

DiagGoldPktTest :
    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.

DiagThermalTest :
    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.

DiagFanTest :
    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.

DiagPhyLoopbackTest :
    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.

DiagScratchRegisterTest :
    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.

DiagPoETest :
    This test checks the PoE controller functionality. This is a disruptive test
    and should not be performed during normal switch operation.

DiagStackCableTest :
    This test verifies the stack ring loopback functionality
    in the stacking environment. It is a disruptive test and
    cannot be run as a health monitoring test.

DiagMemoryTest :
    This test runs the exhaustive ASIC memory test during normal switch operation
    NG3K utilizes mbist for this test. Memory test is very disruptive
    in nature and requires switch reboot after the test.

Switch#
```

This example shows how to display the boot up level:

```
Switch# show diagnostic bootup level
Current bootup diagnostic level: minimal
Switch#
```

## Additional References for Online Diagnostics

### Related Documents

Related Topic	Document Title
System management commands	<i>System Management Command Reference (Catalyst 3650 Switches)</i>

### Standards and RFCs

Standard/RFC	Title
None	—

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

## Feature History and Information for Configuring Online Diagnostics

Release	Modification
Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE	This feature was introduced.





# CHAPTER 18

## Managing Configuration Files

---

- [Prerequisites for Managing Configuration Files, page 239](#)
- [Restrictions for Managing Configuration Files, page 239](#)
- [Information About Managing Configuration Files, page 240](#)
- [How to Manage Configuration File Information, page 246](#)
- [Additional References, page 279](#)

### 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 switch.
- Some of the Cisco IOS configuration commands are only available on certain switch 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 switch. 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 \(CLI\)](#) 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 Switch \(CLI\)](#) section for more information).

## Configuration Mode and Selecting a Configuration Source

To enter configuration mode on the switch, 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 \(CLI\)](#) 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 Switch \(CLI\)](#) 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 switch.

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 \(CLI\)](#) 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)

## Copy Configuration Files from a Network Server to the Switch

You can copy configuration files from a TFTP, rcp, or FTP server to the running configuration or startup configuration of the switch. 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 switch. For example, you may add another switch to your network and want it to have a similar configuration to the original switch. By copying the file to the new switch, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on to all of the switches in your network so that all of the switches have similar configurations.

The **copy {ftp: | rcp: | tftp:}system:running-config** EXEC command loads the configuration files into the switch as if you were typing the commands on the command line. The switch 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:} nvr**am:startup-config command) and reload the switch.

To copy configuration files from a server to a switch, 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 Switch 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 Switch to an RCP Server

You can copy a configuration file from the switch 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 switch 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 switch.

To configure the Cisco IOS software to allow remote users to copy files to and from the switch, 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 switch 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 switch through Telnet and was authenticated through the **username** command, the switch software sends the Telnet username as the remote username.



#### 4 The switch 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 switch. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the switch contains the following configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

If the switch IP address translates to switch1.example.com, then the .rhosts file for User0 on the RCP server should contain the following line:

```
Switch1.example.com Switch1
```

### 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 switch 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 switch through Telnet and is authenticated through the **username** command, the switch software sends the Telnet username as the remote username.
- 4 The switch 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 Switch to an FTP Server

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

## Understanding the FTP Username and Password

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 switch 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 switch 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 switch forms a password *username @switchname.domain*. The variable *username* is the username associated with the current session, *switchname* is the configured host name, and *domain* is the domain of the switch.

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 switch.

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.

## 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 switch 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 switches, 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 \(CLI\)](#) 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 Switch to a TFTP Server \(CLI\)](#) and [Configuring the Switch to Download Configuration Files](#) sections for more information on these commands.

## Configuring the Switch to Download Configuration Files

You can configure the switch 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 switch 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 switch downloads is called the network configuration file. The second file the switch downloads is called the host configuration file. Two configuration files can be used when all of the switches on a network use many of the same commands. The network configuration file contains the standard commands used to configure all of the switches. 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 (CLI)

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

### SUMMARY STEPS

1. **enable**
2. **show boot**
3. **more *file-url***
4. **show running-config**
5. **show startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>show boot</b>  <b>Example:</b> Switch# show boot	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.
<b>Step 3</b>	<b>more <i>file-url</i></b>  <b>Example:</b> Switch# more 10.1.1.1	Displays the contents of a specified file.

	Command or Action	Purpose
<b>Step 4</b>	<b>show running-config</b>  <b>Example:</b> Switch# show running-config	Displays the contents of the running configuration file. (Command alias for the <b>more system:running-config</b> command.)
<b>Step 5</b>	<b>show startup-config</b>  <b>Example:</b> Switch# show startup-config	Displays the contents of the startup configuration file. (Command alias for the <b>more nvram:startup-config</b> command.)  On all platforms except the Class A Flash file system platforms, the default startup-config file usually is stored in NVRAM.  On the Class A Flash file system platforms, the CONFIG_FILE environment variable points to the default startup-config file.  The CONFIG_FILE variable defaults to NVRAM.

## Modifying the Configuration File (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** 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 switch. 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:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **configuration command**
4. Do one of the following:
  - **end**
  - **^Z**
5. **copy system:running-config nvram:startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	<p>Enters global configuration mode.</p>
<b>Step 3</b>	<p><b>configuration command</b></p> <p><b>Example:</b></p> <pre>Switch(config)# configuration command</pre>	<p>Enter the necessary configuration commands. The Cisco IOS documentation set describes configuration commands organized by technology.</p>
<b>Step 4</b>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>end</b></li> <li>• <b>^Z</b></li> </ul> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	<p>Ends the configuration session and exits to EXEC mode.</p> <p><b>Note</b> When you press the Ctrl and Z keys simultaneously, ^Z is displayed to the screen.</p>
<b>Step 5</b>	<p><b>copy system:running-config nvram:startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy system:running-config nvram:startup-config</pre>	<p>Saves the running configuration file as the startup configuration file.</p> <p>You may also use the <b>copy running-config startup-config</b> 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).</p>

## Examples

In the following example, the switch prompt name of the switch is configured. The comment line, indicated by the exclamation mark (!), does not execute any command. The **hostname** command is used to change the switch name from switch 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.

```
Switch# configure terminal
Switch(config)# !The following command provides the switch host name.
Switch(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 switch after rebooting.

## Copying a Configuration File from the Switch to a TFTP Server (CLI)

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

### SUMMARY STEPS

1. `enable`
2. `copy system:running-config tftp: [[[//location ]/directory ]/filename ]`
3. `copy nvram:startup-config tftp: [[[//location ]/directory ]/filename ]`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><code>copy system:running-config tftp: [[[//location ]/directory ]/filename ]</code></p> <p><b>Example:</b></p> <pre>Switch# copy system:running-config tftp: //server1/topdir/file10</pre>	<p>Copies the running configuration file to a TFTP server.</p>

	Command or Action	Purpose
<b>Step 3</b>	<p><b>copy nvram:startup-config tftp:</b> [[[//location ]/directory ]/filename ]</p> <p><b>Example:</b></p> <pre>Switch# copy nvram:startup-config tftp: //server1/1stdir/file10</pre>	Copies the startup configuration file to a TFTP server.

### Examples

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

```
Switch# 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 Switch to an RCP Server (CLI)

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-username** *username*
4. **end**
5. Do one of the following:
  - **copy system:running-config rcp:** [[[//[username@]location ]/directory ]/filename ]
  - **copy nvram:startup-config rcp:** [[[//[username@]location ]/directory ]/filename ]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>	Enables privileged EXEC mode.



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

## 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:

```
Switch# 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
Switch#
```

## 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:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# 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?[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 Switch to the FTP Server (CLI)

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ftp username *username***
4. **ip ftp password *password***
5. **end**
6. Do one of the following:
  - **copy system:running-config ftp: [[[/[*username* [:*password* ]@]*location*]/*directory* ]/*filename* ]**  
or
  - **copy nvram:startup-config ftp: [[[/[*username* [:*password* ]@]*location*]/*directory* ]/*filename* ]**

### DETAILED STEPS

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

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters global configuration mode on the switch.
<b>Step 3</b>	<p><b>ip ftp username <i>username</i></b></p> <p><b>Example:</b></p> <pre>Switch(config)# ip ftp username NetAdmin1</pre>	(Optional) Specifies the default remote username.
<b>Step 4</b>	<p><b>ip ftp password <i>password</i></b></p> <p><b>Example:</b></p> <pre>Switch(config)# ip ftp password adminpassword</pre>	(Optional) Specifies the default password.
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	(Optional) Exits global configuration mode. This step is required only if you override the default remote username or password (see Steps 2 and 3).
<b>Step 6</b>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>copy system:running-config ftp:</b> [[[//[<i>username</i> ]:<i>password</i> ]@]<i>location</i>]/<i>directory</i> ]/<i>filename</i> ] or</li> <li>• <b>copy nvram:startup-config ftp:</b> [[[//[<i>username</i> ]:<i>password</i> ]@]<i>location</i>]/<i>directory</i> ]/<i>filename</i> ]</li> </ul> <p><b>Example:</b></p> <pre>Switch# copy system:running-config ftp:</pre>	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-config` to the `netadmin1` directory on the remote host with an IP address of `172.16.101.101`:

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

### 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:

```
Switch# configure terminal

Switch(config)# ip ftp username netadmin2

Switch(config)# ip ftp password mypass

Switch(config)# end

Switch# copy nvram:startup-config ftp:

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 a TFTP Server to the Switch (CLI)

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

### SUMMARY STEPS

1. `enable`
2. `copy tftp: [[[location]/directory]/filename] system:running-config`
3. `copy tftp: [[[location]/directory]/filename] nvram:startup-config`
4. `copy tftp: [[[location]/directory]/filename] flash-[n]:/directory/startup-config`

## DETAILED STEPS

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

```
Switch# 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 Switch (CLI)

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-username *username***
4. **end**
5. Do one of the following:
  - **copy rcp:[[[/[*username@*]*location*]/*directory*]/*filename*]system:running-config**
  - **copy rcp:[[[/[*username@*]*location*]/*directory*]/*filename*]nvram:startup-config**

### DETAILED STEPS

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

	Command or Action	Purpose
	<ul style="list-style-type: none"> <li>• <b>copy</b> <b>rcp:[[[/[username@]/location]/directory]/filename]nvram:startup-config</b></li> </ul> <p><b>Example:</b></p> <pre>Switch# copy rcp://[user1@example.com/dir10/fileone] nvram:startup-config</pre>	

## 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 switch:

```
Switch# 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]
Switch#
%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.

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# 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]
Switch#
%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 Switch (CLI)

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ftp username** *username*
4. **ip ftp password** *password*
5. **end**
6. Do one of the following:
  - **copy ftp:** `[[[//[username[:password]@]location] /directory ]/filename]system:running-config`
  - **copy ftp:** `[[[ //[username[:password]@]location]/directory]/filename]nvram:startup-config`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Switch# 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).
<b>Step 3</b>	<b>ip ftp username</b> <i>username</i>  <b>Example:</b> Switch(config)# ip ftp username NetAdmin1	(Optional) Specifies the default remote username.
<b>Step 4</b>	<b>ip ftp password</b> <i>password</i>  <b>Example:</b> Switch(config)# ip ftp password adminpassword	(Optional) Specifies the default password.



	Command or Action	Purpose
Step 5	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	(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	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>copy ftp:</b> [[[//[username[:password]@]location] /directory] /filename]system:running-config</li> <li>• <b>copy ftp:</b> [[[//[username[:password]@]location] /directory] /filename]nvram:startup-config</li> </ul> <p><b>Example:</b></p> <pre>Switch# copy ftp:nvram:startup-config</pre>	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 switch:

```
Switch# 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]
Switch#
%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:

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# 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]
```

```
Switch#
%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 (CLI)

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

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service compress-config**
4. **end**
5. Do one of the following:
  - Use FTP, RCP, or TFTP to copy the new configuration.
  - **configure terminal**
6. **copy system:running-config nvram:startup-config**

#### DETAILED STEPS

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

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

```
Switch# configure terminal
Switch(config)# service compress-config
Switch(config)# end
Switch# 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]
Switch# 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 (CLI)

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

### SUMMARY STEPS

1. **enable**
2. **copy nvram:startup-config *flash-filesystem:filename***
3. **configure terminal**
4. **boot config flash-filesystem: *filename***
5. **end**
6. Do one of the following:
  - 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**
7. **copy system:running-config nvram:startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>copy nvram:startup-config <i>flash-filesystem:filename</i></b>  <b>Example:</b> Switch# copy nvram:startup-config usbflash0:switch-config	Copies the current startup configuration to the new location to create the configuration file.
<b>Step 3</b>	<b>configure terminal</b>  <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
<b>Step 4</b>	<b>boot config flash-filesystem: <i>filename</i></b>  <b>Example:</b> Switch(config)# boot config usbflash0:switch-config	Specifies that the startup configuration file be stored in flash memory by setting the CONFIG_FILE variable.

	Command or Action	Purpose
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Switch(config)# end	Exits global configuration mode.
<b>Step 6</b>	Do one of the following: <ul style="list-style-type: none"> <li>• 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 - <i>file-size /buffer-size</i> bytes].”</li> <li>• <b>configure terminal</b></li> </ul> <b>Example:</b> Switch# configure terminal	Enters the new configuration.
<b>Step 7</b>	<b>copy system:running-config nvram:startup-config</b>  <b>Example:</b> Switch(config)# copy system:running-config nvram:startup-config	When you have finished changing the running-configuration, save the new configuration.

### Examples

The following example stores the configuration file in usbflash0:

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

## Loading the Configuration Commands from the Network (CLI)

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

## SUMMARY STEPS

1. **enable**
2. **copy system:running-config {ftp: | rcp: | tftp:}**
3. **configure terminal**
4. **boot network {ftp:[[/[username [:password ]@]location ]/directory ]/filename ] | rcp:[[/[username@]location ]/directory ]/filename ] | tftp:[[/location ]/directory ]/filename ]}**
5. **service config**
6. **end**
7. **copy system:running-config nvram:startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>copy system:running-config {ftp:   rcp:   tftp:}</b>  <b>Example:</b> Switch# copy system:running-config ftp:	Saves the running configuration to an FTP, RCP, or TFTP server.
<b>Step 3</b>	<b>configure terminal</b>  <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
<b>Step 4</b>	<b>boot network {ftp:[[/[username [:password ]@]location ]/directory ]/filename ]   rcp:[[/[username@]location ]/directory ]/filename ]   tftp:[[/location ]/directory ]/filename ]}</b>  <b>Example:</b> Switch(config)# boot network ftp://user1:guessme@example.com/dir10/file1	Specifies that the startup configuration file be loaded from the network server at startup.
<b>Step 5</b>	<b>service config</b>  <b>Example:</b> Switch(config)# service config	Enables the switch to download configuration files at system startup.

	Command or Action	Purpose
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Switch(config)# end	Exits global configuration mode.
<b>Step 7</b>	<b>copy system:running-config nvram:startup-config</b>  <b>Example:</b> Switch# copy system:running-config nvram:startup-config	Saves the configuration.

## Copying Configuration Files from Flash Memory to the Startup or Running Configuration (CLI)

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:

### SUMMARY STEPS

1. **enable**
2. Do one of the following:
  - **copy filesystem: [partition-number:][filename ] nvram:startup-config**
  - **copy filesystem: [partition-number:][filename ] system:running-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	Do one of the following: <ul style="list-style-type: none"> <li>• <b>copy filesystem: [partition-number:][filename ] nvram:startup-config</b></li> <li>• <b>copy filesystem: [partition-number:][filename ] system:running-config</b></li> </ul>	<ul style="list-style-type: none"> <li>• Loads a configuration file directly into NVRAM or</li> <li>• Copies a configuration file to your running configuration</li> </ul>

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch# copy usbflash0:4:ios-upgrade-1 nvram:startup-config</pre>	

### Examples

The following example copies the file named ios-upgrade-1 from partition 4 of the flash memory PC Card in usbflash0 to the switch startup configurations:

```
Switch# 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 (CLI)

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 switches. To copy a configuration file between flash memory file systems, use the following commands in EXEC mode:

### SUMMARY STEPS

1. **enable**
2. **show** *source-filesystem:*
3. **copy** *source-filesystem:* [*partition-number:*][*filename* ] *dest-filesystem:*[*partition-number:*][*filename* ]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>show</b> <i>source-filesystem:</i></p> <p><b>Example:</b></p> <pre>Switch# show flash:</pre>	<p>Displays the layout and contents of flash memory to verify the filename.</p>





## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ftp username *username***
4. **ip ftp password *password***
5. **end**
6. **copy ftp: [[[*location*]/*directory* ]/*bundle\_name* flash:**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username or password (see Steps 3 and 4).
Step 3	<b>ip ftp username <i>username</i></b>  <b>Example:</b> Switch(config)# ip ftp username Admin01	(Optional) Specifies the remote username.
Step 4	<b>ip ftp password <i>password</i></b>  <b>Example:</b> Switch(config)# ip ftp password adminpassword	(Optional) Specifies the remote password.
Step 5	<b>end</b>  <b>Example:</b> Switch(config)# end	(Optional) Exits configuration mode. This step is required only if you override the default remote username (see Steps 3 and 4).
Step 6	<b>copy ftp: [[[<i>location</i>]/<i>directory</i> ]/<i>bundle_name</i> flash:</b>  <b>Example:</b> Switch>copy ftp:/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:	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 (CLI)

To copy a configuration file from an RCP server to a flash memory device, complete the tasks in this section:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-username *username***
4. **end**
5. **copy rcp: [://[*username@*]*location* ]/*directory* ]/*bundle\_name* ] flash:**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username or password (see Step 3).
<b>Step 3</b>	<b>ip rcmd remote-username <i>username</i></b>  <b>Example:</b> Switch(config)# ip rcmd remote-username Admin01	(Optional) Specifies the remote username.

	Command or Action	Purpose
<b>Step 4</b>	<b>end</b>  <b>Example:</b> <pre>Switch(config)# end</pre>	(Optional) Exits configuration mode. This step is required only if you override the default remote username or password (see Step 3).
<b>Step 5</b>	<b>copy rcp: [[[/[username@]location ]/directory] /bundle_name] flash:</b>  <b>Example:</b> <pre>Switch# copy rcp://netadmin@172.16.101.101/bundle1 flash:</pre>	Copies the configuration file from a network server to the flash memory device using RCP. Respond to any switch prompts for additional information or confirmation. Prompting depends on how much information you provide in the <b>copy</b> command and the current setting of the <b>file prompt</b> command.

## Copying a Configuration File from a TFTP Server to Flash Memory Devices (CLI)

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

### SUMMARY STEPS

1. **enable**
2. **copy tftp: [[[/location ]/directory ]/bundle\_name flash:**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>copy tftp: [[[/location ]/directory ]/bundle_name flash:</b>  <b>Example:</b> <pre>Switch# copy tftp:/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:</pre>	Copies the file from a TFTP server to the flash memory device. Reply to any switch prompts for additional information or confirmation. Prompting depends on how much information you provide in the <b>copy</b> command and the current setting of the <b>file prompt</b> command.

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

**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.

```
Switch#
copy tftp:switch-config usbflash0:new-config
```

## Re-executing the Configuration Commands in the Startup Configuration File (CLI)

To re-execute the commands located in the startup configuration file, complete the task in this section:

**SUMMARY STEPS**

1. enable
2. configure memory

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure memory</b></p> <p><b>Example:</b></p> <pre>Switch# configure memory</pre>	<p>Re-executes the configuration commands located in the startup configuration file.</p>

## Clearing the Startup Configuration (CLI)

You can clear the configuration information from the startup configuration. If you reboot the switch with no startup configuration, the switch enters the Setup command facility so that you can configure the switch from scratch. To clear the contents of your startup configuration, complete the task in this section:

**SUMMARY STEPS**

1. `enable`
2. `erase nvram`

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>erase nvram</b>  <b>Example:</b> Switch# erase nvram	Clears the contents of your startup configuration. <p><b>Note</b> 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 <b>erase startup-config</b> EXEC command, the switch erases or deletes the configuration pointed to by the CONFIG_FILE environment variable. If this variable points to NVRAM, the switch erases NVRAM. If the CONFIG_FILE environment variable specifies a flash memory device and configuration filename, the switch deletes the configuration file. That is, the switch marks the file as “deleted,” rather than erasing it. This feature allows you to recover a deleted file.</p>

**Deleting a Specified Configuration File (CLI)**

To delete a specified configuration on a specific flash device, complete the task in this section:

**SUMMARY STEPS**

1. `enable`
2. `delete flash-filesystem:filename`

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>delete flash-filesystem:filename</b>	Deletes the specified configuration file on the specified flash device.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch# delete usbflash0:myconfig</pre>	<p><b>Note</b> 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 <b>undelete</b> EXEC command. Erased files cannot be recovered. To permanently erase the configuration file, use the <b>squeeze</b> 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 (CLI)

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:

### SUMMARY STEPS

1. **enable**
2. **copy** [*flash-url* | *ftp-url* | *rcp-url* | *tftp-url* | **system:running-config** | **nvrाम:startup-config**] *dest-flash-url*
3. **configure terminal**
4. **boot config** *dest-flash-url*
5. **end**
6. **copy** **system:running-config** **nvrाम:startup-config**
7. **show boot**

### DETAILED STEPS

	Command or Action	Purpose
<p><b>Step 1</b></p>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b></p>	<p><b>copy</b> [<i>flash-url</i>   <i>ftp-url</i>   <i>rcp-url</i>   <i>tftp-url</i>   <b>system:running-config</b>   <b>nvrाम:startup-config</b>] <i>dest-flash-url</i></p>	<p>Copies the configuration file to the flash file system from which the switch loads the file on restart.</p>

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch# copy system:running-config nvram:startup-config</pre>	
<b>Step 3</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 4</b>	<p><b>boot config <i>dest-flash-url</i></b></p> <p><b>Example:</b></p> <pre>Switch(config)# boot config 172.16.1.1</pre>	Sets the CONFIG_FILE environment variable. This step modifies the runtime CONFIG_FILE environment variable.
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Exits global configuration mode.
<b>Step 6</b>	<p><b>copy system:running-config nvram:startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy system:running-config nvram:startup-config</pre>	Saves the configuration performed in Step 3 to the startup configuration.
<b>Step 7</b>	<p><b>show boot</b></p> <p><b>Example:</b></p> <pre>Switch# show boot</pre>	(Optional) Allows you to verify the contents of the CONFIG_FILE environment variable.

### Examples

The following example copies the running configuration file to the switch. This configuration is then used as the startup configuration when the system is restarted:

```
Switch# copy system:running-config usbflash0:config2
Switch# configure terminal
Switch(config)# boot config usbflash0:config2
Switch(config)# end
Switch# copy system:running-config nvram:startup-config
[ok]
Switch# 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 **nvr<sub>am</sub>:startup-config** command is aliased to the new location of the startup configuration file. The **more nvr<sub>am</sub>:startup-config EXEC** command displays the startup configuration, regardless of its location. The **erase nvr<sub>am</sub>: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 nvr<sub>am</sub>:startup-config** command, the switch 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 switch prompts you to confirm your overwrite of the complete version with the distilled version. If NVRAM contains a distilled configuration, the switch 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 nvr<sub>am</sub>: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 Switch 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 switch to download configuration files at system startup, perform at least one of the tasks described in the following sections:

- [Configuring the Switch to Download the Network Configuration File \(CLI\)](#)
- [Configuring the Switch to Download the Host Configuration File \(CLI\)](#)

If the switch 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 switch 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 switch enters the Setup command facility.

### Configuring the Switch to Download the Network Configuration File (CLI)

To configure the Cisco IOS software to download a network configuration file from a server at startup, complete the tasks in this section:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot network** {ftp:[[[//[username [:password ]@]location ]/directory ]/filename ] | rcp:[[[//[username@]location ]/directory ]/filename ] | tftp:[[[//[location ]/directory ]/filename ]}
4. **service config**
5. **end**
6. **copy system:running-config nvram:startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>boot network</b> {ftp:[[[//[username [:password ]@]location ]/directory ]/filename ]   rcp:[[[//[username@]location ]/directory ]/filename ]   tftp:[[[//[location ]/directory ]/filename ]}  <b>Example:</b> Switch(config)# boot network tftp:hostfile1	Specifies the network configuration file to download at startup, and the protocol to be used (TFTP, RCP, or FTP). <ul style="list-style-type: none"> <li>• 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 switch uses the broadcast address.</li> <li>• 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.</li> </ul>
<b>Step 4</b>	<b>service config</b>  <b>Example:</b> Switch(config)# service config	Enables the system to automatically load the network file on restart.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Switch(config)# end	Exits global configuration mode.

	Command or Action	Purpose
<b>Step 6</b>	<b>copy system:running-config nvram:startup-config</b>  <b>Example:</b>  Switch# copy system:running-config nvram:startup-config	Saves the running configuration to the startup configuration file.

## Configuring the Switch to Download the Host Configuration File (CLI)

To configure the Cisco IOS software to download a host configuration file from a server at startup, complete the tasks in this section:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot host {ftp:[[[//[username [:password ]@]location ]/directory ]/filename ] | rcp:[[[//[username@]location ]/directory ]/filename ] | tftp:[[[//[location ]/directory ]/filename ] }**
4. **service config**
5. **end**
6. **copy system:running-config nvram:startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b>  Switch# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>boot host {ftp:[[[//[username [:password ]@]location ]/directory ]/filename ]   rcp:[[[//[username@]location ]/directory ]/filename ]   tftp:[[[//[location ]/directory ]/filename ] }</b>	Specifies the host configuration file to download at startup, and the protocol to be used (FTP, RCP, or TFTP): <ul style="list-style-type: none"> <li>• If you do not specify a host configuration filename, the switch uses its own name to form a host configuration filename by converting the name to all lowercase letters, removing all domain</li> </ul>

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch(config)# boot host tftp:hostfile1</pre>	<p>information, and appending “-config.” If no host name information is available, the software uses the default host configuration filename switch-config. If you omit the address, the switch uses the broadcast address.</p> <ul style="list-style-type: none"> <li>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.</li> </ul>
<b>Step 4</b>	<p><b>service config</b></p> <p><b>Example:</b></p> <pre>Switch(config)# service config</pre>	Enables the system to automatically load the host file upon restart.
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Exits global configuration mode.
<b>Step 6</b>	<p><b>copy system:running-config nvram:startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy system:running-config nvram:startup-config</pre>	Saves the running configuration to the startup configuration file.

### Example

In the following example, a switch is configured to download the host configuration file named hostfile1 and the network configuration file named networkfile1. The switch uses TFTP and the broadcast address to obtain the file:

```
Switch# configure terminal
Switch(config)# boot host tftp:hostfile1
Switch(config)# boot network tftp:networkfile1
Switch(config)# service config
Switch(config)# end
Switch# copy system:running-config nvram:startup-config
```

# Additional References

## Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco IOS configuration commands	<i>Cisco IOS Configuration Fundamentals Command Reference</i>

## Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

## Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified	--

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>No new or modified MIBs are supported, and support for existing MIBs has not been modified.</li> </ul>	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

**Technical Assistance**

Description	Link
<p>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.</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>



## Configuration Replace and Configuration Rollback

---

- [Prerequisites for Configuration Replace and Configuration Rollback](#), page 281
- [Restrictions for Configuration Replace and Configuration Rollback](#), page 282
- [Information About Configuration Replace and Configuration Rollback](#), page 282
- [How to Use Configuration Replace and Configuration Rollback](#), page 285
- [Configuration Examples for Configuration Replace and Configuration Rollback](#), page 291
- [Additional References](#), page 293

### 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 switch 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 switch, 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 (CLI)

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.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **path *url***
5. **maximum *number***
6. **time-period *minutes***
7. **end**
8. **archive config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Switch> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
Step 3	<b>archive</b>  <b>Example:</b> Switch(config)# archive	Enters archive configuration mode.

	Command or Action	Purpose
<b>Step 4</b>	<b>path</b> <i>url</i>  <b>Example:</b> <pre>Switch(config-archive)# path flash:myconfiguration</pre>	Specifies the location and filename prefix for the files in the Cisco IOS configuration archive.  <b>Note</b> 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.
<b>Step 5</b>	<b>maximum</b> <i>number</i>  <b>Example:</b> <pre>Switch(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"> <li>The <i>number</i> argument is the maximum number of archive files of the running configuration to be saved in the Cisco IOS configuration archive. Valid values are from 1 to 14. The default is 10.</li> </ul> <b>Note</b> Before using this command, you must configure the <b>path</b> command to specify the location and filename prefix for the files in the Cisco IOS configuration archive.
<b>Step 6</b>	<b>time-period</b> <i>minutes</i>  <b>Example:</b> <pre>Switch(config-archive)# time-period 1440</pre>	(Optional) Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco IOS configuration archive.  <ul style="list-style-type: none"> <li>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.</li> </ul> <b>Note</b> Before using this command, you must configure the <b>path</b> command to specify the location and filename prefix for the files in the Cisco IOS configuration archive.
<b>Step 7</b>	<b>end</b>  <b>Example:</b> <pre>Switch(config-archive)# end</pre>	Exits to privileged EXEC mode.
<b>Step 8</b>	<b>archive config</b>  <b>Example:</b> <pre>Switch# archive config</pre>	Saves the current running configuration file to the configuration archive.  <b>Note</b> The <b>path</b> command must be configured before using this command.

## Performing a Configuration Replace or Configuration Rollback Operation (CLI)

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 \(CLI\)](#) 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.

**SUMMARY STEPS**

1. **enable**
2. **configure replace** *target-url* [**nolock**] [**list**] [**force**] [**ignore case**] [**revert trigger** [**error**] ] [**timer** *minutes*] | **time** *minutes* ]
3. **configure revert** { **now** | **timer** { *minutes* | **idle** *minutes* } }
4. **configure confirm**
5. **exit**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure replace</b> <i>target-url</i> [<b>nolock</b>] [<b>list</b>] [<b>force</b>] [<b>ignore case</b>] [<b>revert trigger</b> [<b>error</b>] ] [<b>timer</b> <i>minutes</i>]   <b>time</b> <i>minutes</i> ]</p> <p><b>Example:</b></p> <pre>Switch# configure replace flash: startup-config time 120</pre>	<p>Replaces the current running configuration file with a saved Cisco IOS configuration file.</p> <ul style="list-style-type: none"> <li>• 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 <b>archive config</b> command.</li> <li>• The <b>list</b> 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.</li> <li>• The <b>force</b> keyword replaces the current running configuration file with the specified saved Cisco IOS configuration file without prompting you for confirmation.</li> <li>• The <b>time minutes</b> keyword and argument specify the time (in minutes) within which you must enter the <b>configure confirm</b> command to confirm replacement of the current running configuration file. If the <b>configure confirm</b> 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 <b>configure replace</b> command).</li> <li>• The <b>nolock</b> keyword disables the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replace operation.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>The <b>revert trigger</b> keywords set the following triggers for reverting to the original configuration: <ul style="list-style-type: none"> <li><b>error</b> —Reverts to the original configuration upon error.</li> <li><b>timer minutes</b> —Reverts to the original configuration if specified time elapses.</li> </ul> </li> <li>The <b>ignore case</b> keyword allows the configuration to ignore the case of the confirmation command.</li> </ul>
<b>Step 3</b>	<b>configure revert { now   timer {minutes   idle minutes} }</b>  <b>Example:</b> Switch# configure revert now	(Optional) To cancel the timed rollback and trigger the rollback immediately, or to reset parameters for the timed rollback, use the <b>configure revert</b> command in privileged EXEC mode. <ul style="list-style-type: none"> <li><b>now</b> —Triggers the rollback immediately.</li> <li><b>timer</b> —Resets the configuration revert timer. <ul style="list-style-type: none"> <li>Use the <i>minutes</i> argument with the <b>timer</b> keyword to specify a new revert time in minutes.</li> <li>Use the <b>idle</b> keyword along with a time in minutes to set the maximum allowable time period of no activity before reverting to the saved configuration.</li> </ul> </li> </ul>
<b>Step 4</b>	<b>configure confirm</b>  <b>Example:</b> Switch# configure confirm	(Optional) Confirms replacement of the current running configuration file with a saved Cisco IOS configuration file. <p><b>Note</b> Use this command only if the <b>time seconds</b> keyword and argument of the <b>configure replace</b> command are specified.</p>
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Switch# exit	Exits to user EXEC mode.

## Monitoring and Troubleshooting the Feature (CLI)

Perform this task to monitor and troubleshoot the Configuration Replace and Configuration Rollback feature.

## SUMMARY STEPS

1. **enable**
2. **show archive**
3. **debug archive versioning**
4. **debug archive config timestamp**
5. **exit**

## DETAILED STEPS

### Step 1

#### **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

#### **Example:**

```
Switch> enable
Switch#
```

### Step 2

#### **show archive**

Use this command to display information about the files saved in the Cisco IOS configuration archive.

#### **Example:**

```
Switch# 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:**

```
Switch# 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:**

```

Switch# 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:**

```

Switch# debug archive config timestamp
Switch# 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:**

```

Switch# exit
Switch>

```

---



# 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.

```
Switch# 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:

```
Switch# 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:

```
Switch# 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).

```
Switch# 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
Switch# 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.

```
Switch# 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:

```
Switch# 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
Switch# configure replace flash:myconfiguration-1
Total number of passes: 1
Rollback Done
```

## Additional References

### Related Documents

Related Topic	Document Title
Configuration Locking	<i>Exclusive Configuration Change Access and Access Session Locking</i>
Commands for managing configuration files	<i>Cisco IOS Configuration Fundamentals Command Reference</i>
Information about managing configuration files	<i>Managing Configuration Files</i>

**Error Message Decoder**

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

**Standards**

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

**MIBs**

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**RFCs**

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

**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>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>





## Working with the Flash File System

---

- [Information About the Flash File System, page 297](#)
- [Displaying Available File Systems, page 298](#)
- [Setting the Default File System, page 300](#)
- [Displaying Information About Files on a File System, page 300](#)
- [Changing Directories and Displaying the Working Directory \(CLI\), page 301](#)
- [Creating Directories \(CLI\), page 302](#)
- [Copying Files, page 303](#)
- [Creating, Displaying and Extracting Files \(CLI\), page 305](#)
- [Additional References, page 307](#)

### 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 switch is named flash:.

As viewed from the active switch, or any stack member, flash: refers to the local flash device, which is the device attached to the same switch on which the file system is being viewed. In a switch stack, each of the flash devices from the various stack members can be viewed from the active switch. The names of these flash file systems include the corresponding switch member numbers. For example, flash-3:, as viewed from the active switch, 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 switch stack.

Only one user at a time can manage the software bundles and configuration files for a switch stack .

## Displaying Available File Systems

To display the available file systems on your switch, use the **show file systems** privileged EXEC command as shown in this example for a standalone switch:

```
Switch# show file systems
File Systems:
  Size(b)      Free(b)      Type      Flags  Prefixes
*  15998976    5135872     flash    rw     flash:
    -          -           opaque   rw     bs:
    -          -           opaque   rw     vb:
    524288     520138      nvram    rw     nvram:
    -          -           network  rw     tftp:
    -          -           opaque   rw     null:
    -          -           opaque   rw     system:
    -          -           opaque   ro     xmodem:
    -          -           opaque   ro     ymodem:
```

This example shows a switch stack. In this example, the active switch is stack member 1; the file system on stack member 2 is displayed as flash-2; the file system on stack member 3 is displayed as flash-3; and so on up to stack member 9, displayed as flash-9; for a 9-member stack. The example also shows the crashinfo directories and a USB flash drive plugged into the active switch:

```
Switch# show file systems
File Systems:
  Size(b)      Free(b)      Type      Flags  Prefixes
  145898496    5479424     disk      rw     crashinfo:crashinfo-1:
  248512512    85983232    disk      rw     crashinfo-2:stby-crashinfo:
  146014208    17301504    disk      rw     crashinfo-3:
  146014208    0           disk      rw     crashinfo-4:
  146014208    1572864     disk      rw     crashinfo-5:
  248512512    30932992    disk      rw     crashinfo-6:
  146014208    6291456     disk      rw     crashinfo-7:
  146276352    15728640    disk      rw     crashinfo-8:
  146276352    73400320    disk      rw     crashinfo-9:
*  741621760    481730560    disk      rw     flash:flash-1:
  1622147072  1360527360  disk      rw     flash-2:stby-flash:
  729546752    469762048  disk      rw     flash-3:
  729546752    469762048  disk      rw     flash-4:
  729546752    469762048  disk      rw     flash-5:
  1622147072  1340604416  disk      rw     flash-6:
  729546752    469762048  disk      rw     flash-7:
  1749549056  1487929344  disk      rw     flash-8:
  1749549056  1487929344  disk      rw     flash-9:
    0          0           disk      rw     unix:
    -          -           disk      rw     usbflash0:usbflash0-1:
    -          -           disk      rw     usbflash0-2: stby-usbflash0:
    -          -           disk      rw     usbflash0-3:
    -          -           disk      rw     usbflash0-4:
    -          -           disk      rw     usbflash0-5:
    -          -           disk      rw     usbflash0-6:
    -          -           disk      rw     usbflash0-7:
    -          -           disk      rw     usbflash0-8:
    -          -           disk      rw     usbflash0-9:
    0          0           disk      ro     wealui:
    -          -           opaque   rw     system:
    -          -           opaque   rw     tmpsys:
  2097152     2055643     nvram    rw     stby-nvram:
    -          -           nvram    rw     stby-rcsf:
    -          -           opaque   rw     null:
    -          -           opaque   ro     tar:
    -          -           network  rw     tftp:
  2097152     2055643     nvram    rw     nvram:
    -          -           opaque   wo     syslog:
    -          -           network  rw     rcp:
    -          -           network  rw     http:
```



```

-          - network  rw  ftp:
-          - network  rw  scp:
-          - network  rw  https:
-          - opaque   ro  cns:
-          - opaque   rw  revrcsf:

```

**Table 32: 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><b>disk</b>—The file system is for a flash memory device, USB flash, and crashinfo file.</p> <p><b>network</b>—The file system for network devices; for example, an FTP server or and HTTP server.</p> <p><b>nvr</b>am—The file system is for a NVRAM device.</p> <p><b>opaque</b>—The file system is a locally generated pseudo file system (for example, the system) or a download interface, such as brimux.</p> <p><b>unknown</b>—The file system is an unknown type.</p>
Flags	<p>Permission for file system.</p> <p><b>ro</b>—read-only.</p> <p><b>rw</b>—read/write.</p> <p><b>wo</b>—write-only.</p>

Field	Value
Prefixes	<p>Alias for file system.</p> <p><b>crashinfo:</b>—Crashinfo file.</p> <p><b>flash:</b>—Flash file system.</p> <p><b>ftp:</b>—FTP server.</p> <p><b>http:</b>—HTTP server.</p> <p><b>https:</b>—Secure HTTP server.</p> <p><b>nvr:</b>—NVRAM.</p> <p><b>null:</b>—Null destination for copies. You can copy a remote file to null to find its size.</p> <p><b>rpx:</b>—Remote Copy Protocol (RCP) server.</p> <p><b>scp:</b>—Session Control Protocol (SCP) server.</p> <p><b>system:</b>—Contains the system memory, including the running configuration.</p> <p><b>tftp:</b>—TFTP network server.</p> <p><b>usbflash0:</b>—USB flash memory.</p> <p><b>xmodem:</b>—Obtain the file from a network machine by using the Xmodem protocol.</p> <p><b>ymodem:</b>—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 33: Commands for Displaying Information About Files**

Command	Description
<b>dir</b> [/all] [filesystem:filename]	Displays a list of files on a file system.
<b>show file systems</b>	Displays more information about each of the files on a file system.
<b>show file information</b> file-url	Displays information about a specific file.
<b>show file descriptors</b>	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:

```
switch# dir flash:
Directory of flash:/
7386  -rwx      2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
7378  drwx         4096 Jan 23 2013 09:35:11 +00:00 mnt
7385  -rw-    221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
7389  -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
712413184 bytes total (445063168 bytes free)
switch#
```

## Changing Directories and Displaying the Working Directory (CLI)

Follow these steps to change directories and to display the working directory:

### SUMMARY STEPS

1. **enable**
2. **dir filesystem:**
3. **cd directory\_name**
4. **pwd**
5. **cd**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>dir filesystem:</b>  <b>Example:</b> Switch# dir flash:	Displays the directories on the specified file system.  For <i>filesystem:</i> , use flash: for the system board flash device.  To access flash partitions of switch members in a stack, use flash- <i>n</i> where <i>n</i> is the stack member number. For example, flash-4.
<b>Step 3</b>	<b>cd directory_name</b>  <b>Example:</b> Switch# cd new_configs	Navigates to the specified directory.  The command example shows how to navigate to the directory named <i>new_configs</i> .
<b>Step 4</b>	<b>pwd</b>  <b>Example:</b> Switch# pwd	Displays the working directory.
<b>Step 5</b>	<b>cd</b>  <b>Example:</b> Switch# cd	Navigates to the default directory.

## Creating Directories (CLI)

Beginning in privileged EXEC mode, follow these steps to create a directory:

## SUMMARY STEPS

1. **dir filesystem:**
2. **mkdir directory\_name**
3. **dir filesystem:**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>dir</b> <i>filesystem:</i>  <b>Example:</b> Switch# dir flash:	Displays the directories on the specified file system.  For <i>filesystem:</i> , use flash: for the system board flash device.
Step 2	<b>mkdir</b> <i>directory_name</i>  <b>Example:</b> Switch# 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	<b>dir</b> <i>filesystem:</i>  <b>Example:</b> Switch# 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.

Network file system URLs include ftp:, rcp:, and tftp: and have these syntaxes:

- FTP—ftp:[[/username [:password]@location]/directory]/filename
- RCP—rcp:[[/username@location]/directory]/filename
- TFTP—tftp:[[/location]/directory]/filename

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
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

## Copying Files from One Switch in a Stack to Another Switch in the Same Stack

To copy a file from one switch in a stack to another switch in the same stack, use the **flash-X:** notation, where **X** is the switch number.

To view all switches in a stack, use the **show switch** command in privileged EXEC mode, as in the following example of a 9-member switch stack:

```
Switch# show switch
Switch/Stack Mac Address : 0006.f6b9.b580 - Local Mac Address Mac persistency wait time:
Indefinite
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
*1	Active	0006.f6b9.b580	15	P3B	Ready
2	Standby	0006.f6ba.0c80	14	P3B	Ready
3	Member	0006.f6ba.3300	7	P3B	Ready
4	Member	0006.f6b9.df80	6	P3B	Ready
5	Member	0006.f6ba.3880	13	P1A	Ready
6	Member	1ce6.c7b6.ef00	4	PP	Ready
7	Member	2037.06ce.2580	3	P2A	Ready
8	Member	2037.0653.7e00	2	P5A	Ready
9	Member	2037.0653.9280	1	P5B	Ready

To view all file systems available to copy on a specific switch, use the **copy** command as in the following example of a 5-member stack:

```
Switch# copy flash: ?
crashinfo-1: Copy to crashinfo-1: file system
crashinfo-2: Copy to crashinfo-2: file system
crashinfo-3: Copy to crashinfo-3: file system
crashinfo-4: Copy to crashinfo-4: file system
crashinfo-5: Copy to crashinfo-5: file system
crashinfo: Copy to crashinfo: file system
flash-1: Copy to flash-1: file system
flash-2: Copy to flash-2: file system
flash-3: Copy to flash-3: file system
flash-4: Copy to flash-4: file system
flash-5: Copy to flash-5: 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
revrcsf: Copy to revrcsf: file system
```

```

running-config  Update (merge with) current system configuration
scp:            Copy to scp: file system
startup-config  Copy to startup configuration
stby-crashinfo: Copy to stby-crashinfo: file system
stby-flash:     Copy to stby-flash: file system
stby-nvram:     Copy to stby-nvram: file system
stby-rcsf:      Copy to stby-rcsf: file system
stby-usbflash0: Copy to stby-usbflash0: file system
syslog:         Copy to syslog: file system
system:         Copy to system: file system
tftp:           Copy to tftp: file system
tmpsyst:        Copy to tmpsys: file system
usbflash0-1:   Copy to usbflash0-1: file system
usbflash0-2:   Copy to usbflash0-2: file system
usbflash0-3:   Copy to usbflash0-3: file system
usbflash0-4:   Copy to usbflash0-4: file system
usbflash0-5:   Copy to usbflash0-5: file system
usbflash0:     Copy to usbflash0: file system

```

Switch#

This example shows how to copy a config file stored in the flash partition of switch 2 to the flash partition of switch 4. It assumes that switch 2 and switch 4 are in the same stack.

```
Switch# copy flash-2:config.txt flash-4:config.txt
```

## 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 switch 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:

```
Switch# delete myconfig
```

## Creating, Displaying and Extracting Files (CLI)

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:

## SUMMARY STEPS

1. **archive tar /create** *destination-url* **flash:** */file-url*
2. **archive tar /table** *source-url*
3. **archive tar /xtract** *source-url* **flash:***/file-url* [*dir/file...*]
4. **more** [ */ascii* | */binary* | */ebcdic* ] */file-url*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>archive tar /create</b> <i>destination-url</i> <b>flash:</b> <i>/file-url</i></p> <p><b>Example:</b></p> <pre>switch# 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"> <li>• Local flash file system syntax: <b>flash:</b></li> <li>• FTP syntax: <b>ftp:</b><i>[[//username[:password]@location]/directory]/-filename.</i></li> <li>• RCP syntax: <b>rcp:</b><i>[[//username@location]/directory]/-filename.</i></li> <li>• TFTP syntax: <b>tftp:</b><i>[[//location]/directory]/-filename.</i></li> </ul> <p>For <b>flash:</b><i>/file-url</i>, 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><b>archive tar /table</b> <i>source-url</i></p> <p><b>Example:</b></p> <pre>switch# 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"> <li>• Local flash file system syntax: <b>flash:</b></li> <li>• FTP syntax: <b>ftp:</b><i>[[//username[:password]@location]/directory]/-filename.</i></li> <li>• RCP syntax: <b>rcp:</b><i>[[//username@location]/directory]/-filename.</i></li> <li>• TFTP syntax: <b>tftp:</b><i>[[//location]/directory]/-filename.</i></li> </ul>



	Command or Action	Purpose
		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.
<b>Step 3</b>	<b>archive tar /xtract</b> <i>source-url</i> <b>flash:</b> <i>/file-url [dir/file...]</i>  <b>Example:</b>  <pre>switch# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs</pre>	<p>Extracts a file into a directory on the flash file system.</p> <p>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:</p> <ul style="list-style-type: none"> <li>Local flash file system syntax:  <b>flash:</b></li> <li>FTP syntax:  <b>ftp:</b><i>[[/username[:password]@location]/directory]/-filename.</i></li> <li>RCP syntax:  <b>rnp:</b><i>[[/username@location]/directory]/-filename.</i></li> <li>TFTP syntax:  <b>tftp:</b><i>[[/location]/directory]/-filename.</i></li> </ul> <p>For <b>flash:</b><i>/file-url [dir/file...]</i>, 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.</p>
<b>Step 4</b>	<b>more</b> [ /ascii   /binary   /ebcdic ] <i>/file-url</i>  <b>Example:</b>  <pre>switch# more flash:/new-configs</pre>	Displays the contents of any readable file, including a file on a remote file system.

## Additional References

### Related Documents

Related Topic	Document Title
Commands for managing flash: file systems	<i>Cisco IOS Configuration Fundamentals Command Reference</i>

**Error Message Decoder**

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

**Standards**

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

**MIBs**

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**RFCs**

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

**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>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>





## CHAPTER 21

# Working with Cisco IOS XE Software Bundles

- [About Software Bundles and Packages, page 311](#)
- [Bundle and Package File Location on the Switch, page 311](#)
- [Upgrading Cisco IOS XE Software, page 312](#)
- [Additional References, page 320](#)

## About Software Bundles and Packages

Cisco IOS XE software bundles include a set of Cisco IOS XE package (.pkg) files. You can install the package files on the switch or you can boot the switch from the IOS XE bundle itself.

To display information about the contents of a Cisco IOS XE bundle (.bin file), use the **show software package** command in privileged EXEC mode. Use the command to display information about an individual IOS XE package (.pkg) file as well.

## Bundle and Package File Location on the Switch

When the switch is running in installed mode, the Cisco IOS XE package (.pkg) files and provisioning file (packages.conf) are stored in the system board flash memory (flash:). When the switch is running in bundle mode, the booted Cisco IOS XE software bundle (.bin) file is stored in the system board flash memory (flash:) or USB flash memory (usbflash0:).

To display information about the provisioning software that is currently running on the switch, use the **show version** privileged EXEC command. In the display, check the line that begins with

```
System bundle file is....
```

When the switch is running in installed mode, this line displays the name and location of the booted Cisco IOS XE provisioning file, typically flash:packages.conf.

When the switch is running in bundle mode, this line displays the name and location of the booted Cisco IOS XE bundle file.

To display information about the Cisco IOS XE package files that are running on the switch, use the **show version running** privileged EXEC command.

When the switch is running in installed mode, this command displays information about the set of package files contained in the booted provisioning file.

When the switch is running in bundle mode, this command displays information about the set of package files contained in the booted Cisco IOS XE software bundle.

**Note**

For `usbflash0:`, the default format is FAT16, while FAT32 format is also supported.

```
Switch# format usbflash0: ?
FAT16  FAT16  filesystem type
FAT32  FAT32  filesystem type
```

## Upgrading Cisco IOS XE Software

The method that you use to upgrade Cisco IOS XE software depends on whether the switch is running in installed mode or in bundle mode.

### Upgrading Cisco IOS XE Software: Install Mode

To upgrade the Cisco IOS XE software when the switch is running in installed mode, use the **software install** privileged EXEC command to install the packages from a new software bundle file. The software bundle can be installed from the local storage media or it can be installed over the network using TFTP or FTP.

The **software install** command expands the package files from the specified source bundle file and copies them to the local flash: storage device. When the source bundle is specified as a tftp: or ftp: URL, the bundle file is first downloaded into the switch's memory (RAM); the bundle file is not copied to local storage media.

After the package files are expanded and copied to flash: the running provisioning file (`flash:packages.conf`) is updated to reflect the newly installed packages, and the switch displays a reload prompt.

**Note**

The **software install** command is not supported when the switch is running in bundle mode. Use the **software expand** privileged EXEC command to convert the switch from bundle mode to installed mode.

### Upgrading Cisco IOS XE Software Install Mode Example

This example shows the **software install file** command being used to expand and copy the packages from a Cisco IOS XE bundle located on a TFTP server in order to upgrade to a new image:

```
Switch#
software install file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
Preparing install operation ...
[1]: Downloading file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
to active switch 1
[1]: Finished downloading file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
to active switch 1
[1]: Starting install operation
[1]: Expanding bundle cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
[1]: Copying package files
```

```
[1]: Package files copied
[1]: Finished expanding bundle
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
[1]: Verifying and copying expanded package files to flash:
[1]: Verified and copied expanded package files to flash:
[1]: Starting compatibility checks
[1]: Finished compatibility checks
[1]: Starting application pre-installation processing
[1]: Finished application pre-installation processing
[1]: Old files list:
Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[1]: New files list:
Added cat3k_caa-base.SPA.03.02.00.SE.pkg
Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
Added cat3k_caa-infra.SPA.03.02.00SE.pkg
Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
Added cat3k_caa-wcm.SPA.03.02.00.SE.pkg
[1]: Creating pending provisioning file
[1]: Finished installing software. New software will load on reboot.
[1]: Setting rollback timer to 45 minutes
[1]: Do you want to proceed with reload? [yes/no]:
```

## Upgrading Cisco IOS XE Software: Bundle Mode

To upgrade the Cisco IOS XE software when the switch is running in bundle mode, follow these steps:

- 1 Download the bundle file to local storage media.
- 2 Configure the **boot system** global configuration command to point to the bundle file.
- 3 Reload the switch.

### Upgrading Cisco IOS XE Software Bundle Mode Example

This example shows the steps to upgrade the Cisco IOS XE software on a switch that is running in bundle mode. It shows using the **copy** command to copy the bundle file to flash:, configuring the boot system variable to point to the bundle file, saving a copy of the running configuration, and finally, reloading the switch.

```
Switch#
copy
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
flash:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Accessing
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...Loading
/tftpboot/cstohs/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
from 172.19.211.47 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK - 220766688 bytes]
220766688 bytes copied in 124.330 secs (1775651 bytes/sec)

Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# boot system switch all
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
Switch(config)# end
Switch#
```

```
*Nov 19 14:02:42.441: %SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch# write memory
Building configuration...
Compressed configuration from 4941 bytes to 2236 bytes[OK]

Switch# reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
```

## Converting from the Bundle Running Mode to the Install Running Mode

To convert the running mode of a switch from bundle mode to installed mode, use the **software expand running** privileged EXEC command. This command expands the packages from the booted IOS XE software bundle and copies them and the provisioning file to the specified destination.

When you use the **software expand running** command to convert the switch from bundle mode to installed mode, specify the **to** destination as **flash:**. After you execute the command, configure the **boot system** command to point to the expanded provisioning file (flash:packages.conf), then reload the switch to boot in installed mode.



### Note

The **software expand running** command is not supported when the switch is running in installed mode.

## Converting from the Bundle Running Mode to the Install Running Mode Example

This example shows using the **software expand running to** command to convert the active switch in a switch stack from the bundle running mode to the installed running mode:

```
Switch# dir flash:
Directory of flash:/
 7386 -rwx      2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
 7378 drwx         4096 Jan 23 2013 09:35:11 +00:00 mnt
 7385 -rw-      221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 7389 -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
712413184 bytes total (445063168 bytes free)

Switch#
Switch# software expand running to flash:
Preparing expand operation ...
[2]: Expanding the running bundle
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding the running bundle
Switch#
Switch# dir flash:
Directory of flash:/
 7386 -rwx      2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
 7378 drwx         4096 Jan 23 2013 09:35:11 +00:00 mnt
 7385 -rw-      221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 7391 -rw-      74410468 Jan 23 2013 14:16:57 +00:00 cat3k_caa-base.SPA.03.02.00SE.pkg
 7392 -rw-      2773680 Jan 23 2013 14:16:57 +00:00 cat3k_caa-drivers.SPA.03.02.00.SE.pkg
 7393 -rw-      32478044 Jan 23 2013 14:16:57 +00:00 cat3k_caa-infra.SPA.03.02.00SE.pkg
 7394 -rw-      30393116 Jan 23 2013 14:16:57 +00:00 cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg

 7389 -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
```



```

7395 -rw-      18313952 Jan 23 2013 14:16:57 +00:00 cat3k_caa-platform.SPA.03.02.00.SE.pkg
7396 -rw-      63402700 Jan 23 2013 14:16:57 +00:00 cat3k_caa-wcm.SPA.10.0.100.0.pkg
7388 -rw-           1218 Jan 23 2013 14:17:43 +00:00 packages.conf
712413184 bytes total (223019008 bytes free)

```

```

Switch#
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# boot system switch all flash:packages.conf
Switch(config)# end
Switch#

*Jan 23 14:28:47.722: %SYS-5-CONFIG_I: Configured from console by console

Switch# write memory
Building configuration...
Compressed configuration from 4851 bytes to 2187 bytes[OK]

Switch#
Switch# reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

```

## Copying IOS XE Package and Bundle Files from One Stack Member to Another

For switch stacks running in installed mode, use the **software install source switch** privileged EXEC command to install the running software packages from an existing stack member to one or more other stack members that are running different (but compatible) software packages.

### Copying IOS XE Package and Bundle Files from One Stack Member to Another Example

This example shows a 2-member stack where each switch is running a different (but compatible) software package. The **software install source switch** command is used to install the packages that are currently running on the standby switch (switch 1) onto the active switch (switch 2):

```

Switch# show version running
Package: Base, version: 03.02.00SE, status: active
File: cat3k_caa-base.SPA.03.02.00SE.pkg, on: Switch1
Built: Wed Jan 09 21:59:52 PST 2013, by: gereddy

Package: Drivers, version: 03.02.00.SE, status: active
File: cat3k_caa-drivers.SPA.03.02.00.SE.pkg, on: Switch1
Built: Wed Jan 09 22:03:41 PST 2013, by: gereddy

Package: Infra, version: 03.02.00SE, status: active
File: cat3k_caa-infra.SPA.03.02.00SE.pkg, on: Switch1
Built: Wed Jan 09 22:00:56 PST 2013, by: gereddy

Package: IOS, version: 150-1.EX, status: active
File: cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg, on: Switch1
Built: Wed Jan 09 22:02:23 PST 2013, by: gereddy

Package: Platform, version: 03.02.00.SE, status: active
File: cat3k_caa-platform.SPA.03.02.00.SE.pkg, on: Switch1
Built: Wed Jan 09 22:01:46 PST 2013, by: gereddy

Package: WCM, version: 10.0.100.0, status: active
File: cat3k_caa-wcm.SPA.10.0.100.0.pkg, on: Switch1
Built: Wed Jan 09 22:03:05 PST 2013, by: gereddy

Switch#
Switch# software install source switch 1
Preparing install operation ...
[2]: Copying software from source switch 1 to switch 2
[2]: Finished copying software to switch 2

```

```

[2]: Starting install operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: New files list:
Added cat3k_caa-base.SPA.03.02.00.SE.pkg
Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
Added cat3k_caa-infra.SPA.03.02.00.SE.pkg
Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
Added cat3k_caa-wcm.SPA.10.0.100.0.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software. New software will load on reboot.
[2]: Committing provisioning file
[2]: Do you want to proceed with reload? [yes/no]:

```

For switch stacks running in bundle mode, follow these steps to copy the bundle file from one stack member to another:

- 1 Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
- 2 Configure the **boot system** global configuration command to point to the bundle file.
- 3 Reload the switch.

This example shows a 2-member stack where each switch is running a different (but compatible) software packages:

```

Switch# copy flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
...
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
Switch#
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
Switch(config)# end
Switch#

```

## Upgrading a Switch Running Incompatible Software

To upgrade a switch that is running in installed mode with software packages that are incompatible with the switch stack (also running in installed mode), use the **software auto-upgrade** privileged EXEC command to install the software packages from an existing stack member to the stack member that is running incompatible software. Upon completion of the auto-upgrade installation, the incompatible switch automatically reloads and joins the stack as a fully functioning member.

**Note**

If you configure the global **software auto-upgrade enable** command, the auto-upgrade functionality is initiated automatically when a switch with incompatible software running in installed mode joins the stack that is running in installed mode. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

## Upgrading a Switch Running Incompatible Software Example

This example shows a 2-member switch stack; switch 2 is the active switch and switch 1 is running incompatible software:

```
Switch# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
-----
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready
Switch#
Switch# software auto-upgrade
% Auto upgrade has been initiated for the following incompatible switches: 1

INFO level system messages will be generated to provide status information during
the auto upgrade process

Switch#
*Oct 19 06:59:14.521: %INSTALLER-6-AUTO_UPGRADE_SW_INITIATED: 2 installer: Auto upgrade
initiated for switch 1
*Oct 19 06:59:14.522: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Searching stack for software
to upgrade switch 1
*Oct 19 06:59:14.523: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Found donor switch 2 to
auto upgrade switch 1
*Oct 19 06:59:14.523: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Upgrading switch 1 with
software from switch 2
*Oct 19 07:00:47.829: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Finished installing software
on switch 1
*Oct 19 07:00:47.829: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Reloading switch 1 to
complete the auto upgrade
```

To upgrade a switch that is running in bundle mode with a software bundle that is incompatible with the switch stack (also running in bundle mode), follow these steps:

- 1 Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
- 2 Configure the **boot system** global configuration command to point to the bundle file.
- 3 Reload the switch.

This example shows a 2-member switch stack running in bundle mode; switch 2 is the active switch and switch 1 is running an incompatible bundle:

```
Switch# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
-----
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready
```

```

Switch#
Switch# copy flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
...
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)

Switch#
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
Switch(config)# end
Switch#
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
Switch# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]

```

## Upgrading a Switch Running in Incompatible Running Mode

When a switch running in bundle mode tries to join a stack running in installed mode, use the **software auto-upgrade** privileged EXEC command to install the incompatible switch's running packages and convert the switch to installed mode. Upon completion of the auto-upgrade running mode conversion, the incompatible switch automatically reloads and attempts to join the stack in installed mode.



### Note

If you configure the global **software auto-upgrade enable** command, the auto-upgrade functionality is initiated automatically when a switch with incompatible software running in installed mode joins the stack that is running in installed mode. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

## Upgrading a Switch Running in Incompatible Running Mode Example

This example shows a 2-member switch stack running in installed mode; switch 2 is the active switch and switch1 is running in bundle mode:

```

Switch# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
-----
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready

Switch#
Switch# software auto-upgrade
% Auto upgrade has been initiated for the following incompatible switches: 1

INFO level system messages will be generated to provide status information during the auto
upgrade process

Switch#
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW_INITIATED: 2 installer: Auto upgrade
initiated for switch 1
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Converting switch 1 to
installed mode by
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: installing its running
software

```

```
*Oct 19 07:18:50.488: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Setting the boot var on
switch 1
*Oct 19 07:18:51.553: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Finished installing the
running software on switch 1
*Oct 19 07:18:51.553: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Reloading switch 1 to boot
in installed mode
```

**Note**

When you use the **software auto-upgrade** command to convert an incompatible switch to installed mode, the command installs the packages from the incompatible switch's running bundle. If, after you reload and boot the incompatible switch in installed mode, the switch's installed packages are found to be incompatible with the stack, you can use the **software auto-upgrade** command again. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

To convert a switch that is running in installed mode and joining a stack that is running in bundle mode, follow these steps:

- 1 Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
- 2 Configure the **boot system** global configuration command to point to the bundle file.
- 3 Reload the switch.

After reloading, the incompatible switch boots in bundle mode and joins the stack as a fully functioning member.

This example shows a 2-member switch stack running in bundle mode; switch 2 is the active switch and switch 1 is running in installed mode:

```
Switch#
Switch# copy flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
....
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
Switch#
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
Switch(config)# end
Switch#
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
Switch# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```

# Additional References

## Related Documents

Related Topic	Document Title
Commands for managing software bundles and packages	<i>Cisco IOS Configuration Fundamentals Command Reference</i>

## Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

**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>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>







## 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.

- [Finding Feature Information](#), page 323
- [Information About Troubleshooting the Software Configuration](#), page 324
- [How to Troubleshoot the Software Configuration](#), page 331
- [Verifying Troubleshooting of the Software Configuration](#), page 344
- [Scenarios for Troubleshooting the Software Configuration](#), page 346
- [Configuration Examples for Troubleshooting Software](#), page 349
- [Additional References for Troubleshooting Software Configuration](#), page 351
- [Feature History and Information for Troubleshooting Software Configuration](#), page 352

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

#### Related Topics

[Feature History and Information for Troubleshooting Software Configuration](#), on page 352

# 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, the switch does not pass the power-on self-test (POST), and there is no connectivity.

### Related Topics

[Recovering from a Software Failure, on page 331](#)

## Lost or Forgotten Password on a Switch

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 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).

---

### Related Topics

[Recovering from a Lost or Forgotten Password, on page 333](#)

## Power over Ethernet Ports

A Power over Ethernet (PoE) switch port automatically supplies power to one of these connected devices if the switch detects that there is no power on the circuit:

- a Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- an IEEE 802.3af-compliant powered device
- an IEEE 802.3at-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

After the switch detects a powered device, the switch determines the device power requirements and then grants or denies power to the device. The switch can also detect the real-time power consumption of the device by monitoring and policing the power usage.

For more information, see the "Configuring PoE" chapter in the *Interface and Hardware Component Configuration Guide (Catalyst 3650 Switches)*.

### Related Topics

[Scenarios to Troubleshoot Power over Ethernet \(PoE\), on page 346](#)

## Disabled Port Caused by Power Loss

If a powered device (such as a Cisco IP Phone 7910) that is connected to a PoE Switch port and powered by an AC power source loses power from the AC power source, the device might enter an error-disabled state. To recover from an error-disabled state, enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface command. You can also configure automatic recovery on the Switch to recover from the error-disabled state.

On a Switch, the **errdisable recovery cause loopback** and the **errdisable recovery interval seconds** global configuration commands automatically take the interface out of the error-disabled state after the specified period of time.

## Disabled Port Caused by False Link-Up

If a Cisco powered device is connected to a port and you configure the port by using the **power inline never** interface configuration command, a false link-up can occur, placing the port into an error-disabled state. To take the port out of the error-disabled state, enter the **shutdown** and the **no shutdown** interface configuration commands.

You should not connect a Cisco powered device to a port that has been configured with the **power inline never** command.

## Ping

The Switch 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.

### Related Topics

[Executing Ping, on page 340](#)

[Example: Pinging an IP Host, on page 349](#)

## 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 Switch in the path. When the Switch detects a device in the path that does not support Layer 2 traceroute, the Switch continues to send Layer 2 trace queries and lets them time out.

The Switch 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 Switch is reachable from another Switch when you can test connectivity by using the **ping** privileged EXEC command. All Switch 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 Switch that is not in the physical path from the source device to the destination device. All Switch 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 Switch 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 Switch uses the associated MAC address and identifies the physical path.
  - If an ARP entry does not exist, the Switch 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.

## 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 Switch 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 Switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate Switch 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 Switch is a multilayer Switch that is routing a particular packet, this Switch shows up as a hop in the traceroute output.

The **traceroute** 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.

### Related Topics

[Executing IP Traceroute, on page 341](#)

[Example: Performing a Traceroute to an IP Host, on page 349](#)

## Time Domain Reflector Guidelines

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

TDR is supported on 10/100/1000 copper Ethernet ports and on Multigigabit Ethernet (100Mbps/1/2.5/5/10 Gbps) ports. It is not supported on SFP module ports.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.
- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire. If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

**Note**


---

When using the feature with Multigigabit Ethernet ports, the cable length is displayed only when an open or short condition is detected.

---

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a Switch
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

When you run TDR, the Switch reports accurate information in these situations:

- The cable for the gigabit link is a solid-core cable.
- The open-ended cable is not terminated.

When you run TDR, the Switch does not report accurate information in these situations:

- The cable for the gigabit link is a twisted-pair cable or is in series with a solid-core cable.
- The link is a 10-megabit or a 100-megabit link.
- The cable is a stranded cable.
- The link partner is a Cisco IP Phone.
- The link partner is not IEEE 802.3 compliant.

## 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.

**Related Topics**

[Redirecting Debug and Error Message Output, on page 342](#)

[Example: Enabling All System Diagnostics, on page 350](#)

## Crashinfo Files

The crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch generates two files at the time of the failure: full core and crashinfo.

The information in the crashinfo file includes the Cisco IOS image name and version that failed, a list of the processor registers, and a stack trace. You can provide this information to the Cisco technical support representative by using the **show tech-support** privileged EXEC command.

The file names have the following format:

```
[fullcore | crashinfo]_[process that crashed]_[date]-[timestamp]-UTC
```

From IOS, you can view the crashinfo files on each switch by using the following command:

```
Switch# dir crashinfo?
crashinfo-1: crashinfo-2: crashinfo-3: crashinfo:
Switch#
```

For example, to access the crashinfo directory for switch 1, enter

```
Switch dir crashinfo-1
```

From the ROMMON prompt, you can view the crashinfo files by using the **dir** command:

```
Switch: dir sda1
```

The following is sample output of a crashinfo file

```
Switch# dir crashinfo:
Directory of crashinfo:/
 12 -rwx      2768  Dec 31 1969 16:00:15 -08:00  koops.dat
 15 -rwx         0  Jan 12 2000 22:53:40 -08:00  deleted_crash_files
 16 -rwx    4246576  Jan 12 2000 22:53:40 -08:00  crashinfo_stack-mgr_20000113-065250-UTC

 17 -rwx         50  Oct 2 2012 03:18:42 -08:00  last_crashinfo
 26 -rwx         39  Jan 22 2013 14:14:14 -08:00  last_systemreport
 18 -rwx    2866565  Jan 12 2000 22:53:41 -08:00  fullcore_stack-mgr_20000113-065250-UTC

 20 -rwx    4391796  Feb 1 2000 17:50:44 -08:00  crashinfo_stack-mgr_20000202-014954-UTC

 21 -rwx    2920325  Feb 1 2000 17:50:45 -08:00  fullcore_stack-mgr_20000202-014954-UTC
34817 -rw-    1050209  Jan 10 2013 20:26:23 -08:00  system-report_1_20130111-042535-UTC.gz
18434 -rw-    1016913  Jan 11 2013 10:35:28 -08:00  system-report_1_20130111-183440-UTC.gz
18435 -rw-    1136167  Jan 22 2013 14:14:11 -08:00  system-report_1_20130122-221322-UTC.gz
34821 -rw-    1094631  Jan 2 2013 17:59:23 -08:00  system-report_1_20130103-015835-UTC.gz

 6147 -rw-    967429  Jan 3 2013 10:32:44 -08:00  system-report_1_20130103-183156-UTC.gz
34824 -rwx         50  Jan 22 2013 14:14:14 -08:00  deleted_sysreport_files
6155 -rwx         373  Jan 22 2013 14:14:13 -08:00  last_systemreport_log

145898496 bytes total (18569216 bytes free)
stack3#
```

The file name of the most recent crashinfo file is stored in last\_crashinfo.  
The file name of the most recent system report is stored in last\_systemreport.

```
Switch#
```

## System Reports

When a switch crashes, a system report is automatically generated for each switch in the switch stack. The system report file captures all the trace buffers, and other system-wide logs found on the switch. System reports are located in the crashinfo directory in the following format:

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

After a switch crash, you should check if a system report file was generated. 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 when troubleshooting your issue.

## Onboard Failure Logging on the Switch

You can use the onboard failure logging (OBFL) feature to collect information about the Switch. The information includes uptime, temperature, and voltage information and helps Cisco technical support representatives to troubleshoot Switch 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 Switch and small form-factor pluggable (SFP) modules. The Switch stores this information in the flash memory:

- CLI commands—Record of the OBFL CLI commands that are entered on a standalone Switch or a switch stack member.
- Environment data—Unique device identifier (UDI) information for a standalone Switch or a switch stack member and for all the connected FRU devices: the product identification (PID), the version identification (VID), and the serial number.
- Message—Record of the hardware-related system messages generated by a standalone Switch or a switch stack member.
- Power over Ethernet (PoE)—Record of the power consumption of PoE ports on a standalone Switch or a switch stack member.
- Temperature—Temperature of a standalone Switch or a switch stack member.
- Uptime data—Time when a standalone Switch or a switch stack member starts, the reason the Switch restarts, and the length of time the Switch has been running since it last restarted.
- Voltage—System voltages of a standalone Switch or a switch stack member.

You should manually set the system clock or configure it by using Network Time Protocol (NTP).

When the Switch is running, you can retrieve the OBFL data by using the **show logging onboard** privileged EXEC commands. If the Switch fails, contact your Cisco technical support representative to find out how to retrieve the data.

When an OBFL-enabled Switch is restarted, there is a 10-minute delay before logging of new data begins.

### Related Topics

[Configuring OBFL, on page 343](#)

[Displaying OBFL Information, on page 344](#)



## 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 Switch does not shut down, and this error message appears:

```
Multiple fan(FRU/PS) failure detected. System may get overheated. Change fan quickly.
```

The Switch might overheat and shut down.

To enable the fan failures feature, enter the **system env fan-fail-action shut** privileged EXEC command. If more than one fan in the Switch fails, the Switch automatically shuts down, and this error message appears:

```
Faulty (FRU/PS) fans detected, shutting down system!
```

After the first fan shuts down, if the Switch detects a second fan failure, the Switch waits for 20 seconds before it shuts down.

To restart the Switch, 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:

**Note**

You may see increased system memory usage when Cisco Catalyst 4500E Supervisor Engine 8-E is used in wireless mode.

- 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 Software Failure

### Before You Begin

This recovery procedure requires that you have physical access to the switch.

This procedure uses boot loader commands and TFTP to recover from a corrupted or incorrect image file.

- 
- Step 1** From your PC, download the software image file (*image.bin*) from Cisco.com.
- Step 2** Load the software image to your TFTP server.
- Step 3** Connect your PC to the switch Ethernet management port.
- Step 4** Unplug the switch power cord.
- Step 5** Press the **Mode** button, and at the same time, reconnect the power cord to the switch.
- Step 6** From the bootloader (ROMMON) prompt, ensure that you can ping your TFTP server.
- a) Set the IP address **switch: set IP\_ADDRESS *ip\_address subnet\_mask***

**Example:**

```
switch: set IP_ADDRESS 192.0.2.123/255.255.255.0
```

- b) Set the default router IP address **switch: set DEFAULT\_ROUTER *ip\_address***

**Example:**

```
switch: set DEFAULT_ROUTER 192.0.2.1
```

- c) Verify that you can ping the TFTP server **switch: ping *ip\_address\_of\_TFTP\_server***

**Example:**

```
switch: ping 192.0.2.15
ping 192.0.2.1 with 32 bytes of data...
Host 192.0.2.1 is alive.
switch:
```

- Step 7** Verify that you have a recovery image in your recovery partition (sda9:).  
This recovery image is required for recovery using the emergency-install feature.

**Example:**

```
switch: dir sda9:
Directory of sda9:/

 2  drwx  1024      .
 2  drwx  1024     ..
11  -rw- 18923068  c3850-recovery.bin

36939776 bytes available (20830208 bytes used)
switch:
```

- Step 8** From the bootloader (ROMMON) prompt, initiate the emergency-install feature that assists you in recovering the software image on your switch.

**WARNING:** The emergency install command will erase your entire boot flash!

**Example:**

```
Switch#
emergency-install
tftp://192.0.2.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
```

```
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin)...
```

```

Reading full image into memory.....done
Nova Bundle Image
-----
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

Initiating Emergency Installation of bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin

Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Package cat3k_caa-base..pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.03.02.00.SE.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.

Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@#####...+@++@++@++@++@

```

**Related Topics**

[Software Failure on a Switch, on page 324](#)

# 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.

**SUMMARY STEPS**

1. Connect a terminal or PC to the switch.
2. Set the line speed on the emulation software to 9600 baud.
3. Power off the standalone switch or the entire switch stack.
4. Reconnect the power cord to the or the active switch. Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until a prompt is seen; then release the **Mode** button.
5. After recovering the password, reload the switch or the active switch .

**DETAILED STEPS**

- 
- 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.
  - Connect a PC to the Ethernet management port.
- 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 or the active switch. Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until a prompt is seen; then release the **Mode** button.

```
Switch:
Xmodem file system is available.
Base ethernet MAC Address: 20:37:06:4d:e9:80
Verifying bootloader digital signature.
```

The system has been interrupted prior to loading the operating system software, console will be reset to 9600 baud rate.

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
```

---

### Related Topics

[Lost or Forgotten Password on a Switch, on page 324](#)

## Procedure with Password Recovery Enabled

If the password-recovery operation is enabled, this message appears:

---

**Step 1** Initialize the flash file system.

```
Switch: flash_init
```

**Step 2** Ignore the startup configuration with the following command:

```
Switch: SWITCH_IGNORE_STARTUP_CFG=1
```

**Step 3** Boot the switch with the *packages.conf* file from flash.

```
Switch: boot flash:packages.conf
```

**Step 4** Terminate the initial configuration dialog by answering **No**.

```
Would you like to enter the initial configuration dialog? [yes/no]: No
```

**Step 5** At the switch prompt, enter privileged EXEC mode.

```
Switch> enable  
Switch#
```

**Step 6** Copy the startup configuration to running configuration.

```
Switch# 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 7** Enter global configuration mode and change the **enable** password.

```
Switch# configure terminal  
Switch(config)#
```

**Step 8** Write the running configuration to the startup configuration file.

```
Switch(config)# copy running-config startup-config
```

**Step 9** Confirm that manual boot mode is enabled.

```
Switch# show boot

BOOT variable = flash:packages.conf;
Manual Boot = yes
Enable Break = yes
```

**Step 10** Reload the switch.

```
Switch# reload
```

**Step 11** Return the Bootloader parameters (previously changed in Steps 2 and 3) to their original values.

```
switch: SWITCH_IGNORE_STARTUP_CFG=0
```

**Step 12** Boot the switch with the *packages.conf* file from flash.

```
Switch: boot flash:packages.conf
```

**Step 13** After the switch boots up, disable manual boot on the switch.

```
Switch(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 Switch 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 Switch 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.

**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:

```
Switch: dir flash:
```

The Switch file system appears.

```
Directory of flash:/
.
.
.i'
15494 drwx      4096   Jan 1 2000 00:20:20 +00:00  kirch
15508 -rw-    258065648   Sep 4 2013 14:19:03 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
162196684
```

**Step 3** Boot up the system:

```
Switch: 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 Switch prompt, enter privileged EXEC mode:

```
Switch> enable
```

**Step 5** Enter global configuration mode:

```
Switch# configure terminal
```

**Step 6** Change the password:

```
Switch(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:

```
Switch(config)# exit
Switch#
```

**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:

```
Switch# copy running-config startup-config
```

The new password is now in the startup configuration.

**Step 9** You must now reconfigure the Switch. If the system administrator has the backup Switch 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 Switch 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 Switch should be green. Depending on the Switch 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 Switch in the stack can make it easier to remotely troubleshoot the switch stack. However, you need to remember that the Switch have manually assigned numbers if you add, remove, or rearrange Switch 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 Switch functions with the exact same configuration as the replaced Switch. This is also assuming the new Switch is using the same member number as the replaced Switch.



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 Switch.

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 Switch 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 Switch 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 Switch, the Switch 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 Switch 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 Switch, 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 Switch 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.

## Monitoring SFP Module Status

You can check the physical or operational status of an SFP module by using the **show interfaces transceiver** privileged EXEC command. This command shows the operational status, such as the temperature and the current for an SFP module on a specific interface and the alarm status. You can also use the command to check the speed and the duplex settings on an SFP module. For more information, see the **show interfaces transceiver** command in the command reference for this release.

## 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 Switch.



### 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 Switch:

Command	Purpose
<p><b>ping ip</b> <i>host</i>   <i>address</i></p> <p>Switch# ping 172.20.52.3</p>	Pings a remote host through IP or by supplying the hostname or network address.

### Related Topics

[Ping, on page 325](#)

[Example: Pinging an IP Host, on page 349](#)

## Monitoring Temperature

The Switch monitors the temperature conditions and uses the temperature information to control the fans.

Use the **show env temperature status** privileged EXEC command to display the temperature value, state, and thresholds. The temperature value is the temperature in the Switch (not the external temperature). You

can configure only the yellow threshold level (in Celsius) by using the **system env temperature threshold yellow value** global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds. For more information, see the command reference for this release.

## 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 34: Monitoring the Physical Path**

Command	Purpose
<b>tracetroute mac</b> [ <b>interface</b> <i>interface-id</i> ] { <i>source-mac-address</i> } [ <b>interface</b> <i>interface-id</i> ] { <i>destination-mac-address</i> } [ <b>vlan</b> <i>vlan-id</i> ] [ <b>detail</b> ]	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.
<b>tracetroute mac ip</b> { <i>source-ip-address</i>   <i>source-hostname</i> } { <i>destination-ip-address</i>   <i>destination-hostname</i> } [ <b>detail</b> ]	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 **tracetroute** privileged EXEC command, they are not supported in this release.

Command	Purpose
<b>tracetroute ip</b> <i>host</i> Switch# <code>tracetroute ip 192.51.100.1</code>	Traces the path that packets take through the network.

**Related Topics**

[IP Traceroute](#) , on page 327

[Example: Performing a Traceroute to an IP Host](#), on page 349

## Running TDR and Displaying the Results

To run TDR, enter the **test cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

To display the results, enter the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

## 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 or the Ethernet management 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*.

**Related Topics**

[Debug Commands](#), on page 328

## Using the show platform forward Command

The output from the **show platform forward** 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 Switch 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.

## Configuring OBFL

**Caution**

We recommend that you do not disable OBFL and that you do not remove the data stored in the flash memory.

- To enable OBFL, use the **hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] global configuration command. On switches, the range for *switch-number* is from 1 to 9. Use the **message level** *level* parameter to specify the severity of the hardware-related messages that the switch generates and stores in the flash memory.
- To copy the OBFL data to the local network or a specific file system, use the **copy onboard switch** *switch-number* **url** *url-destination* privileged EXEC command.
- To disable OBFL, use the **no hw-switch switch** [*switch-number*] **logging onboard** [**message level**] global configuration command.
- To clear all the OBFL data in the flash memory except for the uptime and CLI command information, use the **clear onboard switch** *switch-number* privileged EXEC command.
- In a switch stack, you can enable OBFL on a standalone switch or on all stack members by using the **hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] global configuration command.
- You can enable or disable OBFL on a member switch from the active switch.

For more information about the commands in this section, see the command reference for this release.

### Related Topics

[Onboard Failure Logging on the Switch, on page 330](#)

[Displaying OBFL Information, on page 344](#)

## WSMA Configuration for WebUI

WSMA configurations are available by default to access the Web UI. If you explicitly delete the configuration, you have to reconfigure as below:

```
Switch(config)#wsma agent exec
Switch(wsma-exec-agent)# profile httplistener
Switch(wsma-exec-agent)# profile httpslistener
Switch(wsma-exec-agent)#exit
Switch(config)#wsma agent config
Switch(wsma-config-agent)# profile httplistener
Switch(wsma-config-agent)# profile httpslistener
Switch(wsma-config-agent)#exit
```

```
Switch(config)#wsma agent filesys
Switch(wsma-filesys-agent)# profile httplistener
Switch(wsma-filesys-agent)# profile httpslistener
Switch(wsma-filesys-agent)#exit
Switch(config)#wsma agent notify
```

# Verifying Troubleshooting of the Software Configuration

## Displaying OBFL Information

**Table 35: Commands for Displaying OBFL Information**

Command	Purpose
<p><b>show onboard switch <i>switch-number</i> cliilog</b></p> <p>Switch# show onboard switch 1 cliilog</p>	Displays the OBFL CLI commands that were entered on a standalone switch or the specified stack members.
<p><b>show onboard switch <i>switch-number</i> environment</b></p> <p>Switch# show onboard switch 1 environment</p>	Displays the UDI information for a standalone switch or the specified stack members and for all the connected FRU devices: the PID, the VID, and the serial number.
<p><b>show onboard switch <i>switch-number</i> message</b></p> <p>Switch# show onboard switch 1 message</p>	Displays the hardware-related messages generated by a standalone switch or the specified stack members.
<p><b>show onboard switch <i>switch-number</i> counter</b></p> <p>Switch# show onboard switch 1 counter</p>	Displays the counter information on a standalone switch or the specified stack members.
<p><b>show onboard switch <i>switch-number</i> temperature</b></p> <p>Switch# show onboard switch 1 temperature</p>	Displays the temperature of a standalone switch or the specified switch stack members.
<p><b>show onboard switch <i>switch-number</i> uptime</b></p> <p>Switch# show onboard switch 1 uptime</p>	Displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or specified stack members restart, and the length of time that the standalone switch or specified stack members have been running since they last restarted.
<p><b>show onboard switch <i>switch-number</i> voltage</b></p> <p>Switch# show onboard switch 1 voltage</p>	Displays the system voltages of a standalone switch or the specified stack members.

Command	Purpose
<b>show onboard switch <i>switch-number</i> status</b> Switch# show onboard switch 1 status	Displays the status of a standalone switch or the specified stack members.

**Related Topics**

- [Onboard Failure Logging on the Switch, on page 330](#)
- [Configuring OBFL, on page 343](#)

## 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.

```
Switch# 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 36: 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.”

# Scenarios for Troubleshooting the Software Configuration

## Scenarios to Troubleshoot Power over Ethernet (PoE)

*Table 37: Power over Ethernet Troubleshooting Scenarios*

Symptom or Problem	Possible Cause and Solution
<p>Only one port does not have PoE.</p> <p>Trouble is on only one switch port.</p> <p>PoE and non-PoE devices do not work on this port, but do on other ports.</p>	<p>Verify that the powered device works on another PoE port.</p> <p>Use the <b>show run</b>, or <b>show interface status</b> user EXEC commands to verify that the port is not shut down or error-disabled.</p> <p><b>Note</b> Most switches turn off port power when the port is shut down, even though the IEEE specifications make this optional.</p> <p>Verify that <b>power inline never</b> is not configured on that interface or port.</p> <p>Verify that the Ethernet cable from the powered device to the switch port is good: Connect a known good non-PoE Ethernet device to the Ethernet cable, and make sure that the powered device establishes a link and exchanges traffic with another host.</p> <p><b>Note</b> Cisco powered device works only with straight cable and not with crossover one.</p> <p>Verify that the total cable length from the switch front panel to the powered device is not more than 100 meters.</p> <p>Disconnect the Ethernet cable from the switch port. Use a short Ethernet cable to connect a known good Ethernet device directly to this port on the switch front panel (not on a patch panel). Verify that it can establish an Ethernet link and exchange traffic with another host, or ping the port VLAN SVI. Next, connect a powered device to this port, and verify that it powers on.</p> <p>If a powered device does not power on when connected with a patch cord to the switch port, compare the total number of connected powered devices to the switch power budget (available PoE). Use the <b>show inline power</b> command to verify the amount of available power.</p>



Symptom or Problem	Possible Cause and Solution
<p>No PoE on all ports or a group of ports.</p> <p>Trouble is on all switch ports.</p> <p>Nonpowered Ethernet devices cannot establish an Ethernet link on any port, and PoE devices do not power on.</p>	<p>If there is a continuous, intermittent, or reoccurring alarm related to power, replace the power supply if possible it is a field-replaceable unit. Otherwise, replace the switch.</p> <p>If the problem is on a consecutive group of ports but not all ports, the power supply is probably not defective, and the problem could be related to PoE regulators in the switch.</p> <p>Use the <b>show log</b> privileged EXEC command to review alarms or system messages that previously reported PoE conditions or status changes.</p> <p>If there are no alarms, use the <b>show interface status</b> command to verify that the ports are not shut down or error-disabled. If ports are error-disabled, use the <b>shut</b> and <b>no shut</b> interface configuration commands to reenabte the ports.</p> <p>Use the <b>show env power</b> and <b>show power inline</b> privileged EXEC commands to review the PoE status and power budget (available PoE).</p> <p>Review the running configuration to verify that <b>power inline never</b> is not configured on the ports.</p> <p>Connect a nonpowered Ethernet device directly to a switch port. Use only a short patch cord. Do not use the existing distribution cables. Enter the <b>shut</b> and <b>no shut</b> interface configuration commands, and verify that an Ethernet link is established. If this connection is good, use a short patch cord to connect a powered device to this port and verify that it powers on. If the device powers on, verify that all intermediate patch panels are correctly connected.</p> <p>Disconnect all but one of the Ethernet cables from switch ports. Using a short patch cord, connect a powered device to only one PoE port. Verify the powered device does not require more power than can be delivered by the switch port.</p> <p>Use the <b>show power inline</b> privileged EXEC command to verify that the powered device can receive power when the port is not shut down. Alternatively, watch the powered device to verify that it powers on.</p> <p>If a powered device can power on when only one powered device is connected to the switch, enter the <b>shut</b> and <b>no shut</b> interface configuration commands on the remaining ports, and then reconnect the Ethernet cables one at a time to the switch PoE ports. Use the <b>show interface status</b> and <b>show power inline</b> privileged EXEC commands to monitor inline power statistics and port status.</p> <p>If there is still no PoE at any port, a fuse might be open in the PoE section of the power supply. This normally produces an alarm. Check the log again for alarms reported earlier by system messages.</p>

Symptom or Problem	Possible Cause and Solution
<p>Cisco pre-standard powered device disconnects or resets.</p> <p>After working normally, a Cisco phone intermittently reloads or disconnects from PoE.</p>	<p>Verify all electrical connections from the switch to the powered device. Any unreliable connection results in power interruptions and irregular powered device functioning such as erratic powered device disconnects and reloads.</p> <p>Verify that the cable length is not more than 100 meters from the switch port to the powered device.</p> <p>Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs.</p> <p>Notice whether any error messages appear at the same time a disconnect occurs. Use the <b>show log</b> privileged EXEC command to review error messages.</p> <p>Verify that an IP phone is not losing access to the Call Manager immediately before the reload occurs. (It might be a network problem and not a PoE problem.)</p> <p>Replace the powered device with a non-PoE device, and verify that the device works correctly. If a non-PoE device has link problems or a high error rate, the problem might be an unreliable cable connection between the switch port and the powered device.</p>
<p>IEEE 802.3af-compliant or IEEE 802.3at-compliant powered devices do not work on Cisco PoE switch.</p> <p>A non-Cisco powered device is connected to a Cisco PoE switch, but never powers on or powers on and then quickly powers off. Non-PoE devices work normally.</p>	<p>Use the <b>show power inline</b> command to verify that the switch power budget (available PoE) is not depleted before or after the powered device is connected. Verify that sufficient power is available for the powered device type before you connect it.</p> <p>Use the <b>show interface status</b> command to verify that the switch detects the connected powered device.</p> <p>Use the <b>show log</b> command to review system messages that reported an overcurrent condition on the port. Identify the symptom precisely: Does the powered device initially power on, but then disconnect? If so, the problem might be an initial surge-in (or <i>inrush</i>) current that exceeds a current-limit threshold for the port.</p>

**Related Topics**

[Power over Ethernet Ports, on page 324](#)

# Configuration Examples for Troubleshooting Software

## Example: Pinging an IP Host

This example shows how to ping an IP host:

```
Switch# 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
Switch#
```

**Table 38: 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.

### Related Topics

- [Ping, on page 325](#)
- [Executing Ping, on page 340](#)

## Example: Performing a Traceroute to an IP Host

This example shows how to perform a **traceroute** to an IP host:

```
Switch# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10
```

```

1 192.0.2.1 0 msec 0 msec 4 msec
2 192.0.2.203 12 msec 8 msec 0 msec
3 192.0.2.100 4 msec 0 msec 0 msec
4 192.0.2.10 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 39: 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.

#### Related Topics

[IP Traceroute](#), on page 327

[Executing IP Traceroute](#), on page 341

## Example: Enabling All System Diagnostics



#### Caution

Because debugging output takes priority over other network traffic, and because the **debug all** privileged EXEC command generates more output than any other **debug** command, it can severely diminish switch performance or even render it unusable. In virtually all cases, it is best to use more specific **debug** commands.

This command disables all-system diagnostics:

```
Switch# debug all
```

The **no debug all** privileged EXEC command disables all diagnostic output. Using the **no debug all** command is a convenient way to ensure that you have not accidentally left any **debug** commands enabled.

**Related Topics**

[Debug Commands, on page 328](#)

# Additional References for Troubleshooting Software Configuration

**Related Documents**

Related Topic	Document Title
System management commands	<i>System Management Command Reference (Catalyst 3650 Switches)</i>
Platform-independent command reference	<i>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>
Platform_independent configuration information	<i>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>

**Standards and RFCs**

Standard/RFC	Title
None	—

**MIBs**

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**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>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>

## Feature History and Information for Troubleshooting Software Configuration

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.

**Related Topics**

[Finding Feature Information, on page 21](#)



## INDEX

802.11h, described [117](#)  
802.11n [117](#)  
    devices [117](#)

### A

access points [143](#)  
    assisted roaming [143](#)  
access template [205](#)  
activation, AP-count [99](#)  
activation, base [97](#)  
address resolution [29](#)  
addresses [27, 28, 29, 49](#)  
    dynamic [27, 28](#)  
        defined [27](#)  
        learning [28](#)  
    MAC, discovering [29](#)  
    static [49](#)  
        adding and removing [49](#)  
aging time [41](#)  
    MAC address table [41](#)  
and ARP [326](#)  
and CDP [326](#)  
ARP [29](#)  
    defined [29](#)  
    table [29](#)  
        address resolution [29](#)  
authoritative time source, described [22](#)  
autonegotiation [339](#)  
    mismatches [339](#)

### B

banners [27, 38, 39](#)  
    configuring [38, 39](#)  
        login [39](#)  
        message-of-the-day login [38](#)  
    default configuration [27](#)  
broadcast traffic [326](#)

bundle files [311](#)  
    displaying contents of [311](#)  
    downloading [311](#)  
    uploading [311](#)

### C

CCX Layer 2 client roaming [143](#)  
    described [143](#)  
clock [22](#)  
    See system clock [22](#)  
command modes [240](#)  
    global configuration [240](#)  
comments [240, 247](#)  
    adding to configuration file [240](#)  
    adding to configuration files [247](#)  
CONFIG\_FILE environment variable [273](#)  
    specifying [273](#)  
configuration archive [285](#)  
    creating [285](#)  
Configuration Examples for Configuring SDM Templates  
command [209](#)  
configuration files [240, 241, 242, 244, 245, 246, 249, 250, 252, 254, 260, 265, 266, 267, 273, 275, 277, 303](#)  
    compressing [260](#)  
    CONFIG\_FILE environment variable [273](#)  
    copying [241, 242, 249, 254, 265, 266, 267](#)  
        between Flash memory devices [266](#)  
        from a network server [241, 267](#)  
        from a TFTP server [254](#)  
        from Flash memory [265](#)  
        to a TFTP server [242, 249](#)  
        to an rcp server [242](#)  
    displaying [246](#)  
        information [246](#)  
    downloading [245, 277](#)  
        host configuration files [277](#)  
    failing to load [275](#)  
    host [277](#)  
        See host configuration file [277](#)  
    invalid combinations when copying [303](#)

configuration files (*continued*)  
 larger than NVRAM [244, 260](#)  
 location [241](#)  
 modifying [240](#)  
 network [246](#)  
   See network configuration file [246](#)  
 running [250, 252](#)  
   See also running configuration [250, 252](#)  
 storing in Flash memory [245](#)  
 types [240](#)

configuring [207](#)

Configuring SDM templates [209](#)  
 Examples [209](#)  
   command [209](#)

copy rcp command [267](#)

copy rcp running-config command [256, 258](#)

copy rcp startup-config command [256, 258](#)

copy running-config rcp command [250](#)

copy running-config tftp command [249](#)

copy startup-config command [262](#)

copy startup-config rcp command [250, 252](#)

copy startup-config tftp command [249](#)

copy tftp startup-config command [254](#)

corrupted software, recovery steps with Xmodem [331](#)

crashinfo file [329](#)

crashinfo, description [329](#)

## D

daylight saving time [31](#)

debugging [328, 342, 350](#)  
 enabling all system diagnostics [350](#)  
 redirecting error message output [342](#)  
 using commands [328](#)

default configuration [27, 28](#)  
 banners [27](#)  
 DNS [27](#)  
 MAC address table [28](#)

described [227, 326, 330](#)

directed roam request [144](#)

directories [301, 302, 303](#)  
 changing [301](#)  
 creating [302](#)  
 displaying the working [301](#)  
 removing [303](#)

displaying [344](#)

displaying crash information [329](#)

Displaying SDM Templates [209](#)  
 Examples [209](#)  
   command [209](#)

DNS [26, 27, 36](#)  
 default configuration [27](#)

DNS (*continued*)  
 overview [26](#)  
 setting up [36](#)

Domain Name System [26](#)  
 See DNS [26](#)

domain names [26](#)  
 DNS [26](#)

## E

enable [343](#)

enabling all system diagnostics [350](#)

enhanced neighbor list [143, 144](#)  
 request (E2E) [144](#)  
 described [143](#)

erase command [272](#)

erase startup-config command [271](#)

Example for Performing a Traceroute to an IP Host command [349](#)

Example for Pinging an IP Host command [349](#)

executing [340, 341](#)

extended crashinfo file [329](#)

## F

file system [298, 300, 303](#)  
 displaying available file systems [298](#)  
 displaying file information [300](#)  
 local file system names [298](#)  
 network file system names [303](#)  
 setting the default [300](#)

files [303, 305, 329](#)  
 copying [303](#)  
 crashinfo, description [329](#)  
 deleting [305](#)  
 tar [305](#)  
   creating [305](#)  
   displaying the contents of [305](#)  
   extracting [305](#)

flash [297](#)  
 file system [297](#)

flash device, [298](#)  
 number of [298](#)

flash memory [330](#)

Flash memory [245](#)  
 storing configuration files [245](#)

Flash memory devices [266](#)  
 files [266](#)  
   copying [266](#)

FTP Server [277](#)  
 configuration files, downloading [277](#)



- G**
- global configuration mode [240](#)
    - entering [240](#)
- H**
- host configuration files [246, 257, 259, 277](#)
    - comparison with network configuration files [246](#)
    - copying from an rcp server to startup configuration (example) [257, 259](#)
    - description [246](#)
    - loading from a server [277](#)
- I**
- ICMP [327](#)
    - time-exceeded messages [327](#)
    - traceroute and [327](#)
  - ICMP ping [325, 340](#)
    - executing [340](#)
    - overview [325](#)
  - inter-subnet roaming [143](#)
    - described [143](#)
  - IP addresses [29](#)
    - discovering [29](#)
  - IP addresses and subnets [326](#)
  - IP traceroute [327, 341](#)
    - executing [341](#)
    - overview [327](#)
- L**
- Layer 2 traceroute [326](#)
    - and ARP [326](#)
    - and CDP [326](#)
    - broadcast traffic [326](#)
    - described [326](#)
    - IP addresses and subnets [326](#)
    - MAC addresses and VLANs [326](#)
    - multicast traffic [326](#)
    - multiple devices on a port [326](#)
    - unicast traffic [326](#)
    - usage guidelines [326](#)
  - license ap-count activation [99](#)
  - license base image activation [97](#)
  - login banners [27](#)
- M**
- MAC addresses [28, 29, 41, 49](#)
    - aging time [41](#)
    - and VLAN association [28](#)
    - building the address table [28](#)
    - default configuration [28](#)
    - discovering [29](#)
    - dynamic [28](#)
      - learning [28](#)
    - static [49](#)
      - characteristics of [49](#)
  - MAC addresses and VLANs [326](#)
  - messages, to users through banners [27](#)
  - mismatches [339](#)
  - mismatches, autonegotiation [339](#)
  - monitoring [340](#)
    - SFP status [340](#)
  - monitoring status of [340](#)
  - multicast traffic [326](#)
  - multiple devices on a port [326](#)
- N**
- network configuration files [246](#)
    - comparison with host configuration files [246](#)
    - description [246](#)
  - Network Mobility Services Protocol (NMSP) [194](#)
    - modifying the notification interval for clients, RFID tags, and rogues [194](#)
  - NTP [22, 24](#)
    - associations [24](#)
      - defined [24](#)
    - overview [22](#)
    - time [24](#)
      - services [24](#)
  - number of [205](#)
  - NVRAM [260](#)
    - file compression [260](#)
- O**
- OBFL [330, 343, 344](#)
    - configuring [343](#)
    - described [330](#)
    - displaying [344](#)
  - on-board failure logging [330](#)
  - online diagnostics [227](#)
    - described [227](#)
    - overview [227](#)
  - optimizing system resources [205](#)

overview [227, 325, 327](#)

## P

partitioned [338](#)

passwords [324](#)

recovery of [324](#)

ping [325, 340, 349](#)

character output description [349](#)

executing [340](#)

overview [325](#)

PoE ports [324](#)

## R

rcp (remote copy protocol) [242](#)

server [242](#)

configuration files, copying [242](#)

recovery of [324](#)

recovery procedures [331](#)

redirecting error message output [342](#)

RFC [22](#)

1305, NTP [22](#)

Right-To-Use [93, 94, 95, 97, 99](#)

AP-count activation [99](#)

base image activation [97](#)

evaluation license [94](#)

image based licenses [94](#)

license overview [94](#)

license states [95](#)

permanent license [94](#)

restrictions [93](#)

switch stacks [95](#)

roam reason report [144](#)

rsh (remote shell) [242](#)

running configuration [250, 254, 257, 259](#)

copying [250, 254, 257, 259](#)

from an rcp server (example) [257, 259](#)

to an rcp server [250, 254](#)

## S

SDM [205, 207](#)

templates [205, 207](#)

configuring [207](#)

number of [205](#)

SDM template [205, 207](#)

configuring [207](#)

types of [205](#)

SDM template selection [207](#)

security and identification [339](#)

See also downloading and uploading[software images [331](#)

See also IP traceroute [327](#)

service compress-config command [260](#)

setting packet forwarding [342](#)

SFP security and identification [339](#)

SFP status [340](#)

SFPs [339, 340](#)

monitoring status of [340](#)

security and identification [339](#)

status, displaying [340](#)

show forward command [342](#)

show platform forward command [342](#)

SNMP [42, 44, 46](#)

traps [42, 44, 46](#)

enabling MAC address notification [42, 44, 46](#)

software images [331](#)

recovery procedures [331](#)

See also downloading and uploading[software images [331](#)

stack changes, effects on [28, 207](#)

MAC address tables [28](#)

SDM template selection [207](#)

stacks [315, 317, 318](#)

copying a bundle file from one member to another [315](#)

upgrading [315](#)

upgrading, incompatible running mode [318](#)

upgrading, incompatible software [317](#)

stacks, switch [26, 28, 338](#)

MAC address considerations [28](#)

partitioned [338](#)

system prompt consideration [26](#)

startup configuration [241, 252, 254, 257, 259, 271](#)

clearing [271](#)

copying configuration files to [241](#)

copying from an rcp server [257, 259](#)

(example) [257, 259](#)

copying to an rcp server (example) [252, 254](#)

re-executing configuration commands in [271](#)

static addresses [27](#)

See addresses [27](#)

status, displaying [340](#)

stratum, NTP [24](#)

summer time [31](#)

switch stack [343](#)

switch stack licenses [95](#)

system clock [22, 29, 30, 31](#)

configuring [29, 30, 31](#)

daylight saving time [31](#)

manually [29](#)

summer time [31](#)

time zones [30](#)

overview [22](#)

system name [26, 35](#)

default configuration [26](#)

system name *(continued)*

manual configuration [35](#)

system prompt, default setting [26](#)

system resources, optimizing [205](#)

## T

tar files [305](#)

creating [305](#)

displaying the contents of [305](#)

extracting [305](#)

templates [205, 207](#)

configuring [207](#)

number of [205](#)

TFTP server [242, 249, 254, 277](#)

configuration files [242, 249, 254, 277](#)

copying from [254](#)

copying to [242, 249](#)

downloading [277](#)

time [21](#)

See NTP and system clock [21](#)

time zones [30](#)

time-exceeded messages [327](#)

traceroute and [327](#)

traceroute command [327](#)

See also IP traceroute [327](#)

traceroute, Layer 2 [326](#)

and ARP [326](#)

and CDP [326](#)

broadcast traffic [326](#)

described [326](#)

IP addresses and subnets [326](#)

MAC addresses and VLANs [326](#)

multicast traffic [326](#)

multiple devices on a port [326](#)

unicast traffic [326](#)

usage guidelines [326](#)

traffic stream metrics (TSM) [167](#)

described [167](#)

traps [42, 44, 46](#)

configuring MAC address notification [42, 44, 46](#)

traps *(continued)*

enabling [42, 44, 46](#)

troubleshooting [325, 327, 328, 329, 339, 342](#)

displaying crash information [329](#)

setting packet forwarding [342](#)

SFP security and identification [339](#)

show forward command [342](#)

with debug commands [328](#)

with ping [325](#)

with traceroute [327](#)

Troubleshooting Examples command [349](#)

types of [205](#)

## U

U-APSD [167](#)

described [167](#)

unicast MAC address filtering [50](#)

configuration [50](#)

unicast traffic [326](#)

upgrading software [312, 313, 316, 318](#)

bundle mode [313](#)

incompatible running mode [318](#)

incompatible software [316](#)

install mode [312](#)

usage guidelines [326](#)

using commands [328](#)

## V

VLAN ID, discovering [29](#)

voice-over-IP (VoIP) telephone roaming [143](#)

## W

with debug commands [328](#)

with ping [325](#)

with traceroute [327](#)

