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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS.

CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xv
  Document Conventions xv
  Related Documentation xvii
  Obtaining Documentation and Submitting a Service Request xvii

CHAPTER 1

Using the Command-Line Interface 1
  Information About Using the Command-Line Interface 1
    Command Modes 1
    Using the Help System 3
    Understanding Abbreviated Commands 5
    No and Default Forms of Commands 5
    CLI Error Messages 5
    Configuration Logging 6
  How to Use the CLI to Configure Features 6
    Configuring the Command History 6
      Changing the Command History Buffer Size 6
    Recalling Commands 7
    Disabling the Command History Feature 7
  Enabling and Disabling Editing Features 8
    Editing Commands Through Keystrokes 8
    Editing Command Lines That Wrap 10
  Searching and Filtering Output of show and more Commands 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 13
CHAPTER 3  Administering the System 21

Information About Administering the Controller 21
  System Time and Date Management 21
  System Clock 21
  Network Time Protocol 22
    NTP Stratum 23
    NTP Associations 24
    NTP Security 24
    NTP Implementation 24
    NTP Version 4 24

DNS 25
  Default DNS Settings 25

Login Banners 25
  Default Banner Configuration 25

MAC Address Table 25
  MAC Address Table Creation 26
  MAC Addresses and VLANs 26
  Default MAC Address Table Settings 26

ARP Table Management 27

How to Administer the Controller 27
  Configuring the Time and Date Manually 27
    Setting the System Clock 27
    Configuring the Time Zone 28
    Configuring Summer Time (Daylight Saving Time) 29

Configuring a System Name 30

Setting Up DNS 31

Configuring a Message-of-the-Day Login Banner 32

Configuring a Login Banner 33

Managing the MAC Address Table 34
Configuring DHCP Autoconfiguration (Only Configuration File) 55
Manually Assigning IP Information to Multiple SVIs 57
Modifying the Controller Startup Configuration 59
  Specifying the Filename to Read and Write the System Configuration 59
  Booting the Controller in Installed Mode 60
  Booting the Controller in Bundle Mode 61
  Configuring a Scheduled Software Image Reload 62
Monitoring Controller Setup Configuration 63
  Example: Verifying the Controller Running Configuration 63
  Examples: Displaying Software Bootup in Install Mode 64
  Example: Emergency Installation 65
Configuration Examples for Performing Controller Setup 65
  Example: Configuring a Controller to Download Configurations from a DHCP Server 65
  Examples: Scheduling Software Image Reload 66
Feature History and Information For Performing Controller Setup Configuration 66

CHAPTER 5

Configuring Right-To-Use Licenses 67
  Finding Feature Information 67
  Restrictions for Right-To-Use AP-Count Licenses 67
  Information About Configuring RTU Licenses 68
    Right-To-Use AP-Count Licensing 68
    Right-to-Use AP-Count Evaluation Licenses 68
    Right-To-Use Adder AP-Count Rehosting Licenses 69
  How to Configure RTU Licenses 69
    Activating an AP-Count Evaluation License (CLI) 69
    Activating an AP-Count Permanent License 69
    Obtaining an Upgrade or Capacity Adder License 70
    Transferring Licenses to a Replacement Controller after an RMA 71
  Configuring Right-To-Use Licenses (GUI) 71
  Monitoring and Maintaining RTU Licenses 72
    Viewing Right-To-Use AP-Count Licenses (GUI) 72
    Viewing Right-To-Use AP-Count Licenses (CLI) 73
  Examples: RTU Licenses Configuration 75
  Additional References for RTU Licensing 75
  Feature History and Information for RTU Licensing 76
CHAPTER 8
Configuring Aggressive Load Balancing 105
Finding Feature Information 105
Restrictions for Aggressive Load Balancing 105
Information for Configuring Aggressive Load Balancing Parameters 106
Aggressive Load Balancing 106
How to Configure Aggressive Load Balancing 107
Configuring Aggressive Load Balancing 107
Monitoring Aggressive Load Balancing 108
Examples: Aggressive Load Balancing Configuration 108
Additional References for Aggressive Load Balancing 109
Feature History and Information For Performing Aggressive Load Balancing Configuration 110

CHAPTER 9
Configuring Client Roaming 111
Finding Feature Information 111
Prerequisites for Configuring Client Roaming 111
Restrictions for Configuring Client Roaming 111
Information About Client Roaming 112
Inter-Subnet Roaming 113
Voice-over-IP Telephone Roaming 113
CCX Layer 2 Client Roaming 113
How to Configure Layer 2 or Layer 3 Roaming 114
Configuring Layer 2 or Layer 3 Roaming 114
Configuring CCX Client Roaming Parameters (CLI) 115
Configuring Mobility Oracle 117
Configuring Mobility Controller 118
Configuring Mobility Agent 120
Monitoring Client Roaming Parameters 121
Monitoring Mobility Configurations 121
CHAPTER 10
Configuring Application Visibility and Control 125

Finding Feature Information 125
Information About Application Visibility and Control 125
Supported AVC Class Map and Policy Map Formats 126
Prerequisites for Application Visibility and Control 129
Guidelines for Inter-Controller Roaming with Application Visibility and Control 129
Restrictions for Application Visibility and Control 129
How to Configure Application Visibility and Control 131

Configuring Application Visibility and Control (CLI) 131
Creating a Flow Record 131
Creating a Flow Exporter (Optional) 133
Creating a Flow Monitor 135
Creating AVC QoS Policy 136
Creating a Class Map 137
Creating a Policy Map 138

Configuring Local Policies (CLI) 139
Creating a Service Template (CLI) 140
Creating a Parameter Map (CLI) 140
Creating a Policy Map (CLI) 141
Applying a Local Policy for a Device on a WLAN (CLI) 142

Configuring Local Policies (GUI) 143
Creating a Service Template (GUI) 144
Creating a Policy Map (GUI) 144
Applying Local Policies to WLAN (GUI) 145

Configuring WLAN to Apply Flow Monitor in IPV4 Input/Output Direction 146

Configuring Application Visibility and Control (GUI) 146
Configuring Application Visibility (GUI) 146
Configuring Application Visibility and Control (GUI) 147

Monitoring Application Visibility and Control 149
Monitoring Application Visibility and Control (CLI) 149
Monitoring Application Visibility and Control (GUI) 149
Monitoring SSID and Client Policies Statistics (GUI) 150
# Configuring Voice and Video Parameters

- **Finding Feature Information** 157
- **Prerequisites for Voice and Video Parameters** 157
- **Restrictions for Voice and Video Parameters** 158
- **Information About Configuring Voice and Video Parameters** 158
  - Call Admission Control 158
    - Static-Based CAC 159
    - Load-Based CAC 159
  - IOSd Call Admission Control 160
  - Expedited Bandwidth Requests 160
  - U-APSD 161
  - Traffic Stream Metrics 161
  - Information About Configuring Voice Prioritization Using Preferred Call Numbers 162
  - Information About EDCA Parameters 163
- **How to Configure Voice and Video Parameters** 163
  - Configuring Voice Parameters (CLI) 163
  - Configuring Video Parameters (CLI) 167
  - Configuring SIP-Based CAC (CLI) 169
  - Configuring a Preferred Call Number (CLI) 171
  - Configuring EDCA Parameters (CLI) 172
  - Configuring EDCA Parameters (GUI) 174
- **Monitoring Voice and Video Parameters** 175
- **Configuration Examples for Voice and Video Parameters** 177
  - Example: Configuring Voice and Video 177
- **Additional References for Voice and Video Parameters** 178
- **Feature History and Information For Performing Voice and Video Parameters** 179
CHAPTER 12 Configuring RFID Tag Tracking 181
Finding Feature Information 181
Information About Configuring RFID Tag Tracking 181
How to Configure RFID Tag Tracking 182
  Configuring RFID Tag Tracking (CLI) 182
Monitoring RFID Tag Tracking Information 183
Additional References RFID Tag Tracking 183
Feature History and Information For Performing RFID Tag Tracking Configuration 184

CHAPTER 13 Configuring Location Settings 185
Finding Feature Information 185
Information About Configuring Location Settings 185
How to Configure Location Settings 186
  Configuring Location Settings (CLI) 186
  Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI) 188
  Modifying the NMSP Notification threshold for Clients, RFID Tags, and Rogues (CLI) 189
Monitoring Location Settings and NMSP Settings 190
  Monitoring Location Settings (CLI) 190
  Monitoring NMSP Settings (CLI) 190
Examples: Location Settings Configuration 191
Examples: NMSP Settings Configuration 191
Additional References for Location Settings 192
Feature History and Information For Performing Location Settings Configuration 193

CHAPTER 14 Monitoring Flow Control 195
Finding Feature Information 195
Information About Flow Control 195
Monitoring Flow Control 195
Examples: Monitoring Flow Control 196
Additional References for Monitoring Flow Control 197
Feature History and Information For Monitoring Flow Control 198

CHAPTER 15 Configuring System Message Logs 199
Information About Configuring System Message Logs 199
CHAPTER 16

Configuring Online Diagnostics 213

Information About Configuring Online Diagnostics 213

Online Diagnostics 213

How to Configure Online Diagnostics 214

Starting Online Diagnostic Tests 214

Configuring Online Diagnostics 214

Scheduling Online Diagnostics 215

Configuring Health-Monitoring Diagnostics 216

Monitoring and Maintaining Online Diagnostics 218

Displaying Online Diagnostic Tests and Test Results 218

Configuration Examples for Online Diagnostic Tests 219

Examples: Start Diagnostic Tests 219

Example: Configure a Health Monitoring Test 219

Examples: Schedule Diagnostic Test 219

Examples: Displaying Online Diagnostics 219
CHAPTER 17

Predownloading an Image to Access Points 223

Finding Feature Information 223

Predownloading an Image to an Access Point 223

Restrictions for Predownloading an Image to an Access Point 224

How to Predownload an Image to an Access Point 224

Predownloading an Image to Access Points (CLI) 224

Monitoring Access Point Predownload Process 225

Examples: Access Point Predownload Process 226

Additional References for Predownloading an Image to an Access Point 226

Feature History and Information For Performing Predownloading an Image to an Access Point 227

CHAPTER 18

Troubleshooting the Software Configuration 229

Information About Troubleshooting the Software Configuration 229

Software Failure on a Switch 229

Lost or Forgotten Password on a Controller 230

Power over Ethernet Ports 230

Disabled Port Caused by Power Loss 230

Disabled Port Caused by False Link-Up 231

Ping 231

Layer 2 Traceroute 231

Layer 2 Traceroute Guidelines 231

IP Traceroute 232

Time Domain Reflector Guidelines 233

Debug Commands 234

Crashinfo Files 234

System Reports 235

Onboard Failure Logging on the Switch 235

Fan Failures 236

Possible Symptoms of High CPU Utilization 236

How to Troubleshoot the Software Configuration 237

Recovering from a Software Failure 237
Contents

Recovering from a Lost or Forgotten Password 238
    Procedure with Password Recovery Enabled 240
    Procedure with Password Recovery Disabled 241
Preventing Switch Stack Problems 243
Preventing Autonegotiation Mismatches 243
Troubleshooting SFP Module Security and Identification 244
    Monitoring SFP Module Status 244
Executing Ping 244
Monitoring Temperature 245
Monitoring the Physical Path 245
Executing IP Traceroute 246
Running TDR and Displaying the Results 246
Redirecting Debug and Error Message Output 246
Using the show platform forward Command 247
Configuring OBFL 247
Verifying Troubleshooting of the Software Configuration 248
    Displaying OBFL Information 248
    Example: Verifying the Problem and Cause for High CPU Utilization 249
Scenarios for Troubleshooting the Software Configuration 250
    Scenarios to Troubleshoot Power over Ethernet (PoE) 250
Configuration Examples for Troubleshooting Software 253
    Example: Pinging an IP Host 253
    Example: Performing a Traceroute to an IP Host 253
    Example: Enabling All System Diagnostics 254
Feature History and Information for Troubleshooting Software Configuration 255
Preface

- Document Conventions, page xv
- Related Documentation, page xvii
- Obtaining Documentation and Submitting a Service Request, page xvii

Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D 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.)</td>
</tr>
<tr>
<td>bold font</td>
<td>Commands and keywords and user-entered text appear in bold font.</td>
</tr>
<tr>
<td>Italic font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.</td>
</tr>
<tr>
<td>Courier font</td>
<td>Terminal sessions and information the system displays appear in courier font.</td>
</tr>
<tr>
<td>Bold Courier font</td>
<td>Bold Courier font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td>A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z;}]</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

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 controller, refer to the controller release notes.

- Cisco Validated Designs documents, located at:
  http://www.cisco.com/go/designzone
- Error Message Decoder, located at:
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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:


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

This chapter contains the following topics:

- 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, a 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 controller 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 controller 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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
<th>About This Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Begin a session using Telnet, SSH, or console.</td>
<td>Controller&gt;</td>
<td>Enter <code>logout</code> or <code>quit</code>.</td>
<td>Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>While in user EXEC mode, enter the <code>enable</code> command.</td>
<td>Controller#</td>
<td>Enter <code>disable</code> to exit.</td>
<td>Use this mode to verify commands that you have entered. Use a password to protect access to this mode. Use this mode to execute privilege EXEC commands for access points. These commands are not part of the running config of the controller, they are sent to the IOS config of the access point.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>While in privileged EXEC mode, enter the <code>configure</code> command.</td>
<td>Controller(config)#</td>
<td>To exit to privileged EXEC mode, enter <code>exit</code> or <code>end</code>, or press Ctrl-Z.</td>
<td>Use this mode to configure parameters that apply to the entire controller. Use this mode to configure access point commands that are part of the running config of the controller.</td>
</tr>
<tr>
<td>VLAN configuration</td>
<td>While in global configuration mode, enter the <code>vlan vlan-id</code> command.</td>
<td>Controller(config-vlan)#</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**About This Mode**

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 controller startup configuration file.

**Exit Method**

To exit to global configuration mode, enter the `exit` command.

To return to privileged EXEC mode, press Ctrl-Z or enter `end`.

**Prompt**

Controller(config-if)#

**Access Method**

While in global configuration mode, enter the `interface` command (with a specific interface).

**Mode**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
<th>About This Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface configuration</td>
<td>While in global configuration mode, enter the interface command (with a specific interface).</td>
<td>Controller(config-if)#</td>
<td>To exit to global configuration mode, enter <code>exit</code>. To return to privileged EXEC mode, press Ctrl-Z or enter <code>end</code>.</td>
<td>Use this mode to configure parameters for the Ethernet ports.</td>
</tr>
<tr>
<td>Line configuration</td>
<td>While in global configuration mode, specify a line with the line vty or line console command.</td>
<td>Controller(config-line)#</td>
<td>To exit to global configuration mode, enter <code>exit</code>. To return to privileged EXEC mode, press Ctrl-Z or enter <code>end</code>.</td>
<td>Use this mode to configure parameters for the terminal line.</td>
</tr>
</tbody>
</table>

**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

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

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

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

```
Controller# 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 reenable 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 controller.

`Table 2: Common CLI Error Messages`

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Meaning</th>
<th>How to Get Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Ambiguous command: &quot;show con&quot;</td>
<td>You did not enter enough characters for your controller to recognize the command.</td>
<td>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.</td>
</tr>
<tr>
<td>% Incomplete command.</td>
<td>You did not enter all of the keywords or values required by this command.</td>
<td>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.</td>
</tr>
</tbody>
</table>
| % 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 controller 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.

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 controller 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: terminal history [size number-of-lines]</td>
<td>Changes the number of command lines that the controller records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.</td>
</tr>
</tbody>
</table>

Example:
Controller# terminal history size 200
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Ctrl-P or use the up arrow key</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Ctrl-N or use the down arrow key</td>
<td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.</td>
</tr>
<tr>
<td><strong>Step 3</strong> show history</td>
<td>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 terminal history global configuration command and the history line configuration command.</td>
</tr>
</tbody>
</table>

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
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal no history</td>
<td>Disables the feature during the current terminal session in privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Controller# terminal no history</td>
<td></td>
</tr>
</tbody>
</table>

Step 1

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal editing</td>
<td>Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Controller# terminal editing</td>
<td></td>
</tr>
</tbody>
</table>

Step 2

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal no editing</td>
<td>Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Controller# terminal no editing</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Editing Commands</th>
<th>Description</th>
</tr>
</thead>
</table>

System Management Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)
| **Ctrl-B or use the left arrow key** | Moves the cursor back one character. |
| **Ctrl-F or use the right arrow key** | Moves the cursor forward one character. |
| **Ctrl-A** | Moves the cursor to the beginning of the command line. |
| **Ctrl-E** | Moves the cursor to the end of the command line. |
| **Esc B** | Moves the cursor back one word. |
| **Esc F** | Moves the cursor forward one word. |
| **Ctrl-T** | Transposes the character to the left of the cursor with the character located at the cursor. |
| **Delete or Backspace key** | Erases the character to the left of the cursor. |
| **Ctrl-D** | Deletes the character at the cursor. |
| **Ctrl-K** | Deletes all characters from the cursor to the end of the command line. |
| **Ctrl-U or Ctrl-X** | Deletes all characters from the cursor to the beginning of the command line. |
| **Ctrl-W** | Deletes the word to the left of the cursor. |
| **Esc D** | Deletes from the cursor to the end of the word. |
| **Esc C** | Capitalizes at the cursor. |
| **Esc L** | Changes the word at the cursor to lowercase. |
| **Esc U** | Capitalizes letters from the cursor to the end of the word. |
| **Ctrl-V or Esc Q** | Designates a particular keystroke as an executable command, perhaps as a shortcut. |
| **Return key** | Scrolls down a line or screen on displays that are longer than the terminal screen can display. **Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the More prompt. |
| **Space bar** | Scrolls down one screen. |
Ctrl-L or Ctrl-R | Redisplays the current command line if the controller 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> access-list</td>
<td>Displays the global configuration command entry that extends beyond one line. 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.</td>
</tr>
<tr>
<td>Example: Controller(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 Controller(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Controller(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Controller(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Ctrl-A</td>
<td>Checks the complete syntax. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right.</td>
</tr>
<tr>
<td>Example: Controller(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 Controller(config)# $</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Return key</td>
<td>Execute the commands.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the terminal width privileged EXEC command to set the width of your terminal. Use line wrapping with the command history feature to recall and modify previous complex command entries.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`{show</td>
<td>more} command</td>
</tr>
</tbody>
</table>

**Example:**

```
Controller# show interfaces | include protocol
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
```

**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 controller console or connect a PC to the Ethernet management port and then power on the controller, as described in the hardware installation guide that shipped with your controller.

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

You can use one of these methods to establish a connection with the controller:
• Connect the controller 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 controller hardware installation guide.

• Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The controller must have network connectivity with the Telnet or SSH client, and the controller must have an enable secret password configured.
  - The controller supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
  - The controller 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 13
- Connecting the Console Port of the Controller, page 15
- Logging On to the Web GUI, page 15
- Enabling Web and Secure Web Modes, page 15
- Configuring the Controller Web GUI, page 16

Prerequisites for Using the Web GUI

- The GUI must be used on a PC running Windows 7, Windows XP SP1 (or later releases), or Windows 2000 SP4 (or later releases).
- The controller GUI is compatible with Microsoft Internet Explorer version 10.x, Mozilla Firefox 20.x, or Google Chrome 26.x.

Information About Using The Web GUI

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

Web GUI Features

The controller 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 controller, 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 controller 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 controller, WLAN, and radios.
- Enables you to configure and set security policies on your controller.
- Enables you to access the controller operating system software management commands.

The Administration tab enables you to configure system logs.
Connecting the Console Port of the Controller

**Before You Begin**

Before you can configure the controller 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 controller's RJ-45 console port and the other end to your PC's serial port.

**Step 2**  
Plug the AC power cord into the controller 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 controller 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 controller is configured with the IP address for service port.

---

Logging On to the Web GUI

**Step 1**  
Enter the controller 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.

**Step 2**  
When prompted, enter a valid username and password and click OK.

*Note*  
The administrative username and password that you created in the configuration wizard are case sensitive. The default username is admin, and the default password is cisco.

The Accessing page appears.

---

Enabling Web and Secure Web Modes

**Step 1**  
Choose Configuration > Controller > Management > Protocol Management > HTTP-HTTPS.

The HTTP-HTTPS Configuration page appears.

**Step 2**  
To enable web mode, which allows users to access the controller 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.
Configuring the Controller Web GUI

The configuration wizard enables you to configure basic settings on the controller. You can run the wizard after you receive the controller from the factory or after the controller 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 controller. The controller 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 Controller <Model Number> <Hostname>** page appears.

Step 3 On the **Accessing Cisco Controller** page, click the **Wireless Web GUI** link to access controller web GUI **Home** page.

Step 4 Choose **Configuration > Wizard** to perform all steps that you need to configure the controller initially. The **Admin Users** page appears.

Step 5 On the **Admin Users** page, enter the administrative username to be assigned to this controller in the User Name text box and the administrative password to be assigned to this controller 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 controller. 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 controller, and click **Next**:

- Customer-definable controller 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**.

- Displays Mobility Controller in the Mobility Role text box.
• Displays mobility protocol port number in the Mobility Protocol Port text box.
• Displays the mobility group name in the Mobility 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.
• Displays the number of members configured on the controller in the Mobility Domain Member Count text box.
• To enable the controller as a Mobility Oracle, select the Mobility Oracle Enabled check box.
  Note Only the controller can be configured as Mobility Oracle. You cannot configure the switch as Mobility Oracle.
  The Mobility Oracle is optional, it maintains the client database under one complete mobility domain.
• The amount of time (in seconds) between each ping request sent to an peer controller 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 controller 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 controller in the Mobility Control Message DSCP Value (0-63) text box.
  The valid range is 0 to 63, and the default value is 0.

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 controller based on the following parameters, and click Next.
• Displays current timestamp on the controller 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 controller, synchronizes its time based on the NTP server settings available.
• Choose date on the controller 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 offset setting required when compared to the current time configured on the controller 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 controller using these steps, and if you wish to change any configuration value, click **Previous** and navigate to that page. You can save the controller 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 controller.
Configuring the Controller Web GUI
Administering the System

- Information About Administering the Controller, page 21
- How to Administer the Controller, page 27
- Monitoring and Maintaining Administration of the Controller, page 42
- Configuration Examples for Controller Administration, page 43
- Feature History and Information for Controller Administration, page 45

Information About Administering the Controller

System Time and Date Management

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

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 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 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.

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 controller. 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.
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 controller, 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 4: Default DNS Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS enable state</td>
<td>Enabled.</td>
</tr>
<tr>
<td>DNS default domain name</td>
<td>None configured.</td>
</tr>
<tr>
<td>DNS servers</td>
<td>No name server addresses are configured.</td>
</tr>
</tbody>
</table>

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.

The MOTD and login banners are not configured.

Default Banner Configuration

The MOTD and login banners are not configured.

MAC Address Table

The MAC address table contains address information that the controller 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 controller 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 controller 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).

MAC Address Table Creation

With multiple MAC addresses supported on all ports, you can connect any port on the controller to other network devices. The controller 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 controller 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 controller maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The controller sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the controller 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 controller 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.

Default MAC Address Table Settings

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

Table 5: Default Settings for the MAC Address

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aging time</td>
<td>300 seconds</td>
</tr>
<tr>
<td>Dynamic addresses</td>
<td>Automatically learned</td>
</tr>
<tr>
<td>Static addresses</td>
<td>None configured</td>
</tr>
</tbody>
</table>
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.

How to Administer the Controller

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

**Note**

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

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.

**SUMMARY STEPS**

1. Use one of the following:
   * `clock set hh:mm:ss day month year`
   * `clock set hh:mm:ss month day year`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Use one of the following:</td>
<td>Sets the system clock using one of these formats:</td>
</tr>
<tr>
<td>• clock set  hh:mm:ss day month year</td>
<td>• <em>hh:mm:ss</em>—Specifies the time in hours (24-hour format), minutes,</td>
</tr>
<tr>
<td>• clock set  hh:mm:ss month day year</td>
<td>and seconds. The time specified is relative to the configured time</td>
</tr>
<tr>
<td>Example:</td>
<td>zone.</td>
</tr>
<tr>
<td>Controller# clock set 13:32:00 23 March 2013</td>
<td>• <em>day</em>—Specifies the day by date in the month.</td>
</tr>
<tr>
<td></td>
<td>• <em>month</em>—Specifies the month by name.</td>
</tr>
<tr>
<td></td>
<td>• <em>year</em>—Specifies the year (no abbreviation).</td>
</tr>
</tbody>
</table>

Configuring the Time Zone

SUMMARY STEPS

1. configure terminal  
2. clock timezone zone hours-offset [minutes-offset]  
3. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>clock timezone zone hours-offset [minutes-offset]</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# clock timezone AST -3 30</td>
<td></td>
</tr>
</tbody>
</table>

• *zone*—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC.  
• *hours-offset*—Enters the hours offset from UTC.  
• (Optional) *minutes-offset*—Enters the minutes offset from UTC. This available where the local time zone is a percentage of an hour different from UTC.
### 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. `configure terminal`
2. `clock summer-time zone date month year hh:mm date month year hh:mm [offset]`
3. `clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><code>clock summer-time zone date month year hh:mm date month year hh:mm [offset]</code></td>
<td>Configures summer time to start and end on specified days every year.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Controller(config)# clock summer-time</td>
<td></td>
</tr>
<tr>
<td>PDT date</td>
<td></td>
</tr>
<tr>
<td>10 March 2013 2:00 3 November 2013 2:00</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><code>clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]</code></td>
<td>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. The end time is relative to summer time. Summer time is disabled by default. If you specify <code>clock summer-time zone recurring</code> without parameters, the summer time rules default to the United States rules.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Controller(config)# clock summer-time</td>
<td></td>
</tr>
<tr>
<td>PDT recurring 10 March 2013 2:00 3</td>
<td></td>
</tr>
</tbody>
</table>
If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

- **zone**—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect.
- (Optional) **week**—Specifies the week of the month (1 to 4, first, or last).
- (Optional) **day**—Specifies the day of the week (Sunday, Monday...).
- (Optional) **month**—Specifies the month (January, February...).
- (Optional) **hh:mm**—Specifies the time (24-hour format) in hours and minutes.
- (Optional) **offset**—Specifies the number of minutes to add during summer time. The default is 60.

### Configuring a System Name

**SUMMARY STEPS**

1. configure terminal
2. hostname name
3. end

**DETAILED STEPS**

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

**Example:**

Controller# configure terminal
### Purpose

**Command or Action**

**Purpose**

**Step 2**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hostname name</code></td>
<td>Configures a system name. When you set the system name, it is also used as the system prompt. The default setting is Controller. 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.</td>
</tr>
</tbody>
</table>

**Example:**

```
Controller(config)# hostname remote-users
```

**Step 3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Controller(config)# end
```

### Setting Up DNS

If you use the controller 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.

### SUMMARY STEPS

1. `configure terminal`
2. `ip domain-name name`
3. `ip name-server server-address1 [server-address2 ... server-address6]`
4. `ip domain-lookup [nsap | source-interface interface]`
5. `end`

### DETAILED STEPS

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

**Example:**

```
Controller# configure terminal
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>ip domain-name <em>name</em></td>
<td>Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the controller 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).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# ip domain-name Cisco.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>ip name-server <em>server-address1</em> [server-address2 ... server-address6]</td>
<td>Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The controller sends DNS queries to the primary server first. If that query fails, the backup servers are queried.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>ip domain-lookup [nsap</td>
<td>source-interface <em>interface</em>]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# ip domain-lookup</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**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 controller

**SUMMARY STEPS**

1. configure terminal
2. banner motd *c message c*
3. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>banner motd c message c</strong></td>
<td>Specifies the message of the day. Example: Controller(config)# banner motd # This is a secure site. Only authorized users are allowed. For access, contact technical support. #</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>end</strong></td>
<td>Returns to privileged EXEC mode. <strong>Example:</strong> Controller(config)# end</td>
</tr>
</tbody>
</table>

### 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.

### SUMMARY STEPS

1. configure terminal
2. banner login c message c
3. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Managing the MAC Address Table

#### Changing the Address Aging Time

**SUMMARY STEPS**

1. `configure terminal`
2. `mac address-table aging-time [0 | 10-1000000] [routed-mac | vlan vlan-id]`
3. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Controller# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table.</td>
</tr>
<tr>
<td>`mac address-table aging-time [0</td>
<td>10-1000000] [routed-mac</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Controller(config)# mac address-table aging-time 500 vlan 2</code></td>
<td></td>
</tr>
</tbody>
</table>

---

### Purpose

**Command or Action**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><code>banner login c message c</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Controller(config)# banner login $ Access for authorized users only. Please enter your username and password. $</code></td>
</tr>
</tbody>
</table>

**Purpose**

Specifies the login message.

- `c`—Enters the delimiting character of your choice, for example, a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.

- `message`—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.

**Step 3**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Controller(config)# end</code></td>
</tr>
</tbody>
</table>

---

**Managing the MAC Address Table**

---

**Administering the System**

---

**System Management Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)**

---
Purpose
Command or Action

Step 3
end

Example:
Controller(config)# end

Returns to privileged EXEC mode.

Configuring MAC Address Change Notification Traps

SUMMARY STEPS

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

DETAILED STEPS

Step 1
configure terminal

Example:
Controller# configure terminal

Enters global configuration mode.

Step 2
snmp-server host host-addr community-string notification-type { informs | traps } { version { 1 | 2c | 3 } } { vrf vrf instance name }

Example:
Controller(config)# snmp-server host 172.20.10.10 traps private mac-notification

Specifies the recipient of the trap message.

- host-addr—Specifies the name or address of the NMS.
- traps (the default)—Sends SNMP traps to the host.
- informs—Sends SNMP informs to the host.
- version—Specifies the SNMP version to support. Version 1, the default, is not available with informs.
- community-string—Specifies the string to send with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define
Enables the controller to send MAC address change notification traps to the NMS.

Example:
Controller(config)# snmp-server enable traps mac-notification change

Step 4
mac address-table notification change

Enables the MAC address change notification feature.

Example:
Controller(config)# mac address-table notification change

Step 5
mac address-table notification change [interval value] [history-size value]

Enters the trap interval time and the history table size.

Example:
Controller(config)# mac address-table notification change interval 123
Controller(config)# mac address-table notification change history-size 100

Step 6
interface interface-id

Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap.

Example:
Controller(config)# interface gigabitethernet1/0/2

Step 7
snmp trap mac-notification change [added | removed]

Enables the MAC address change notification trap on the interface.

Example:
Controller(config-if)# snmp trap mac-notification change added

System Management Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)
<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Example:

```
Controller(config-if)# end
```
### 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.

#### SUMMARY STEPS

1. `configure terminal`
2. `snmp-server host host-addr {traps | informs} {version 1 | 2c | 3} community-string notification-type`
3. `snmp-server enable traps mac-notification threshold`
4. `mac address-table notification threshold`
5. `mac address-table notification threshold [limit percentage] [interval time]`
6. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`snmp-server host host-addr {traps</td>
<td>informs} {version {1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# <code>snmp-server host 172.20.10.10 traps private mac-notification</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>snmp-server enable traps mac-notification threshold</code></td>
<td>Enables MAC threshold notification traps to the NMS.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# <code>snmp-server enable traps mac-notification threshold</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>mac address-table notification threshold</code></td>
<td>Enables the MAC address threshold notification feature.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# <code>mac address-table notification threshold</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>mac address-table notification threshold [limit percentage] [interval time]</code></td>
<td>Enters the threshold value for the MAC address threshold usage monitoring.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# <code>mac address-table notification threshold interval 123</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) <code>limit percentage</code>—Specifies the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) <code>interval time</code>—Specifies the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.</td>
</tr>
</tbody>
</table>
Example:
Controller(config)# end

What to Do Next

Adding and Removing Static Address Entries

SUMMARY STEPS

1. configure terminal
2. mac address-table static mac-addr vlan vlan-id interface interface-id
3. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 mac address-table static mac-addr vlan vlan-id interface interface-id</td>
<td>Adds a static address to the MAC address table.</td>
</tr>
<tr>
<td>Example: Controller(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
</tbody>
</table>

- **mac-addr**—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.
- **vlan-id**—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.
- **interface-id**—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.
## Configuring Unicast MAC Address Filtering

### SUMMARY STEPS

1. `configure terminal`
2. `mac address-table static mac-addr vlan vlan-id drop`
3. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# <code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
| Step 2 | `mac address-table static mac-addr vlan vlan-id drop` | Enables unicast MAC address filtering and configure the controller to drop a packet with the specified source or destination unicast static address.  
  - `mac-addr`—specifies a source or destination unicast MAC address (48-bit). Packets with this MAC address are dropped.  
  - `vlan-id`—specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. |
| Example: | Controller(config)# `mac address-table static c2f3.220a.12f4 vlan 4 drop` | |
| Step 3 | `end` | Returns to privileged EXEC mode. |
| Example: | Controller(config)# `end` | |
## Monitoring and Maintaining Administration of the Controller

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

Example: Setting the System Clock

This example shows how to manually set the system clock:

```
Controller# 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:

```
Controller(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:

```
Controller(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:

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

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

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

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

```
Controller(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:

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

Feature History and Information for Controller Administration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Information About Performing Controller Setup Configuration

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

Controller Boot Process

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

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 controller 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 controller 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.
- In a stack of switches, Cisco recommends all switches in install mode.
- Software rollback to a previously installed package set.
- Emergency installation in the event that no valid installed packages reside on the boot flash.

**Note**  
Software installation and rollback must be performed while running only in installed mode. You can use the `software expand` EXEC command to convert bundle boot mode to install mode.

**Software Boot Modes**

Your controller supports two modes to boot the software packages:

- Installed mode
- Bundle mode

**Related Topics**

Examples: Displaying Software Bootup in Install Mode, on page 64  
Example: Emergency Installation, on page 65
Installed Boot Mode

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

`controller: 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 64
- Example: Emergency Installation, on page 65

Bundle Boot Mode

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

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.

---

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

**Related Topics**

- Examples: Displaying Software Bootup in Install Mode, on page 64
- Example: Emergency Installation, on page 65

Controllers Information Assignment

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

The switch stack is managed through a single IP address. The IP address is a system-level setting and is not specific to the stack master or to any other stack member. You can still manage the stack through the same
IP address even if you remove the stack master or any other stack member from the stack, provided there is IP connectivity.

**Note**

Stack members retain their IP address when you remove them from a switch stack. To avoid a conflict by having two devices with the same IP address in your network, change the IP address of the switch that you removed from the switch stack.

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 controller receives the dynamically assigned IP address and reads the configuration file.

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

### 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 controller can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your controller (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 controller. 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.

The DHCP server for your controller can be on the same LAN or on a different LAN than the controller. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your controller 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 controller.

### DHCP Client Request Process

When you boot up your controller, the DHCP client is invoked and requests configuration information from a DHCP server when the configuration file is not present on the controller. 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 2: DHCP Client and Server Message Exchange*

The client, Controller 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 DHCP-OFFER 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 controller receives depends on how you configure the DHCP server.

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

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

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

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

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 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 controller by the controller hardware address.

- If you want the controller 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 controller) (required)

• If you want the controller 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 controller 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 controller is not configured. If the router IP address or the TFTP server name are not found, the controller might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.

• The controller can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your controller but are not configured. (These features are not operational.)

**Purpose of the TFTP Server**

Based on the DHCP server configuration, the controller attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the controller 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 controller 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 controller 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 controller’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 controller 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 controller configuration file).

• The network-config or the cisconet.cfg file (known as the default configuration files).

• The router-config or the ciscortr.cfg file (These files contain commands common to all controllers. 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 controller, or if it is to be accessed by the controller 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 controller.

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

- The IP address and the configuration filename is reserved for the controller and provided in the DHCP reply (one-file read method).
  
The controller receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. The controller 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 controller, but the TFTP server address is not provided in the DHCP reply (one-file read method).
  
The controller receives its IP address, subnet mask, and the configuration filename from the DHCP server. The controller 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 controller and provided in the DHCP reply. The configuration filename is not provided (two-file read method).
  
The controller receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The controller sends a unicast message to the TFTP server to retrieve the network-config or ciscoconf file default configuration file. (If the network-config file cannot be read, the controller reads the ciscoconf file.)

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

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

  If the controller cannot read the network-config, ciscoconf, or the hostname file, it reads the router-config file. If the controller cannot read the router-config file, it reads the ciscortr.cfg file.
The controller 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 controller, you enter the boot loader mode only through the console connection configured for 9600 bps. Unplug the controller 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 controller prompt then appears.

The controller 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.

Scheduled Reload of the Software Image

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

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

If you modify your configuration file, the controller 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 Controller Setup Configuration

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

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller# <code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring DHCP Autoconfiguration (Only Configuration File)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ip dhcp pool poolname</code></td>
<td>Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>ip dhcp pool pool</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>boot filename</code></td>
<td>Specifies the name of the configuration file that is used as a boot image.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(dhcp-config)# <code>boot config-boot.text</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>network network-number mask prefix-length</code></td>
<td>Specifies the subnet network number and mask of the DHCP address pool. <strong>Note</strong> 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 (/).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(dhcp-config)# <code>network 10.10.0 255.255.255.0</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>default-router address</code></td>
<td>Specifies the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(dhcp-config)# <code>default-router 10.10.10.1</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>option 150 address</code></td>
<td>Specifies the IP address of the TFTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(dhcp-config)# <code>option 150 10.10.10.1</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(dhcp-config)# <code>exit</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>tftp-server flash:filename.text</code></td>
<td>Specifies the configuration file on the TFTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>tftp-server flash:config-boot.text</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>interface interface-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config)# interface gigabitethernet1/0/4</td>
<td></td>
</tr>
<tr>
<td>Specifies the address of the client that will receive the configuration file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>no switchport</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config-if)# no switchport</td>
<td></td>
</tr>
<tr>
<td>Puts the interface into Layer 3 mode.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>ip address address mask</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config-if)# ip address 10.10.10.1 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Specifies the IP address and mask for the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config-if)# end</td>
<td></td>
</tr>
<tr>
<td>Returns to privileged EXEC mode.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface vlan vlan-id</td>
<td>Enters interface configuration mode, and enters the VLAN to which the IP information is assigned. The range is 1 to 4094.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# interface vlan 99</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip address ip-address subnet-mask</td>
<td>Enters the IP address and subnet mask.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config-vlan)# ip address 10.10.10.2 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip default-gateway ip-address</td>
<td>Enters the IP address of the next-hop router interface that is directly connected to the controller where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the controller. Once the default gateway is configured, the controller has connectivity to the remote networks with which a host needs to communicate.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# ip default-gateway 10.10.10.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Step 7
**Command or Action:** `show interfaces vlan vlan-id`
Verifies the configured IP address.

**Example:**
```
Controller# show interfaces vlan 99
```

### Step 8
**Command or Action:** `show ip redirects`
Verifies the configured default gateway.

**Example:**
```
Controller# show ip redirects
```

---

# Modifying the Controller 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 controller 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

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

**Example:**
```
Controller# configure terminal
```
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 2 | `boot flash:file-url` | Specifies the configuration file to load during the next boot cycle.  
*Example:*  
Controller(config)# `boot flash:config.text`  
*file-url*—The path (directory) and the configuration filename.  
Filenames and directory names are case-sensitive. |
| Step 3 | `end` | Returns to privileged EXEC mode.  
*Example:*  
Controller(config)# `end` |
| Step 4 | `show boot` | Verifies your entries.  
The `boot` global configuration command changes the setting of the `CONFIG_FILE` environment variable.  
*Example:*  
Controller# `show boot` |
| Step 5 | `copy running-config startup-config` | (Optional) Saves your entries in the configuration file.  
*Example:*  
Controller# `copy running-config startup-config` |

---

### Booting the Controller in Installed Mode

**SUMMARY STEPS**

1. `cp source_file_path destination_file_path`  
2. `software expand file source_file_path`  
3. `reload`  
4. `boot flash:packages.conf`  
5. `show version`  

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `cp source_file_path destination_file_path` | (Optional) Copies the bin file (image.bin) from the FTP or TFTP server to flash or USB flash.  
*Example:*  
Controller# |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>software expand file source_file_path</td>
<td>Expands the bin file stored in flash, FTP, TFTP, HTTP, or HTTPS server on the booted controller. <strong>Note</strong> Ensure that the packages.conf file is available in the expanded list.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>reload</td>
<td>Reloads the controller. <strong>Note</strong> You can boot the controller manually or automatically using the packages.conf file. If you are booting manually, you can proceed to Step 4. Otherwise, the controller boots up automatically.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>boot flash:packages.conf</td>
<td>Boots the controller with the packages.conf file.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>show version</td>
<td>Verifies that the controller is in the INSTALL mode.</td>
</tr>
</tbody>
</table>

**Booting the Controller in Bundle Mode**

There are several methods by which you can boot the controller—either by copying the bin file from the TFTP server and then boot the controller, or by booting the controller 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 controller from the TFTP server in the bundle mode.

**SUMMARY STEPS**

1. cp source_file_path destination_file_path
2. boot
4. show version

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>cp source_file_path destination_file_path</td>
<td>(Optional) Copies the bin file (image.bin) from the FTP or TFTP server to flash or USB flash.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>software expand file source_file_path</td>
<td>Expands the bin file stored in flash, FTP, TFTP, HTTP, or HTTPS server on the booted controller. <strong>Note</strong> Ensure that the packages.conf file is available in the expanded list.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>reload</td>
<td>Reloads the controller. <strong>Note</strong> You can boot the controller manually or automatically using the packages.conf file. If you are booting manually, you can proceed to Step 4. Otherwise, the controller boots up automatically.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>boot flash:packages.conf</td>
<td>Boots the controller with the packages.conf file.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>show version</td>
<td>Verifies that the controller is in the INSTALL mode.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller:</td>
<td>Sets the boot parameters.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>boot</td>
<td>Boots the controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch: boot</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>show version</td>
<td>Verifies that the controller is in the BUNDLE mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

---

**Configuring a Scheduled Software Image Reload**

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

**SUMMARY STEPS**

1. configure terminal
2. copy running-config startup-config
3. reload in 
4. reload at
5. reload cancel
6. show reload

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Saves your controller configuration information to the startup configuration before you use the <strong>reload</strong> command.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>reload in [hh:]mm [text]</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# reload in 12</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>System configuration has been modified. Save? [yes/no]: y</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**reload at hh: mm [month day</td>
</tr>
<tr>
<td>Example: Controller(config)# reload at 14:00</td>
<td>Specifies the time in hours and minutes for the reload to occur. <strong>Note</strong> Use the <strong>at</strong> keyword only if the controller system clock has been set (through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured timezone on the controller. To schedule reloads across several controllers to occur simultaneously, the time on each controller must be synchronized with NTP.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>reload cancel</strong></td>
</tr>
<tr>
<td>Example: Controller(config)# reload cancel</td>
<td>Cancels a previously scheduled reload.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show reload</strong></td>
</tr>
<tr>
<td>Example: show reload</td>
<td>Displays information about a previously scheduled reload or identifies if a reload has been scheduled on the controller.</td>
</tr>
</tbody>
</table>

**Monitoring Controller Setup Configuration**

**Example: Verifying the Controller Running Configuration**

```
Controller# 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 $1$e$9.$5DUvAUnZOAmvmgqBEzIXE0
!
<output truncated>
interface gigabitethernet6/0/2
mvr type source
<output truncated>
...
interface VLAN1
```
Examples: Displaying Software Bootup in Install Mode

This example displays software bootup in install mode:

```
switch: boot flash:packages.conf
```

Getting rest of image
Reading full image into memory... done
Reading full base package into memory... done = 74596432
Nova Bundle Image

Kernel Address : 0x6042f354
Kernel Size : 0x318412/3245074
Initramfs Address : 0x60747768
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000, 0x90000000].

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 09:57:05 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2 is starting stack discovery
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has finished stack discovery
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2 has been added to the stack
Nov 7 09:59:14 %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
Example: Emergency Installation

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

```
Example: Configuring a Controller 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:

```
Example: Configuring a Controller 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:

```
```
Examples: Scheduling Software Image Reload

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

Controller# 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 controller at a future time:

Controller# 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]

Feature History and Information For Performing Controller Setup Configuration

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Right-To-Use Licenses

• Finding Feature Information, page 67
• Restrictions for Right-To-Use AP-Count Licenses, page 67
• Information About Configuring RTU Licenses, page 68
• How to Configure RTU Licenses, page 69
• Monitoring and Maintaining RTU Licenses, page 72
• Examples: RTU Licenses Configuration, page 75
• Additional References for RTU Licensing, page 75
• Feature History and Information for RTU Licensing, page 76

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 Right-To-Use AP-Count Licenses

The following are the restrictions you must keep in mind when using license for the Cisco 5700 Series Wireless Controller:

• The license you have purchased is applicable only for the Cisco 5700 Series Wireless Controller. You cannot use the same license for the earlier version of the Cisco 5700 Series Wireless Controllers.

• The CLI commands that you run for the Cisco 5700 Series Wireless Controller are applicable only for these controllers. You cannot run these commands for the earlier version of the controllers.
Information About Configuring RTU Licenses

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 controller.

You can order your controller with support for a specific number of adder access point count licenses, but the total number of licenses ordered should not exceed 1000. You can also order your adder access point count licenses after receiving the controller.

For example, if you have ordered 700 new adder licenses, you can add only those ordered adder licenses to the controller. The licenses can be added in increments of 1, but the total number of licenses added for the controller should not exceed 1000.

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

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 controller capacity at a later time. You can transfer the adder access point count license from one controller 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 1000.
   - The evaluation period for using the access point licenses is 90 days.
   - You can activate and deactivate the evaluation licenses from the CLI.

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 50-access-point count and want to try an evaluation license with a 100-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 1000 access points are available for 90 days.

To prevent disruptions in operation, the controller 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 controller reboots after the evaluation license expiry, the license defaults to a permanent license.
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. For example, if you want to move your Office Extend or indoor access points to a different controller, you could transfer the adder ap-count license from one controller to another.

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 AP-Count Evaluation License (CLI)

When an evaluation license is activated, the maximum supported ap-count licenses are made available. A maximum of 1000 access points can be evaluated for 90 days by enabling the evaluation ap-count licenses.

SUMMARY STEPS

1. license right-to-use activate ap-count evaluation
2. show license right-to-use summary

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> license right-to-use activate ap-count evaluation</td>
<td>Enables the ap-count evaluation licenses on the controller. By default during activation, the EULA gets displayed. If the <code>acceptEULA</code> is passed, the EULA content is not displayed, and you can activate the evaluation license. This option is useful for automation and scripting.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# license right-to-use activate ap-count evaluation</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show license right-to-use summary</td>
<td>Verifies that the evaluation license is activated on the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use summary</td>
<td></td>
</tr>
</tbody>
</table>

Activating an AP-Count Permanent License

You can deactivate an evaluation ap-count license and activate the permanent ap-count license on the controller.
After activating ap-count permanent or adder license, if the `show license right-to-use summary` command still shows evaluation ap-count licenses, then you must deactivate the previously used evaluation license that was not deactivated earlier. Deactivate the evaluation license to enable permanent or adder ap-count licenses.

**SUMMARY STEPS**

1. `license right-to-use deactivate ap-count evaluation`
2. `show license right-to-use summary`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>license right-to-use deactivate ap-count evaluation</code></td>
<td>Deactivates particular evaluation license level and activates the permanent ap-count licenses on the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller# `license right-to-use deactivate</td>
<td></td>
</tr>
<tr>
<td>ap-count evaluation</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>show license right-to-use summary</code></td>
<td>Verifies the number of permanent ap-count licenses activated on the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller# <code>show license right-to-use summary</code></td>
<td></td>
</tr>
</tbody>
</table>

### Obtaining an Upgrade or Capacity Adder License

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

**SUMMARY STEPS**

1. `license right-to-use activate ap-count ap-number slot 1`
2. `show license right-to-use summary`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>license right-to-use activate ap-count ap-number slot 1</code></td>
<td>Obtains an upgrade or increases the license capacity by adding new adder licenses.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller# `license right-to-use activate ap-count</td>
<td></td>
</tr>
<tr>
<td>500 slot 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>show license right-to-use summary</code></td>
<td>Verifies the number of permanent ap-count licenses activated on the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller# <code>show license right-to-use summary</code></td>
<td></td>
</tr>
</tbody>
</table>
Transferring Licenses to a Replacement Controller after an RMA

The replacement controller comes with same permanent ap-count licences.

SUMMARY STEPS

1. license right-to-use deactivate ap-count \textit{count slot} / acceptEULA
2. license right-to-use activate ap-count \textit{count slot} / acceptEULA
3. show license right-to-use summary

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>license right-to-use deactivate ap-count \textit{count slot} / acceptEULA</td>
<td>Deactivates the permanent ap-count licenses on earlier controller to be replaced.</td>
</tr>
<tr>
<td>Example: Controller# license right-to-use deactivate ap-count 55 slot 1 acceptEULA</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>license right-to-use activate ap-count \textit{count slot} / acceptEULA</td>
<td>Activates the same permanent ap-count licenses on the replacement controller.</td>
</tr>
<tr>
<td>Example: Controller# license right-to-use activate ap-count 55 slot 1 acceptEULA</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>show license right-to-use summary</td>
<td>Verifies the number of ap-count licenses points activated on the replacement controller.</td>
</tr>
<tr>
<td>Example: Controller# show license right-to-use summary</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Right-To-Use Licenses (GUI)

Step 1 Choose Administration > Software Activation > Licenses to open the Licenses page.
Step 2 In the License Activation area, choose Activate or Deactivate from the License drop box and enter the number of adder licenses you want to activate or deactivate in the License Adder of AP-Count (1 to 1000) text box.
Step 3 Click Apply and Save Configuration.
Monitoring and Maintaining RTU Licenses

Viewing Right-To-Use AP-Count Licenses (GUI)

You can view the details of access point licenses installed on the controller using the Licenses and License Usage pages from the controller GUI.

---

**Step 1** Choose Administration > Software Activation > Licenses.

**Example:**
The Licenses page appears.

This page lists all of the access point licenses installed on the controller. You can view the following details for the license:

- License name
- License type (adder, permanent, or evaluation)
- Count (the maximum number of access points allowed for this license)
- Period left for the license

In addition, you can view the following details of the AP-Count licenses:

- Whether the ap-count license is enabled or not
- The maximum number of access points allowed for this license
- The number of access points currently using this license
- The remaining ap-count licenses

---

**Step 2** Choose Administration > Software Activation > License Usage.

**Example:**
The License Usage page appears.

In the License Usage page, you can view the consolidated list of all of the licenses based on their usage duration, use of the license, and the end-user license agreement (EULA) acceptance state.

---

**Step 3** Choose Administration > Software Activation > Eula > Adder, Evaluation, or Permanent.

**Example:**
The Eula page for the selected license appears.

You can read the terms and the conditions for the Adder, Evaluation, or Permanent license.
Viewing Right-To-Use AP-Count Licenses (CLI)

You can view the detailed information of ap-count licenses installed on the controller using the `show license right-to-use` commands from the controller CLI.

**SUMMARY STEPS**

1. `show license right-to-use detail`
2. `show license right-to-use detail | output modifiers`
3. `show license right-to-use eula`
4. `show license right-to-use`
5. `show license right-to-use usage`
6. `show license right-to-use | output modifiers`
7. `show license right-to-use summary`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>show license right-to-use detail</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller# <code>show license right-to-use detail</code></td>
</tr>
</tbody>
</table>

| **Step 2** | `show license right-to-use detail | output modifiers` | Displays the details of licenses based on the filtered search using output modifiers such as append, begin, count, exclude, format, include, redirect, section, and tee. |
| **Example:** | Controller# `show license right-to-use detail | output modifiers` | Appends the redirected license information output to URL. The URLs supporting append operation are crash information, flash, FTP, HTTP, HTTPS, NVRAM, RCP, SCP, TFTP, UNIX, and USB flash0. Displays the license information that begins with the lines which match the regular expression. Displays the number of lines that match the regular expression. Displays the details of license information that excludes lines which match the regular expression. Displays the details of license information based on the format specified in the spec file. Displays the lines that match the regular expression. Redirects the license information output to URL. The URLs that support the redirect operation are crash information, flash, FTP, HTTP, HTTPS, NVRAM, RCP, SCP, TFTP, UNIX, and USB flash0. Filters the section of the license information output based on the include, exclude, or other regular expression options specified. |
| **Example:** | Controller# `show license right-to-use detail | output modifiers` | |
| **Example:** | Controller# `show license right-to-use detail | output modifiers` | Append <url> |
| **Example:** | Controller# `show license right-to-use detail | output modifiers` | begin apcount |
| **Example:** | Controller# `show license right-to-use detail | exclude apcount` | |
| **Example:** | Controller# `show license right-to-use detail | format <spec file location>` | |
| **Example:** | Controller# `show license right-to-use detail | output modifiers` | include apcount |
### Configuring Right-To-Use Licenses

#### Viewing Right-To-Use AP-Count Licenses (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use detail</td>
<td>Copies the license information output to URL. The URLs that support the copy operation are crash information, flash, FTP, HTTP, HTTPS, NVRAM, RCP, SCP, TFTP, UNIX, and USB flash0.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use detail</td>
<td>Copies the license information output to URL. The URLs that support the copy operation are crash information, flash, FTP, HTTP, HTTPS, NVRAM, RCP, SCP, TFTP, UNIX, and USB flash0.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use detail</td>
<td>Copies the license information output to URL. The URLs that support the copy operation are crash information, flash, FTP, HTTP, HTTPS, NVRAM, RCP, SCP, TFTP, UNIX, and USB flash0.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use eula adder</td>
<td>Displays the EULA content for the adder, evaluation, and permanent AP-count licenses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use eula evaluation</td>
<td>Displays the EULA content for the adder, evaluation, and permanent AP-count licenses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use eula permanent</td>
<td>Displays the EULA content for the adder, evaluation, and permanent AP-count licenses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use</td>
<td>Displays the licenses that got activated with EULA.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use usage</td>
<td>Displays the usage details of all licenses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use</td>
<td>Displays the usage details of all licenses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use</td>
<td>Displays the usage details of all licenses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use summary</td>
<td>Displays the summary of licenses that are currently in use.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Controller# show license right-to-use summary</td>
<td>Displays the summary of licenses that are currently in use.</td>
</tr>
</tbody>
</table>
Examples: RTU Licenses Configuration

This example shows how to activate an ap-count evaluation license:

Controller# license right-to-use activate ap-count evaluation
Controller# show license right-to-use summary

This example shows how to activate an ap-count permanent license:

Controller# license right-to-use deactivate ap-count evaluation
Controller# show license right-to-use summary

This example shows how to obtain an upgrade or adder license:

Controller# license right-to-use activate ap-count 700 slot 1
Controller# show license right-to-use summary

This example shows how to transfer licenses to a replacement controller after an RMA. Deactivate the licenses from the controller to be replaced and activate or add the same number of licenses in the replacement controller:

Controller# license right-to-use deactivate ap-count 250 slot 1
Controller# license right-to-use activate ap-count 250 slot 1
Controller# show license right-to-use summary

Additional References for RTU Licensing

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTU commands</td>
<td>System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>RTU AP image preload feature</td>
<td>System Management Configuration Guide (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information for RTU Licensing

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Administrator Usernames and Passwords

- Finding Feature Information, page 77
- Information About Configuring Administrator Usernames and Passwords, page 77
- Configuring Administrator Usernames and Passwords, page 78
- Examples: Administrator Usernames and Passwords Configuration, page 80
- Additional References for Administrator Usernames and Passwords, page 81
- Feature History and Information For Performing Administrator Usernames and Passwords Configuration, page 82

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 controller 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 controller.

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, digits, and special characters.
- 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, ocisc, admin, nimda, or any variant obtained by changing the capitalization of letters therein, or by substituting "1" "|" 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.
## DETAILED STEPS

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

| **Step 2**        | Enables strong password policy for the administrator user. |
| wireless security strong-password | |
| Example: Controller(config)# wireless security strong-password | |

| **Step 3**        | Specifies a username and password for an administrator. The administrator can configure the controller and view the configured information. |
| username admin-username password {0 unencrypted_password | 7 hidden_password | unencrypted_text} | |
| Example: Controller(config)# username adminuser1 password 0 QZsek239@ | |

| **Step 4**        | Specifies the secret for the administrator. |
| username admin-username secret {0 unencrypted_secret_text | 4 SHA256 encrypted_secret_text | 5 MD5 encrypted_secret_text | LINE} | |
| Example: Controller(config)# username adminuser1 secret 0 QZsek239@ | |

| **Step 5**        | Specifies administrator username and password for managing all of the access points configured to the controller. You can also include the secret text to perform privileged access point management. |
| ap mgmtuser username username password {0 unencrypted_password | 8 AES encrypted password }secret {0 unencrypted_password | 8 AES encrypted password } | |
| Example: Controller(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@ | |

| **Step 6**        | Specifies the 802.1X username and password for managing all of the access points configured to the controller. |
| ap dot1x username username password {0 unencrypted password | 8 AES encrypted password } | |
| Example: Controller(config)# ap dot1x username cisco password 0 Qwci12@ | |

**Note:** 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.

Controller# ap mgmtuser username cisco password 0 abcd secret 0 1234
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Configures the administrator username, password, and secret text for managing a specific access point that is configured to the controller.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Configures the 802.1X username and password for a specific access point.</td>
</tr>
</tbody>
</table>

### Examples: Administrator Usernames and Passwords Configuration

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

```plaintext
Controller# configure terminal
Controller(config)# wireless security strong-password
cController(config)# ap mgmtuser username cisco password Qwci12@ secret Qwci14@
Controller(config)# end
```

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

```plaintext
Controller# wireless security strong-password
Controller# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@ secret Qwci14@
Controller# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
Controller# end
```
# Additional References for Administrator Usernames and Passwords

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td><em>System Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
## Feature History and Information For Performing Administrator Usernames and Passwords Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 7

Configuring 802.11 parameters and Band Selection

• Finding Feature Information, page 83
• Restrictions on Band Selection, 802.11 Bands, and Parameters, page 83
• Information About Configuring Band Selection, 802.11 Bands, and Parameters, page 84
• How to Configure 802.11 Bands and Parameters, page 85
• Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters, page 96
• Configuration Examples for Band Selection, 802.11 Bands, and Parameters, page 100
• Additional References for 802.11 Parameters and Band Selection, page 102
• Feature History and Information For Performing 802.11 parameters and Band Selection Configuration, page 103

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 1040, 1140, 1250, 1260, 2600, 3500, 3600, 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 controller.

Band selection is enabled globally by default.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

#### 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 devices such as the Cisco Aironet 1140 and 3600 Series 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.
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td><code>wireless client band-select cycle-count cycle_count</code></td>
<td>Sets the probe cycle count for band select. You can enter a value between 1 and 10 for the <code>cycle_count</code> parameter.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# wireless client band-select cycle-count 3</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><code>wireless client band-select cycle-threshold milliseconds</code></td>
<td>Sets the time threshold for a new scanning cycle period. You can enter a value for threshold between 1 and 1000 for the <code>milliseconds</code> parameter.</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 4**

```
wireless client band-select expire suppression seconds
```

**Example:**

```
Controller(config)# wireless client band-select expire suppression 100
```

Sets the suppression expire to the band select.
You can enter a value for suppression between 10 to 200 for the `seconds` parameter.

**Step 5**

```
wlan wlan_profile_name wlan_ID SSID_network_name band-select
```

**Example:**

Controller(config)# wlan wlan1 25 ssid12
Controller(config-wlan)# band-select

Configures band selection on specific WLANs.
You can enter a value between 1 and 512 for the `wlan_ID` parameter.
You can enter the up to 32 alphanumeric characters for `SSID_network_name` parameter.

**Step 6**

```
wireless client band-select client-rssi client_rssi
```

**Example:**

```
Controller(config)# wireless client band-select client-rssi 40
```

Sets the client RSSI threshold.
You can enter a value for minimum dBm of a client RSSI to respond to a probe between 20 and 90 for the `client_rssi` parameter.

**Step 7**

```
end
```

**Example:**

```
Controller(config)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

**Step 8**

```
wlan wlan_profile_name wlan_ID SSID_network_name band-select
```

**Example:**

Controller(config-wlan)# band-select

Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** 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 {disable | mandatory | supported}
9. no ap dot11 5ghz shutdown
10. no ap dot11 24ghz shutdown
11. ap dot11 24ghz dot11g
12. end

DETAILLED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Controller# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ap dot11 5ghz shutdown</td>
<td>Disables the 802.11a band.</td>
</tr>
<tr>
<td>Example: Controller(config)# ap dot11 5ghz shutdown</td>
<td>Note You must disable the 802.11a band before configuring the 802.11a network parameters.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ap dot11 24ghz shutdown</td>
<td>Disables the 802.11b band.</td>
</tr>
<tr>
<td>Example: Controller(config)# ap dot11 24ghz shutdown</td>
<td>Note You must disable the 802.11b band before configuring the 802.11b network parameters.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ap dot11 {5ghz</td>
<td>24ghz} beaconperiod time_unit</td>
</tr>
<tr>
<td>Example: Controller(config)# ap dot11 5ghz beaconperiod 500</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>ap dot11 {5ghz</td>
<td>24ghz} fragmentation threshold</td>
</tr>
<tr>
<td>Example: Controller(config)# ap dot11 5ghz fragmentation 300</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>**ap dot11 {5ghz</td>
<td>24ghz} dtpc**&lt;br&gt;Enables access points to advertise their channels and transmit the power levels in beacons, and probe responses. 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 DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there. <strong>Note</strong>&lt;br&gt;On access points that run Cisco IOS software, this feature is called world mode.&lt;br&gt;The no form of the command disables the 802.11a or 802.11b DTPC setting.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>wireless client association limit number interval milliseconds</strong>&lt;br&gt;Specifies the maximum allowed clients that can be configured. 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. The association request limit interval is measured between 100 to 10000 milliseconds.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>**ap dot11 {5ghz</td>
<td>24ghz} rate {disable</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>no ap dot11 5ghz shutdown</strong>&lt;br&gt;Enables the 802.11a band. <strong>Note</strong>&lt;br&gt;The default value is enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>no ap dot11 24ghz shutdown</strong>&lt;br&gt;Enables the 802.11b band. <strong>Note</strong>&lt;br&gt;The default value is enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>ap dot11 24ghz dot11g</strong>&lt;br&gt;Enables or disables 802.11g network support.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config)# ap dot11 24ghz dot11g</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the 802.11 Bands (GUI)

**Step 1** Choose *Configuration > Wireless > 802.11a/n/ac > Network* or *Configuration > Wireless > 802.11b/g/n > Network* to open the Global Parameters page.

**Step 2** Select the *802.11a/n/ac* (or *802.11b/g*) *Network Status* check box to enable the 802.11a or 802.11b/g band. To disable the band, unselect the check box. The default value is enabled. You can enable both the 802.11a and 802.11b/g bands.

**Step 3** If you enabled the 802.11b/g band in *Step 2*, select the *802.11g Support* check box if you want to enable 802.11g network support. The default value is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

**Step 4** Specify the period at which the SSID is broadcast by the access point by entering a value between 20 and 1000 milliseconds (inclusive) in the Beacon Period text box. The default value is 100 milliseconds. **Note** The beacon period in controllers is listed in terms of milliseconds. The beacon period can also be measured in time units, where one time unit equals 1024 microseconds or 102.4 milliseconds. If a beacon interval is listed as 100 milliseconds in a controller, it is only a rounded off value for 102.4 milliseconds. Due to hardware limitation in certain radios, even though the beacon interval is, say 100 time units, it is adjusted to 102 time units, which roughly equals 104.448 milliseconds. When the beacon period is to be represented in terms of time units, the value is adjusted to the nearest multiple of 17.

**Step 5** Specify the size at which packets are fragmented by entering a value between 256 and 2346 bytes (inclusive) in the Fragmentation Threshold text box. Enter a low number for areas where communication is poor or where there is a great deal of radio interference.

**Step 6** Make access points advertise their channel and transmit power level in beacons and probe responses for CCX clients. Select the *DTPC Support* check box. Otherwise, unselect this check box. The default value is enabled. **Note** On access points that run Cisco IOS software, this feature is called *world mode*. **Note** DTPC and 801.11h power constraint cannot be enabled simultaneously.

**Step 7** Specify the maximum allowed clients by entering a value between 1 to 200 in the Maximum Allowed Client text box. The default value is 200.

**Step 8** Use the *Data Rates* options to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
• 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps
• 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

• **Mandatory**—Clients must support this data rate in order to associate to an access point on the controller.
• **Supported**—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.
• **Disabled**—The clients specify the data rates used for communication.

**Step 9**  Click **Apply**.

**Step 10**  Click **Save Configuration**.

---

### 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. `wlan wlan_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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 {5ghz</td>
<td>24ghz} dot11n</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config)# ap dot11 5ghz dot11n</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring 802.11 Parameters and Band Selection

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`ap dot11 {5ghz</td>
<td>24ghz} dot11n mcs tx rtu`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Controller(config)# ap dot11 5ghz dot11n mcs tx 20</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>wlan wlan_profile_name wlan_ID SSID_network_name wmm require</code></td>
<td>Enables WMM on the WLAN and uses the 802.11n data rates that you configured. The require parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Controller(config)# wlan wlan1 25 ssid12 Controller(config-wlan)# wmm require</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>`ap dot11 {5ghz</td>
<td>24ghz} shutdown`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Controller(config)# ap dot11 5ghz shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>`{ap</td>
<td>no ap} dot11 {5ghz</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Controller(config)# ap dot11 5ghz dot11n a-mpdu tx priority all</code></td>
<td></td>
</tr>
</tbody>
</table>

### Table 6: Traffic Type Priority Levels

<table>
<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>
</tbody>
</table>
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.

- When you use the **ap** command along with the other options, the traffic associated with that priority level uses A-MPDU transmission.
- When you use the **no ap** command along with the other options, the traffic associated with that priority level uses A-MSDU transmission.

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.
Configuring the 802.11n Parameters (GUI)

Step 1: Choose Configuration > Wireless > 802.11a/n/ac or 802.11b/g/n > High Throughput (802.11n) to open the 802.11n/ac (5 GHz or 2.4 GHz) Throughput page.

Step 2: Select the Enable 11n check box to enable 802.11n support on the network. The default value is enabled.

Step 3: Select the check boxes of the desired rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. These data rates, which are calculated for a 20-MHz channel width using a short guard interval, are available:

- 0 (7 Mbps)
- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps)
- 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
- 10 (43 Mbps)
- 11 (58 Mbps)
- 12 (87 Mbps)
- 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)
- 16 (22 Mbps)
- 17 (43 Mbps)
- 18 (65 Mbps)
- 19 (87 Mbps)
- 20 (130 Mbps)
- 21 (173 Mbps)
- 22 (195 Mbps)
- 23 (217 Mbps)
- Any associated clients that support the selected rates may communicate with the access point using those rates. However, the clients are not required to be able to use this rate in order to associate. The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used.

**Step 4** Click **Apply**.

**Step 5** Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

a) Choose **WLANs** to open the WLANs page.
b) Click the ID number of the WLAN for which you want to configure WMM mode.
c) When the WLANs > Edit page appears, choose the **QoS** tab to open the WLANs > Edit (Qos) page.
d) From the WMM Policy drop-down list, choose **Required** or **Allowed** to require or allow client devices to use WMM. Devices that do not support WMM cannot join the WLAN.
   If you choose **Allowed**, devices that cannot support WMM can join the WLAN but will not benefit from the 802.11n rates.
e) Click **Apply**.

**Step 6** Click **Save Configuration**.

**Note** To determine if an access point supports 802.11n, look at the 11n Supported text box on either the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page or the 802.11a/n (or 802.11b/g/n) AP Interfaces > Details page.

---

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ap dot11 5ghz shutdown</td>
<td>Disables the 802.11a network.</td>
</tr>
<tr>
<td>Example: Controller(config)# ap dot11 5ghz shutdown</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring 802.11 parameters and Band Selection

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 3 | `{ap | no ap} dot11 5ghz channelswitch mode switch_mode` | 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 `channelswitch` 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 | `ap dot11 5ghz power-constraint value` | 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 | `no ap dot11 5ghz shutdown` | Reenables the 802.11a network. |
| Step 6 | `end` | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |

### Configuring the 802.11h Parameters (GUI)

**Step 1**  
Disable the 802.11 band as follows:  
a) Choose Configuration > Wireless > 802.11a/n/ac > Network to open the 802.11a/n/ac Global Parameters page.  
b) Unselect the 802.11a Network Status check box.  
c) Click Apply.  

**Step 2**  
Choose Configuration > Wireless > 802.11a/n/ac > DFS (802.11h) to open the 802.11h Global Parameters page.  

**Step 3**  
In the Power Constraint area, enter the local power constraint. The valid range is between 0 dBm and 30 dBm.  

**Step 4**  
In the Channel Switch Announcement area, enter the channel switch announcement mode. You can enter a value of either 1 or 0.  

**Step 5**  
Click Apply.  

**Step 6**  
Reenable the 802.11a band as follows:  
a) Choose Wireless > 802.11a/n/ac > Network to open the 802.11a/n/ac Global Parameters page.  
b) Select the 802.11a Network Status check box.  
c) Click Apply.  

**Step 7**  
Click Save Configuration.
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 controller.

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

Example: Viewing the Configuration Settings for 5-GHz Band

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

Controller# 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
Example: Viewing the status of 802.11h Parameters

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

Example: Verifying the Band Selection Settings

Controller# show wireless band-select
Band Select Probe Response : per WLAN enabling
Cycle Count : 2
Cycle Threshold (millisecond): 200
Age Out Suppression (second): 20
Age Out Dual Band (second): 60
Client 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:

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

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

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

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

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

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

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

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

```
Controller# configure terminal
Controller(config)# wlan wlan1 25 ssid12
Controller(config-wlan)# band-select
Controller(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:

```
Controller# configure terminal
Controller(config)# ap dot11 5ghz shutdown
Controller(config)# ap dot11 24ghz shutdown
Controller(config)# ap dot11 5ghz beaconperiod 500
Controller(config)# ap dot11 5ghz fragmentation 300
Controller(config)# ap dot11 5ghz.dtpc
Controller(config)# wireless client association limit 50 interval 1000
Controller(config)# ap dot11 5ghz rate 36 mandatory
Controller(config)# no ap dot11 5ghz shutdown
Controller(config)# no ap dot11 24ghz shutdown
Controller(config)# ap dot11 24ghz dot11g
Controller(config)# end
```
Examples: 802.11n Configuration

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

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

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

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

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

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

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

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

```
Controller# configure terminal
Controller(config)# ap dot11 5ghz shutdown
Controller(config)# ap dot11 5ghz power-constraint 200
Controller(config)# no ap dot11 5ghz shutdown
Controller(config)# end
```
# Additional References for 802.11 Parameters and Band Selection

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td><em>System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</em></td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

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

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
## Feature History and Information For Performing 802.11 parameters and Band Selection Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 8

Configuring Aggressive Load Balancing

- Finding Feature Information, page 105
- Restrictions for Aggressive Load Balancing, page 105
- Information for Configuring Aggressive Load Balancing Parameters, page 106
- How to Configure Aggressive Load Balancing, page 107
- Monitoring Aggressive Load Balancing, page 108
- Examples: Aggressive Load Balancing Configuration, page 108
- Additional References for Aggressive Load Balancing, page 109
- Feature History and Information For Performing Aggressive Load Balancing Configuration, page 110

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 probe 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 controller but not for the clients between access points on the different controller.
• The load balancing uses an existing association denial mechanism based on the number of clients 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 responds 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 reached or 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).

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).

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless load-balancing window client-count</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config)# wireless load-balancing window 1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wireless load-balancing denial denial-count</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config)# wireless load-balancing denial-count 1</td>
</tr>
</tbody>
</table>
### Step 4

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Controller(config)# end
```

### Step 5

#### wlan wlan_profile_name wlan_ID SSID_network_name load-balance

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wlan wlan_profile_name wlan_ID SSID_network_name load-balance</code></td>
<td>Enables or disables aggressive load balancing on specific WLANs. You can enter a value between 1 and 512 for the <code>wlan_ID</code> parameter. You can enter the up to 32 alphanumeric characters for <code>SSID_network_name</code> parameter.</td>
</tr>
</tbody>
</table>

**Example:**

```
Controller(config)# wlan wlan1 25 ssid12
Controller(config-wlan)# load-balance
```

### Step 6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Controller(config)# end
```

---

### 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 controller.

**Table 8: Monitoring Aggressive Load Balancing Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless load-balancing</code></td>
<td>Displays the status of the load-balancing feature.</td>
</tr>
</tbody>
</table>

### Examples: Aggressive Load Balancing Configuration

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

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

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

```
Controller# configure terminal
Controller(config)# wireless load-balancing window 1
Controller(config)# end
Controller# show wireless load-balancing
```
This example shows how to configure load balancing on specific WLAN:

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

### Additional References for Aggressive Load Balancing

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature History and Information For Performing Aggressive Load Balancing Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Client Roaming

• Finding Feature Information, page 111
• Prerequisites for Configuring Client Roaming, page 111
• Restrictions for Configuring Client Roaming, page 111
• Information About Client Roaming, page 112
• How to Configure Layer 2 or Layer 3 Roaming, page 114
• Monitoring Client Roaming Parameters, page 121
• Monitoring Mobility Configurations, page 121
• Additional References for Configuring Client Roaming, page 123
• Feature History and Information For Performing Client Roaming Configuration, page 124

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 Configuring Client Roaming

• There should be one active mobility controller to manage client roaming.
• The WLAN SSID on the mobility agents across which roaming is desired should be the same.

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 controller and cannot be disabled. The controller 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 Unified Wireless Network (Cisco UWN) 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 UWN 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

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

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} | default | custom min-rssi roam-hyst scan-thresh trans-time |
3. end
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td><strong>Configures CCX Layer 2 client roaming parameters.</strong></td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>To choose the default RF parameters, enter the <code>default</code> option.</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>To fine-tune the RF parameters that affect client roaming, enter the <code>custom</code> option and then enter any one of the following options:</strong></td>
</tr>
<tr>
<td>`ap dot11 {5ghz</td>
<td>24ghz} l2roam rf-params {default</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# <code>ap dot11 5ghz l2roam rf-params custom -80</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Mobility Oracle

#### SUMMARY STEPS

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

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller# configure terminal</td>
<td>--</td>
</tr>
<tr>
<td><strong>Step 2</strong> wireless mobility oracle</td>
<td>Enables mobility oracle on the controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# wireless mobility oracle</td>
<td>--</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# end</td>
<td>--</td>
</tr>
</tbody>
</table>
## 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-group 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>wireless mobility controller</td>
<td>Enables wireless mobility controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# wireless mobility controller</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wireless mobility controller peer-group switch-peer-group-name</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# wireless mobility controller peer-group SPG1</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The No form of the command deletes the switch peer group.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>wireless mobility controller peer-group switch-peer-group-name member ip ip-address {public-ip public-ip-address}</td>
<td>Adds a mobility group member to a switch peer group.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The No form of the command deletes the member from the switch peer group.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>wireless mobility controller peer-group SPG1 member ip 10.0.0.1</td>
<td>Configures the multicast mode within a switch peer group.</td>
</tr>
<tr>
<td>4</td>
<td>wireless mobility controller peer-group switch-peer-group-name multicast ip peer-group-multicast-ip-addr</td>
<td>Configures the multicast IP address for a switch peer group.</td>
</tr>
<tr>
<td>5</td>
<td>wireless mobility controller peer-group switch-peer-group-name multicast</td>
<td>Configures the multicast mode within a switch peer group.</td>
</tr>
<tr>
<td>6</td>
<td>wireless mobility controller peer-group switch-peer-group-name multicast ip peer-group-multicast-ip-addr</td>
<td>Configures the multicast IP address for a switch peer group.</td>
</tr>
<tr>
<td>7</td>
<td>wireless mobility controller peer-group switch-peer-group-name bridge-domain-id {id}</td>
<td>Configures the bridge domain ID for a switch peer group. The default is zero.</td>
</tr>
<tr>
<td>8</td>
<td>wireless mobility group member ip {ip-address} [public-ip {public-ip-address}] [group {group-name}]</td>
<td>Adds a mobility group member.</td>
</tr>
<tr>
<td>9</td>
<td>wireless mobility dscp value</td>
<td>Sets the DSCP value for mobility control packet.</td>
</tr>
<tr>
<td>10</td>
<td>wireless mobility group keepalive {count</td>
<td>interval}</td>
</tr>
<tr>
<td>11</td>
<td>wireless mobility group name name</td>
<td>Specifies the case sensitive wireless mobility group name which can be ASCII printable string up to 31 characters.</td>
</tr>
<tr>
<td>12</td>
<td>wireless mobility oracle ip {mo-ip-address}</td>
<td>Configures the mobility oracle IP address.</td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code> Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>wireless mobility controller ip ip-address</code> Sets the IP address of the mobility controller.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# <code>wireless mobility controller ip 10.10.10.20</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>wireless mobility load-balance</code> Configures wireless mobility load balancing.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# <code>wireless mobility load-balance</code></td>
</tr>
</tbody>
</table>
### 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 controller.

**Table 9: Monitoring Client Roaming Parameters Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ap dot11 {5ghz</td>
<td>24ghz} l2roam rf-param`</td>
</tr>
<tr>
<td>`show ap dot11 {5ghz</td>
<td>24ghz} l2roam statistics`</td>
</tr>
<tr>
<td>`show ap dot11 {5ghz</td>
<td>24ghz} l2roam mac-address mac-address statistics`</td>
</tr>
</tbody>
</table>

### 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 10: Monitoring Mobility Configuration Commands on the Mobility Controller and Mobility Agent

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless mobility summary</code></td>
<td>Displays the summary information for the Mobility Controller and Mobility Agent.</td>
</tr>
<tr>
<td><code>show wireless mobility statistics</code></td>
<td>Displays mobility statistics.</td>
</tr>
<tr>
<td><code>show wireless mobility dtls connections</code></td>
<td>Displays established DTLS connections.</td>
</tr>
</tbody>
</table>

### Table 11: Monitoring Mobility Configuration Commands on the Mobility Oracle

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

### Table 12: Monitoring Mobility Configuration Commands on the Mobility Controller

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show wireless mobility controller client summary</code></td>
<td>Displays a list of clients in the subdomain.</td>
</tr>
<tr>
<td><code>show wireless mobility controller client mac-address detail</code></td>
<td>Displays detailed information for a client in a subdomain.</td>
</tr>
<tr>
<td><code>show wireless mobility agent ma-ip client summary</code></td>
<td>Displays a list of clients anchored or associated to a specified Mobility Agent.</td>
</tr>
<tr>
<td><code>show wireless mobility ap-list</code></td>
<td>Displays the list of Cisco APs known to the mobility group.</td>
</tr>
</tbody>
</table>
### Table 13: Monitoring Mobility Configuration Commands on the Mobility Agent

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless mobility load-balance summary</td>
<td>Displays the summary of mobility load-balance properties.</td>
</tr>
</tbody>
</table>

### Additional References for Configuring Client Roaming

#### Related Documents

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

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Client Roaming Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 10

Configuring Application Visibility and Control

- Finding Feature Information, page 125
- Information About Application Visibility and Control, page 125
- Supported AVC Class Map and Policy Map Formats, page 126
- Prerequisites for Application Visibility and Control, page 129
- Guidelines for Inter-Controller Roaming with Application Visibility and Control, page 129
- Restrictions for Application Visibility and Control, page 129
- How to Configure Application Visibility and Control, page 131
- Monitoring Application Visibility and Control, page 149
- Examples: Application Visibility and Control, page 151
- Additional References for Application Visibility and Control, page 154
- Feature History and Information For Application Visibility and Control, page 155

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 (NBAR2) 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.

AVC is configured by defining a class map in a QoS client policy to match a protocol.
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.

Traffic flows are analyzed and recognized using the NBAR2 engine at the access point. Refer to [8.0 protocol pack](#) for the NBAR2-supported protocols or applications. The specific flow is marked with the recognized protocol or application, such as WebEx. This per-flow information can be used for application visibility using Flexible NetFlow (FNF). For more information on FNF, see the *Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*. The same application name can also be used for control of traffic using QoS. For more information on QoS, see the *QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*.

AVC QoS actions are applied with AVC filters in both upstream and downstream directions. The QoS actions supported for upstream flow are drop, mark, and police, and for downstream flow are mark and police. AVC QoS is applicable only when the application is classified correctly and matched with the class map filter in the policy map. For example, if the policy has a filter based on an application name, and the traffic has also been classified to the same application name, then the action specified for this match in the policy will be applied. For all QoS actions, refer *Supported AVC Class Map and Policy Map Formats*, on page 126.

### Supported AVC Class Map and Policy Map Formats

#### Supported AVC Class Map Format

<table>
<thead>
<tr>
<th>Class Map Format</th>
<th>Class Map Example</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>match protocol</td>
<td>protocol name</td>
<td>Both upstream and downstream</td>
</tr>
<tr>
<td>match protocol attribute category</td>
<td>category-name</td>
<td>Both upstream and downstream</td>
</tr>
<tr>
<td>match protocol attribute sub-category</td>
<td>sub-category-name</td>
<td>Both upstream and downstream</td>
</tr>
<tr>
<td>match protocol attribute application-group</td>
<td>application-group-name</td>
<td>Both upstream and downstream</td>
</tr>
<tr>
<td>Combination filters</td>
<td></td>
<td>Upstream only</td>
</tr>
</tbody>
</table>

**Supported AVC Class Map Format**

- **match protocol protocol name**
  - class-map match-any webex-class
  - match protocol webex-media

- **match protocol attribute category category-name**
  - class-map match-any IM
  - match protocol attribute category instant-messaging

- **match protocol attribute sub-category sub-category-name**
  - class-map match-any realtimeconferencing
  - match protocol attribute sub-category voice-video-chat-collaboration

- **match protocol attribute application-group application-group-name**
  - class-map match-any skype
  - match protocol attribute application-group skype-group

- Combination filters
  - class-map match-any webex-class
  - match protocol webex
  - match dscp 45
  - match wlan user-priority 6

---

*[OL-32324-01 System Management Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*]
Supported AVC Policy Format

<table>
<thead>
<tr>
<th>Policy Format</th>
<th>QoS Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstream client policy based on match protocol filter</td>
<td>Mark, police, and drop</td>
</tr>
<tr>
<td>Downstream client policy based on match protocol filter</td>
<td>Mark and police</td>
</tr>
</tbody>
</table>

The following table describes the detailed AVC policy format with an example:
<table>
<thead>
<tr>
<th>AVC Policy Format</th>
<th>AVC Policy Example</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic set</td>
<td>policy-map webex-policy&lt;br&gt;class webex-class&lt;br&gt;set dscp ef //or set up,cos</td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Basic police</td>
<td>policy-map webex-policy&lt;br&gt;class webex-class&lt;br&gt;police 5000000</td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Basic set and police</td>
<td>policy-map webex-policy&lt;br&gt;class webex-class&lt;br&gt;set dscp ef //or set up,cos&lt;br&gt;police 5000000</td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Multiple set and police including default</td>
<td>policy-map webex-policy&lt;br&gt;class webex-class&lt;br&gt;set dscp af31 //or set up,cos&lt;br&gt;police 4000000&lt;br&gt;class class-webex-category&lt;br&gt;set dscp ef //or set up,cos&lt;br&gt;police 5000000&lt;br&gt;class class-default&lt;br&gt;set dscp &lt;&gt;</td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Hierarchical police</td>
<td>policy-map webex-policy&lt;br&gt;class webex-class&lt;br&gt;police 5000000&lt;br&gt;service-policy&lt;br&gt;client-in-policy-only&lt;br&gt;policy-map&lt;br&gt;client-in-policy-only&lt;br&gt;class webex-class&lt;br&gt;police 100000&lt;br&gt;class class-webex-category&lt;br&gt;set dscp ef //or set up,cos&lt;br&gt;police 5000000&lt;br&gt;police 6000000&lt;br&gt;police 200000</td>
<td>Upstream and downstream</td>
</tr>
<tr>
<td>Hierarchical set and police</td>
<td>policy-map webex-policy&lt;br&gt;class class-default&lt;br&gt;police 1500000&lt;br&gt;service policy&lt;br&gt;client-up-child&lt;br&gt;policy-map webex-policy&lt;br&gt;class webex-class&lt;br&gt;police 100000&lt;br&gt;set dscp ef&lt;br&gt;class class-webex-category&lt;br&gt;police 200000&lt;br&gt;set dscp af31</td>
<td>Upstream only</td>
</tr>
<tr>
<td>Drop action</td>
<td></td>
<td>Upstream only</td>
</tr>
</tbody>
</table>
### Prerequisites for Application Visibility and Control

- The access points should be AVC capable.
- For the control part of AVC (QoS) to work, the application visibility feature with FNF has to be configured.

### Guidelines for Inter-Controller Roaming with Application Visibility and Control

Follow these guidelines to prevent clients from getting excluded due to malformed QoS policies:

- When a new QoS policy is added to the controller, a QoS policy with the same name should be added to other controller within the same roam or mobility domain.
- When a controller is loaded with a software image of a later release, the new policy formats are supported. If you have upgraded the software image from an earlier release to a later release, you should save the configuration separately. When an earlier release image is loaded, some QoS policies might show as not supported, and you should restore those QoS policies to supported policy formats.

### 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.
• Only the applications that are recognized with application visibility can be used for applying QoS control.
• 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. For more information, refer Creating a Flow Exporter (Optional), on page 133.

• When there is a mix of AVC-enabled APs such as 3600, and non-AVC-enabled APs such as 1140, and the chosen policy for the client is AVC-enabled, the policy will not be sent to the APs that cannot support AVC.

• Only ingress AVC statistics are supported. The frequency of statistics updates depends on the number of clients loaded at the AP at that time. Statistics are not supported for very large policy format sizes.

• The total number of flows for which downstream AVC QoS supported per client is 1000.

• The maximum number of flows supported for Cisco WLC 5700 Series is 360 K and Catalyst 3850 Series Switch is 48 K.

• These are some class map and policy map-related restrictions. For supported policy formats, see Supported AVC Class Map and Policy Map Formats, on page 126.
  - AVC and non-AVC classes cannot be defined together in a policy in a downstream direction. For example, when you have a class map with match protocol, you cannot use any other type of match filter in the policy map in the downstream direction.
  - Drop action is not applicable for the downstream AVC QoS policy.
  - Match protocol is not supported in ingress or egress for SSID policy.
How to Configure Application Visibility and Control

Configuring Application Visibility and Control (CLI)

To configure Application Visibility, follow these general steps:

1. Create a flow record by specifying keys and non-key fields to the flow.
2. Create an optional flow exporter by specifying the flow record as an option.
3. Create a flow monitor based on the flow record and flow exporter.
4. Configure WLAN to apply flow monitor in IPv4 input or output direction.

To configure Application Control, follow these general steps:

1. Create an AVC QoS policy.
2. Attach AVC QoS policy to the client in one of three ways: configuring WLAN, using ACS or ISE, or adding local policies.

Creating a Flow Record

By default, wireless avc basic (flow record) is available. When you click Apply from the GUI, then the record is mapped to the flow monitor.

Default flow record cannot be edited or deleted. If you require a new flow record, you need to create one and map it to the flow monitor from CLI.

SUMMARY STEPS

1. configure terminal
2. flow record flow_record_name
3. description string
4. match ipv4 protocol
5. match ipv4 source address
6. match ipv4 destination address
7. match transport source-port
8. match transport destination-port
9. match flow direction
10. match application name
11. match wireless ssid
12. collect counter bytes long
13. collect counter packets long
14. collect wireless ap mac address
15. collect wireless client mac address
16. end
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>flow record /flow_record_name</td>
<td>Enters flow record configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller(config)# flow record record1 Controller (config-flow-record)#</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>description string</td>
<td>(Optional) Describes the flow record as a maximum 63-character string.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller(config-flow-record)# description IPv4flow</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>match ipv4 protocol</td>
<td>Specifies a match to the IPv4 protocol.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-record)# match ipv4 protocol</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>match ipv4 source address</td>
<td>Specifies a match to the IPv4 source address-based field.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-record)# match ipv4 source address</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>match ipv4 destination address</td>
<td>Specifies a match to the IPv4 destination address-based field.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-record)# match ipv4 destination address</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>match transport source-port</td>
<td>Specifies a match to the transport layer source-port field.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-record)# match transport source-port</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>match transport destination-port</td>
<td>Specifies a match to the transport layer destination-port field.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-record)# match transport destination-port</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>match flow direction</td>
<td>Specifies a match to the direction the flow was monitored in.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-record)# match flow direction</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>match application name</td>
<td>Specifies a match to the application name.</td>
</tr>
</tbody>
</table>
## Configuring Application Visibility and Control (CLI)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong> match wireless ssid</td>
<td>Specifies a match to the SSID name identifying the wireless network.</td>
<td>Controller (config-flow-record)# match wireless ssid</td>
</tr>
<tr>
<td><strong>Step 12</strong> collect counter bytes long</td>
<td>Specifies to collect counter fields total bytes.</td>
<td>Controller (config-flow-record)# collect counter bytes long</td>
</tr>
<tr>
<td><strong>Step 13</strong> collect counter packets long</td>
<td>Specifies to collect counter fields total packets.</td>
<td>Controller (config-flow-record)# collect counter bytes long</td>
</tr>
<tr>
<td><strong>Step 14</strong> collect wireless ap mac address</td>
<td>Specifies to collect the BSSID with MAC addresses of the access points that the wireless client is associated with.</td>
<td>Controller (config-flow-record)# collect wireless ap mac address</td>
</tr>
<tr>
<td><strong>Step 15</strong> collect wireless client mac address</td>
<td>Specifies to collect MAC address of the client on the wireless network.</td>
<td>Controller (config-flow-record)# collect wireless client mac address</td>
</tr>
<tr>
<td><strong>Step 16</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <strong>Ctrl-Z</strong> to exit global configuration mode.</td>
<td>Controller(config)# end</td>
</tr>
</tbody>
</table>

### Creating a Flow Exporter (Optional)

You can create a flow export to define the export parameters for a flow. This is an optional procedure for configuring flow parameters.

---

**Note**: This action is mandatory for AVC support, as this allows the flow to be matched against the application.
SUMMARY STEPS

1. configure terminal
2. flow exporter flow_exporter_name
3. description string
4. destination {hostname | ip-address}
5. transport udp port-value
6. option application-table timeout seconds (optional)
7. option usermac-table timeout seconds (optional)
8. end
9. show flow exporter
10. end

DETAILED STEPS

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

| **Step 2**        |         |
| flow exporter flow_exporter_name | Enters flow exporter configuration mode. |
| Example:           |         |
| Controller(config)# flow exporter record1 |         |
| Controller (config-flow-exporter)# |         |

| **Step 3**        |         |
| description string | Describes the flow record as a maximum 63-character string. |
| Example:           |         |
| Controller(config-flow-exporter)# description IPv4flow |         |

| **Step 4**        |         |
| destination {hostname | ip-address} | Specifies the hostname or IPv4 address of the system to which the exporter sends data. |
| Example:           |         |
| Controller (config-flow-exporter) # destination 10.99.1.4 |         |

| **Step 5**        |         |
| transport udp port-value | Configures a port value for the UDP protocol. |
| Example:           |         |
| Controller (config-flow-exporter) # transport udp 2 |         |

| **Step 6**        |         |
| option application-table timeout seconds (optional) | (Optional) Specifies application table timeout option. The valid range is from 1 to 86400 seconds. |
| Example:           |         |
| Controller (config-flow-exporter)# option application-table timeout 500 |         |
### Command or Action

**Step 7**  
**Option Command or Action:** `option usermac-table timeout seconds (optional)`

**Example:**
```
Controller (config-flow-exporter)# option usermac-table timeout 1000
```

(Optional) Specifies wireless usermac-to-username table option. The valid range is from 1 to 86400 seconds.

**Step 8**  
**Command or Action:** `end`

**Example:**
```
Controller(config)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode.

**Step 9**  
**Command or Action:** `show flow exporter`

**Example:**
```
Controller # show flow exporter
```

Verifies your configuration.

**Step 10**  
**Command or Action:** `end`

**Example:**
```
Controller(config)# end
```

Returns to privileged EXEC mode. Alternatively, you can also press `Ctrl-Z` to exit global configuration mode.

---

### Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter.

#### SUMMARY STEPS

1. `configure terminal`
2. `flow monitor monitor-name`
3. `description description`
4. `record record-name`
5. `exporter exporter-name`
6. `cache timeout {active | inactive} (Optional)`
7. `end`
8. `show flow monitor`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
</tbody>
</table>

**Example:**
```
Controller# configure terminal
```

Enters global configuration mode.
### Command or Action

<table>
<thead>
<tr>
<th>Step 2</th>
<th><code>flow monitor monitor-name</code></th>
<th>Creates a flow monitor and enters flow monitor configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Example: Controller (config)# flow monitor flow-monitor-1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>description description</code></td>
<td>Creates a description for the flow monitor.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-monitor)# description flow-monitor-1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>record record-name</code></td>
<td>Specifies the name of a recorder that was created previously.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-monitor)# record flow-record-1</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>exporter exporter-name</code></td>
<td>Specifies the name of an exporter that was created previously.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-monitor)# exporter flow-exporter-1</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>`cache timeout {active</td>
<td>inactive} (Optional)`</td>
</tr>
<tr>
<td></td>
<td>Example: Controller (config-flow-monitor)# cache timeout active 1800</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller (config-flow-monitor)# cache timeout inactive 200</td>
<td>Note To achieve optimal result for the AVC flow monitor, we recommend you to configure the inactive cache timeout value to be greater than 90 seconds.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>show flow monitor</code></td>
<td>Verifies your configuration.</td>
</tr>
<tr>
<td></td>
<td>Example: Controller # show flow monitor</td>
<td></td>
</tr>
</tbody>
</table>

### Creating AVC QoS Policy

To create AVC QoS policy, perform these general steps:

1. Create a class map with match protocol filters.
2. Create a policy map.
3. Apply a policy map to the client in one of the following ways:
   - Apply a policy map over WLAN either from the CLI or GUI.
b  Apply a policy map through the AAA server (ACS server or ISE) from the CLI.
   For more information, refer to the Cisco Identity Services Engine User Guide and Cisco Secure Access
   Control System User Guide.

c  Apply local policies either from the CLI or GUI.

Creating a Class Map

You need to create a class map before configuring any match protocol filter. The QoS actions such as marking,
policing, and dropping can be applied to the traffic. The AVC match protocol filters are applied only for the
wireless clients. Refer 8.0 protocol pack for the protocols supported.

SUMMARY STEPS

1. configure terminal
2. class-map class-map-name
3. match protocol \{application-name | attribute category category-name | attribute sub-category
   sub-category-name | attribute application-group application-group-name\}
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> class-map class-map-name</td>
<td>Creates a class map.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config)# class-map webex-class</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3** match protocol \{application-name | attribute category category-name
   | attribute sub-category sub-category-name | attribute application-group application-group-name\} | Specifies match to the application name, category name, subcategory name, or application group. |
| **Example:** Controller(config)# class-map webex-class
Controller(config-cmap)# match protocol webex-media
Controller(config)# class-map class-webex-category
Controller(config-cmap)# match protocol attribute category webex-media
Controller# class-map class-webex-sub-category
Controller(config-cmap)# match protocol attribute sub-category webex-media
Controller# class-map class-webex-application-group |
Creating a Policy Map

**SUMMARY STEPS**

1. `configure terminal`
2. `policy-map policy-map-name`
3. `class [class-map-name | class-default]`
4. `police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]`
5. `set {dscp new-dscp | cos cos-value}`
6. `end`

**DETAILED STEPS**

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>policy-map <code>policy-map-name</code></th>
<th>Creates a policy map by entering the policy map name, and enters policy-map configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Controller(config)# <code>policy-map webex-policy</code></td>
<td>By default, no policy maps are defined.</td>
<td></td>
</tr>
<tr>
<td>Controller(config-pmap)#</td>
<td>The default behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> To delete an existing policy map, use the <code>no policy-map policy-map-name</code> global configuration command.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| Step 3 | class [class-map-name | class-default] | Defines a traffic classification, and enters policy-map class configuration mode. |
|--------|---------------------|-------------------------------------------------------------------------------|
| Example: Controller(config-pmap)# <code>class-map webex-class</code> | By default, no policy map and class maps are defined. |
| Controller(config-pmap-c)# | If a traffic class has already been defined by using the <code>class-map</code> global configuration command, specify its name for <code>class-map-name</code> in this command. |
| | A <code>class-default</code> traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied <code>match any</code> is included |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>in the class-default class, all packets that have not already matched the other traffic classes will match class-default. <strong>Note</strong> To delete an existing class map, use the no class class-map-name policy-map configuration command.</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 4** | police rate-bps burst-byte [exceed-action \{drop | policed-dscp-transmit\}]
Example:
Controller(config-pmap-c)# police 100000 80000 drop |
| Defines a policer for the classified traffic. By default, no policer is defined.
- For rate-bps, specify an average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
- For burst-byte, specify the normal burst size in bytes. The range is 8000 to 1000000.
- (Optional) Specifies the action to take when the rates are exceeded. Use the exceed-action drop keywords to drop the packet. Use the exceed-action policed-dscp-transmit keywords to mark down the DSCP value (by using the policed-DSCP map) and to send the packet. |
| **Step 5** | set \{dscp new-dscp | cos cos-value\}
Example:
Controller(config-pmap-c)# set dscp 45 |
| Classifies IP traffic by setting a new value in the packet.
- For dscp new-dscp, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63. |
| **Step 6** | end
Example:
Controller(config)# end |
| Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |

**What to Do Next**

After creating your policy maps, attach the traffic policy or polices to an interface using the service-policy command.

**Configuring Local Policies (CLI)**

To configure local policies, complete these procedures:

1. Create a service template.
2. Create a parameter map.
3. Create a policy map.
4. Apply a local policy on a WLAN.
# Creating a Service Template (CLI)

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>service-template service-template-name</code></td>
<td>Enters service template configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>service-template</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>cisco-phone-template</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller(config-service-template)# <code>access-group</code></td>
<td>Specifies the access list to be applied.</td>
</tr>
<tr>
<td></td>
<td><code>acl_list</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config-service-template)# <code>access-group</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>foo-acl</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>vlan vlan_id</code></td>
<td>Specifies VLAN ID. You can specify a value from 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config-service-template)# <code>vlan</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>100</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>absolute-timer seconds</code></td>
<td>Specifies session timeout value for service template. You can specify a value from 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config-service-template)# <code>absolute-timer</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>20</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>`service-policy qos {input</td>
<td>output}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config-service-template)# <code>service-policy</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>qos input foo-qos</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press <code>Ctrl-Z</code> to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>

## Creating a Parameter Map (CLI)

Parameter map is preferred to use than class map.
### DETAILED STEPS

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>parameter-map type subscriber attribute-to-service</td>
<td>Specifies the parameter map type and name.</td>
</tr>
<tr>
<td></td>
<td>parameter-map-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>map-index map { device-type</td>
<td>mac-address</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config-parameter-map-filter)# 10 map device-type eq &quot;WindowsXP-Workstation&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>service-template service-template-name</td>
<td>Enters service template configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config-parameter-map-filter-submode)# service-template cisco-phone-template</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

---

### Creating a Policy Map (CLI)

#### DETAILED STEPS

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

**Command or Action**

**Step 2**

`policy-map type control subscriber policy-map-name`

Specifies the policy map type.

**Example:**

```
Controller(config)# policy-map type control subscriber Aironet-Policy
```

**Step 3**

`event identity-update {match-all | match-first}`

Specifies match criteria to the policy map.

**Example:**

```
Controller(config-policy-map)# event identity-update match-all
```

**Step 4**

`class_number class {class_map_name | always } {do-all | do-until-failure | do-until-success}`

Configures the local profiling policy class map number and specifies how to perform the action. The class map configuration mode includes the following command options:

- **always**—Executes without doing any matching but returns success.
- **do-all**—Executes all the actions.
- **do-until-failure**—Execute all the actions until any match failure is encountered. This is the default value.
- **do-until-success**—Execute all the actions until any match success happens.

**Example:**

```
Controller(config-class-control-policymap)# 1 class local_policy1_class do-until-success
```

**Step 5**

`action-index map attribute-to-service table parameter-map-name`

Specifies parameter map table to be used.

**Example:**

```
Controller(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para
```

**Step 6**

`end`

Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

**Example:**

```
Controller(config)# end
```

### Applying a Local Policy for a Device on a WLAN (CLI)

**Before You Begin**

If the service policy contains any device type-based rules in the parameter map, ensure that the device classifier is already enabled.
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>  &lt;br&gt;Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wlan wlan-name</code></td>
<td>Enters WLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>  &lt;br&gt;Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>service-policy type control subscriber policymapname</code></td>
<td>Applies local policy to WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>  &lt;br&gt;Controller(config-wlan)# service-policy type control subscriber Aironet-Policy</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>profiling local http (optional)</code></td>
<td>Enables only profiling of devices based on HTTP protocol (optional).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>  &lt;br&gt;Controller(config-wlan)# profiling local http</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>profiling radius http (optional)</code></td>
<td>Enables profiling of devices on ISE (optional).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>  &lt;br&gt;Controller(config-wlan)# profiling radius http</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>no shutdown</code></td>
<td>Specifies not to shut down the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>  &lt;br&gt;Controller(config-wlan)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>  &lt;br&gt;Controller(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Local Policies (GUI)

To configure local policies, complete these procedures:

1. Create a service template.
2. Create a policy map.
3. Apply a local policy that you have created to a WLAN.
Creating a Service Template (GUI)

Step 1  
Choose Configuration > Security > Local Policies > Service Template to open the Service Template page.

Step 2  
Create a new template as follows:

   a) Click New to open the Service Template > New page.
   b) In the Service Template name text box, enter the new service template name.
   c) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
   d) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
   e) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
   f) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
   g) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
   h) Click Apply to save the configuration.

Step 3  
Edit a service template as follows:

   a) From the Service Template page, click the service template to open the Service Template > Edit page.
   b) In the VLAN ID text box, enter the VLAN identifier that has to be associated with the policy. The value ranges from 1 to 4094.
   c) In the Session timeout text box, enter the maximum amount of time, in seconds, after which a client is forced to reauthenticate. The value ranges from 1 to 65535 seconds.
   d) From the Access control list drop-down list, choose the access control list to be mapped to the policy.
   e) From the Ingress QoS drop-down list, choose the ingress QoS policy to be applied.
   f) From the Egress QoS drop-down list, choose the egress QoS policy to be applied.
   g) Click Apply to save the configuration.

Step 4  
Remove a service template as follows:

   a) From the Service Template page, select the service template.
   b) Click Remove.
   c) Click Apply to save the configuration.

Creating a Policy Map (GUI)

Step 1  
Choose Configuration > Security > Local Policies > Policy Map to open the Policy Map page.

Step 2  
Create a new policy map as follows:

   a) Click New to open the Policy Map > New page.
   b) In the Policy Map name text box, enter the new policy map name.
   c) Click Add to open the Match Criteria area.
   d) From the Device Type drop-down list, choose the device type. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
   e) From the User Role drop-down list, select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user, for example, student, teacher, and so on.
   f) From the Service Template drop-down list, choose the service template to be mapped to the policy.
g) Click Add. The match criteria is added to the Match Criteria Lists.
h) In the Match Criteria Lists area, click Add to add the match criteria to the policy.
i) Click Apply to save the configuration.

Step 3 Edit a policy map as follows:
a) In the Policy Map page, select the policy map that you want to edit, and click Edit to open the Policy Map > Edit page.
b) In the Match Criteria area, choose the device type from the Device Type drop-down list. The match criteria for the device type can be eq, not-eq, or regex with respect to the device type you are choosing.
c) In the Match Criteria area, choose the user role from the User Role drop-down list. Select the match criteria as eq, not-eq, or regex and enter the user type or user group of the user.
d) From the Service Template drop-down list, choose the service template to be mapped to the policy.
e) Click Ok to save the configuration or Cancel to discard the configuration.
f) Click Add to add more match criteria based on device type, user role, and service template to the policy.
g) In the Match Criteria Lists area, select the match criteria and click Move to to move the match criteria with respect to a value entered in the row text box.
h) Select the match criteria and click Move up to move the match criteria up in the list.
i) Select the match criteria and click Move down to move the match criteria down in the list.
j) Select the match criteria and click Remove to remove the match criteria from the policy map list.
k) Click Apply to save the configuration.

Step 4 Remove a policy map as follows:
a) From the Policy Map page, select the policy map.
b) Click Remove.
c) Click Apply to save the configuration.

Applying Local Policies to WLAN (GUI)

Step 1 Choose Configuration > Wireless > WLAN to open the WLANs page.
Step 2 Click the corresponding WLAN profile. The WLANs > Edit page is displayed.
Step 3 Click the Policy-Mapping tab.
Step 4 Check the Device Classification check box to enable classification based on device type.
Step 5 From the Local Subscriber Policy drop-down list, choose the policy that has to be applied for the WLAN.
Step 6 Select Local HTTP Profiling to enable profiling on devices based on HTTP (optional).
Step 7 Select Radius HTTP Profiling to enable profiling on devices based on RADIUS (optional).
Step 8 Click Apply to save the configuration.
Configuring WLAN to Apply Flow Monitor in IPV4 Input/Output Direction

SUMMARY STEPS

1. configure terminal
2. wlan wlan-id
3. ip flow monitor monitor-name {input | output}
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> wlan wlan-id</td>
<td>Enters WLAN configuration submode. For wlan-id, enter the WLAN ID. The range is 1 to 64.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config) # wlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip flow monitor monitor-name {input</td>
<td>output}</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller (config-wlan) # ip flow monitor flow-monitor-1 input</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

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.

---

**Configuring Application Visibility and Control (GUI)**

**Step 1**
Choose Configuration > Wireless.

**Step 2**
Expand the QoS node by clicking the left pane and choosing QOS-Policy.
The QOS-Policy page is displayed.

**Step 3**
Click Add New to create a new QoS Policy.
The Create QoS Policy page is displayed.

**Step 4**
Select Client from the Policy Type drop-down list.

**Step 5**
Select the direction into which the policy needs to be applied from the Policy Direction drop-down list.
The available options are:

- Ingress
- Egress

**Step 6**  In the **Policy Name** text box, specify a policy name.

**Step 7**  In the **Description** text box, provide a description to the policy.

**Step 8**  Check the **Enable Application Recognition** check box to configure the AVC class map for a client policy.

**Note**  For an egress client policy, when you enable Application Recognition, the Voice, Video, and User Defined check boxes are disabled.

The following options are available:

- **Trust**—Specify a classification type for this policy.
  
  * **Protocol**—Allows you to choose the protocols and configure the marking and policing of the packets.
  
  * **Category**—Allows you to choose the category of the application, for example, browsing.
  
  * **Subcategory**—Allows you to choose the subcategory of the application, for example, file-sharing.
  
  * **Application-Group**—Allows you to choose the application group, for example, ftp-group.

- **Protocol Choice**—Choose the protocols, category, subcategory, or application group from the **Available Protocols** list into the **Assigned Protocols** to apply the marking and policing of the packets.

- **Mark**—Specify the marking label for each packet. The following options are available:
  
  * **DSCP**—Assigns a label to indicate the given quality of service. The range is from 0 to 63.
  
  * **CoS**—Matches IEEE 802.1Q class of service. The range is from 0 to 7.
  
  * **None**—Does not mark the packets.

- **Police (kbps)**—Specify the policing rate in kbps. This option is available when the **Policy Direction** is egress.

- **Drop**—Specify to drop the ingress packets that correspond to the chosen protocols.

**Note**  You can add a maximum of five AVC classes for each client policy.

**Step 9**  Click **Add** to create an AVC class map. The new class map is listed in a tabular format.

**Step 10**  Click **Apply** to create an AVC QoS policy.

**Step 11**  Click the QoS policy link in the **QOS-Policy** page to edit the QoS policy. The **QOS-Policy > Edit** page is displayed. Make changes and click **Apply** to commit your changes.

**Step 12**  Remove an AVC class map from the QoS policy by navigating to the corresponding AVC class map row in the AVC class map table and clicking **Remove**. Click **Apply** to commit your changes.
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 controller and access points.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show avc client client-mac top n application [aggregate</td>
<td>Displays information about top &quot;N&quot; applications for the given client MAC.</td>
</tr>
<tr>
<td>upstream</td>
<td>downstream]</td>
</tr>
<tr>
<td>show avc wlan ssid top n application [aggregate</td>
<td>Displays information about top &quot;N&quot; applications for the given SSID.</td>
</tr>
<tr>
<td>upstream</td>
<td>downstream]</td>
</tr>
<tr>
<td>show wlan id wlan-id</td>
<td>Displays information whether AVC is enabled or disabled on a particular WLAN.</td>
</tr>
<tr>
<td>show flow monitor flow_monitor_name cache</td>
<td>Displays information about flow monitors.</td>
</tr>
<tr>
<td>show wireless client mac-address mac-address service-policy { input</td>
<td>output }</td>
</tr>
<tr>
<td>show policy-map target</td>
<td>Displays information about policy map.</td>
</tr>
<tr>
<td>show policy-map</td>
<td></td>
</tr>
<tr>
<td>show policy-map policy-name</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear avc client mac stats</td>
<td>Clears the statistics per client.</td>
</tr>
<tr>
<td>clear avc wlan wlan-name stats</td>
<td>Clears the statistics per WLAN.</td>
</tr>
</tbody>
</table>

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 controller. 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 (%)

**Monitoring SSID and Client Policies Statistics (GUI)**

Statistics are supported only for ingress policies with a maximum of five classes on wireless targets. For very large policies, statistics for ingress policies are not visible at the controller. The frequency of the statistics depends on the number of clients associated with the access point. Maximum time for the client statistics to appear at the controller is around 5 minutes.
<table>
<thead>
<tr>
<th>Type of Statistics</th>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID Policies</td>
<td>Choose Monitor &gt; Controller &gt; Statistics &gt; QoS.</td>
<td>The QoS page is displayed with a list of SSID policies, Radio Type, and AP. Choose an SSID policy, radio, and access point from the drop-down lists and click Apply to view the statistics of the chosen SSID policy. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.</td>
</tr>
<tr>
<td>Client Policies</td>
<td>Choose Monitor &gt; Clients &gt; Client Details.</td>
<td>The Clients page is displayed with a list of client MAC addresses, AP, and other details. Click the MAC address of a client and click the QoS Statistics tab. You can view details such as match criteria, confirmed bytes, conformed rate, and exceeded rate.</td>
</tr>
</tbody>
</table>

### 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:

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

Controller# configure terminal
Controller# flow monitor fm_v4
Controller(config-flow-monitor)# record fr_v4
Controller(config-flow-monitor)# cache timeout active 1800
```
Examples: Application Visibility and Control QoS Configuration

This example shows how to create class maps with apply match protocol filters for application name, category, and subcategory:

```
Controller# configure terminal
Controller(config)# class-map cat-browsing
Controller(config-cmap)# match protocol attribute category browsing
Controller(config-cmap)# end

Controller# configure terminal
Controller(config)# class-map cat-fileshare
Controller(config-cmap)# match protocol attribute category file-sharing
Controller(config-cmap)# end

Controller# configure terminal
Controller(config)# class-map match-any subcat-terminal
Controller(config-cmap)# match protocol attribute sub-category terminal
Controller(config-cmap)# end

Controller# configure terminal
Controller(config)# class-map match-any webex-meeting
Controller(config-cmap)# match protocol webex-meeting
Controller(config-cmap)# end
```

This example shows how to create policy maps and define existing class maps for upstream QoS:

```
Controller# configure terminal
Controller(config)# policy-map test-avc-up
Controller(config-pmap)# class cat-browsing
Controller(config-pmap-c)# police 150000
Controller(config-pmap-c)# set dscp 12
Controller(config-pmap-c)# end

Controller# configure terminal
Controller(config)# policy-map test-avc-up
Controller(config-pmap)# class cat-fileshare
Controller(config-pmap-c)# police 1000000
Controller(config-pmap-c)# set dscp 20
Controller(config-pmap-c)# end

Controller# configure terminal
Controller(config)# policy-map test-avc-up
Controller(config-pmap)# class subcat-terminal
Controller(config-pmap-c)# police 120000
Controller(config-pmap-c)# set dscp 15
Controller(config-pmap-c)# end

Controller# configure terminal
Controller(config)# policy-map test-avc-up
Controller(config-pmap)# class webex-meeting
Controller(config-pmap-c)# police 50000000
Controller(config-pmap-c)# set dscp 21
Controller(config-pmap-c)# end
```
This example shows how to create policy maps and define existing class maps for downstream QoS:

```plaintext
Controller# configure terminal
Controller(config)# policy-map test-avc-down
Controller(config-pmap)# class cat-browsing
Controller(config-pmap-c)# police 200000
Controller(config-pmap-c)# set dscp 10
Controller(config-pmap-c)# end

Controller# configure terminal
Controller(config)# policy-map test-avc-up
Controller(config-pmap)# class cat-fileshare
Controller(config-pmap-c)# police 300000
Controller(config-pmap-c)# set wlan user-priority 2
Controller(config-pmap-c)# set dscp 20
Controller(config-pmap-c)# end

Controller# configure terminal
Controller(config)# policy-map test-avc-up
Controller(config-pmap)# class subcat-terminal
Controller(config-pmap-c)# police 100000
Controller(config-pmap-c)# set dscp 25
Controller(config-pmap-c)# end

Controller# configure terminal
Controller(config)# policy-map test-avc-up
Controller(config-pmap)# class webex-meeting
Controller(config-pmap-c)# police 60000000
Controller(config-pmap-c)# set dscp 41
Controller(config-pmap-c)# end
```

This example shows how to apply defined QoS policy on a WLAN:

```plaintext
Controller# configure terminal
Controller(config)# wlan alpha
Controller(config-wlan)# shut
Controller(config-wlan)# end
Controller(config-wlan)# service-policy client input test-avc-up
Controller(config-wlan)# service-policy client output test-avc-down
Controller(config-wlan)# no shut
Controller(config-wlan)# end
```

**Example: Configuring QoS Attribute for Local Profiling Policy**

The following example shows how to configure QoS attribute for a local profiling policy:

```plaintext
Controller(config)# class-map type control subscriber match-all local_policy1_class
Controller(config-filter-control-classmap)# match device-type android
Controller(config)# service-template local_policy1_template
Controller(config-service-template)# vlan 40
Controller(config-service-template)# service-policy qos output local_policy1
Controller(config)# policy-map type control subscriber local_policy1
Controller(config-event-control-policymap)# event identity-update match-all
Controller(config-class-control-policymap)# 1 class local_policy1_class do-until-success
Controller(config-action-control-policymap)# 1 activate service-template local_policy1_template
Controller(config)# wlan open_auth 9
Controller(config-wlan)# client vlan VLAN40
Controller(config-wlan)# service-policy type control subscriber local_policy1
```
Additional References for Application Visibility and Control

Related Documents

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

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Application Visibility and Control

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3E</td>
<td>AVC control with QoS was introduced.</td>
</tr>
</tbody>
</table>
Configuring Voice and Video Parameters

• Finding Feature Information, page 157
• Prerequisites for Voice and Video Parameters, page 157
• Restrictions for Voice and Video Parameters, page 158
• Information About Configuring Voice and Video Parameters, page 158
• How to Configure Voice and Video Parameters, page 163
• Monitoring Voice and Video Parameters, page 175
• Configuration Examples for Voice and Video Parameters, page 177
• Additional References for Voice and Video Parameters, page 178
• Feature History and Information For Performing Voice and Video Parameters Configuration, page 179

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 controller 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.
- The following features are not supported for the 802.11 module on the Cisco 3600 Access Point:
  - Voice support
  - CAC support
  - TSM support

- When the 802.11 module is enabled, the 11n LBCAC parameters can be inaccurate resulting in degradation in voice quality of 11ac enabled calls.

- 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 controller 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 controller 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 controller 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, queueing, 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, controller 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 16: TSPEC Request Handling Examples

<table>
<thead>
<tr>
<th>CAC Mode</th>
<th>Reserved bandwidth for voice calls¹</th>
<th>Usage²</th>
<th>Normal TSPEC Request</th>
<th>TSPEC with Expedited Bandwidth Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth-based CAC</td>
<td>75% (default setting)</td>
<td>Less than 75%</td>
<td>Admitted</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between 75% and 90% (reserved bandwidth for voice calls exhausted)</td>
<td>Rejected</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>More than 90%</td>
<td>Rejected</td>
<td>Rejected</td>
</tr>
<tr>
<td>Load-based CAC</td>
<td>Less than 75%</td>
<td>Less than 75%</td>
<td>Admitted</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between 75% and 85% (reserved bandwidth for voice calls exhausted)</td>
<td>Rejected</td>
<td>Admitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>More than 85%</td>
<td>Rejected</td>
<td>Rejected</td>
</tr>
</tbody>
</table>

¹ 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.

² 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.

<table>
<thead>
<tr>
<th>TSM Entries</th>
<th>5700</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAX AP TSM entries</td>
<td>100</td>
</tr>
<tr>
<td>MAX Client TSM entries</td>
<td>250</td>
</tr>
<tr>
<td>MAX TSM entries</td>
<td>100*250=25000</td>
</tr>
</tbody>
</table>

**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 vice versa. 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 controller 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 controller 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 controller does not check the configured maximum voice bandwidth. The controller 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 output_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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show wlan summary</td>
<td>Specifies all of the WLANs configured on the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# show wlan summary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show wlan wlan_id</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# show wlan 25</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> policy-map policy-map name</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config)# policy-map test_2000 Controller(config-pmap)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> class {class-name</td>
<td>class-default}</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config-pmap)# class test_1000 Controller(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> admit cac wmm-tspec</td>
<td>(Optional) Admits the request for Call Admission Control (CAC) for policy map.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config-pmap-c)# admit cac wmm-tspec Controller(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> service-policy policy-map name</td>
<td>Configures the QoS service policy.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config-pmap-c)# service-policy test_2000 Controller(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> wlan wlan_profile_name wlan_ID SSID_network_name wlan shutdown</td>
<td>Disables all WLANs with WMM enabled prior to changing the video parameters.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Controller(config-wlan)# wlan shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>wlan wlan_profile_name wlan_ID SSID_network_name</td>
<td>Disables all WLANs with WMM enabled prior to changing the voice parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Controller(config-wlan)# wlan shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td>wlan wlan_name call-snoop</td>
<td>Enables the call-snooping on a particular WLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# wlan wlan1 call-snoop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td>wlan wlan_name service-policy input input_policy_name</td>
<td>Configures input SSID policy on a particular WLAN to voice.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Controller(config-wlan)# service-policy input platinum-up</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td></td>
</tr>
<tr>
<td>wlan wlan_name service-policy output output_policy_name</td>
<td>Configures output SSID policy on a particular WLAN to voice.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Controller(config-wlan)# service-policy output platinum</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td></td>
</tr>
<tr>
<td>wlan wlan_name service-policy input ingress_policy_name</td>
<td>Configures ingress SSID policy on a particular WLAN as user-defined policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Controller(config-wlan)# service-policy input policy1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td></td>
</tr>
<tr>
<td>wlan wlan_name service-policy output egress_policy_name</td>
<td>Configures egress SSID policy on a particular WLAN as user-defined policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td>Controller(config-wlan)# service-policy output policy2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td></td>
</tr>
<tr>
<td>ap dot11 {5ghz</td>
<td>24ghz} shutdown</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Controller(config)# ap dot11 5ghz shutdown</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td>Enables or disables SIP IOSd CAC for the 802.11a or 802.11b/g network.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config) # ap dot11 5ghz cac voice sip</td>
</tr>
<tr>
<td><strong>Step 18</strong></td>
<td>Enables or disables bandwidth-based voice CAC for the 802.11a or 802.11b/g network.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config) # ap dot11 5ghz cac voice acm</td>
</tr>
<tr>
<td><strong>Step 19</strong></td>
<td>Sets the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network. 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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config) # ap dot11 5ghz cac voice max-bandwidth 85</td>
</tr>
<tr>
<td><strong>Step 20</strong></td>
<td>Sets the percentage of maximum allocated bandwidth reserved for roaming voice clients. The bandwidth range is 0 to 25%, and the default value is 6%. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config) # ap dot11 5ghz cac voice roam-bandwidth 10</td>
</tr>
<tr>
<td><strong>Step 21</strong></td>
<td>Reenables all WLANs with WMM enabled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config-wlan) # no wlan shutdown</td>
</tr>
<tr>
<td><strong>Step 22</strong></td>
<td>Reenables the radio network.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config) # no ap dot11 5ghz shutdown</td>
</tr>
<tr>
<td><strong>Step 23</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config) # end</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>show wlan summary</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller# show wlan summary</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>show wlan wlan_id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller# show wlan 25</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller# configure terminal</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>policy-map policy-map name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# policy-map test_2000 Controller(config-pmap)#</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>`class {class-name</td>
<td>class-default}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config-pmap)# class test_1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>admit cac wmm-tspec</code></td>
<td><strong>Purpose</strong>: (Optional) Admits the request for Call Admission Control (CAC) for policy map.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config-pmap-c)# admit cac wmm-tspec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>service-policy policy-map name</code></td>
<td><strong>Purpose</strong>: Configures the QoS service policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config-pmap-c)# service-policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>test_2000 Controller(config-pmap-c)#</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>end</code></td>
<td><strong>Purpose</strong>: Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config)# end</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>wlan wlan_profile_name</code></td>
<td><strong>Purpose</strong>: Disables all WLANs with WMM enabled prior to changing the video parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller(config-wlan)# wlan shutdown</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} shutdown`</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config)# ap dot11 5ghz shutdown</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} cac video acm`</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config)# ap dot11 5ghz cac video acm</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} cac video load-based`</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config)# ap dot11 5ghz cac video load-based</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} cac video max-bandwidth bandwidth`</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: Controller(config)# ap dot11 5ghz cac video max-bandwidth 20</td>
<td></td>
</tr>
</tbody>
</table>

---

**Configuring Video Parameters (CLI)**

---

**System Management Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)**

168

**OL-32324-01**
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>should not exceed 85% or configured maximum media bandwidth.</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>ap dot11 {5ghz</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>no wlan shutdown wlan_id&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Controller(config-wlan)# no wlan shutdown 25</td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td>no ap dot11 {5ghz</td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td>end&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Controller(config)# end</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wlan wlan-name</code></td>
<td>Enters WLAN configuration submode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>wlan qos-wlan</code> Controller(config-wlan)#</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>call-snoop</code></td>
<td>Enables the call-snooping feature for a particular WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config-wlan)# <code>call-snoop</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>service-policy [client] input policy-map name</code></td>
<td>Assigns a policy map to WLAN input traffic. Ensure that you provide QoS policy to voice for input traffic.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config-wlan)# <code>service-policy input platinum-up</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>service-policy [client] output policy-map name</code></td>
<td>Assigns policy map to WLAN output traffic. Ensure that you provide QoS policy to voice for output traffic.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config-wlan)# <code>service-policy output platinum</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>`show wlan {wlan-id</td>
<td>wlan-name}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller# <code>show wlan qos-wlan</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} cac {voice</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>ap dot11 5ghz cac voice acm</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} cac voice sip`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>ap dot11 5ghz cac voice sip</code></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller(# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>wlan wlan-name qos platinum</td>
<td>Sets QoS to voice on a particular WLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller(config)# wlan wlan1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller(config-wlan)# qos platinum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ap dot11 {5ghz</td>
<td>24ghz} cac {voice</td>
</tr>
</tbody>
</table>
### Configuring Voice and Video Parameters (CLI)

**SUMMARY STEPS**

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz } shutdown`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>ap dot11 5ghz shutdown</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>`ap dot11 {5ghz</td>
<td>24ghz} edca-parameters {custom-voice</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>ap dot11 5ghz edca-parameters optimized-voice</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- custom-voice— Enables custom voice parameters for the 802.11a or 802.11b/g network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- optimized-video-voice— Enables EDCA voice- and video-optimized parameters for the 802.11a or 802.11b/g network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Choose this option when both voice and video services are deployed on your network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- optimized-voice— Enables non-SpectraLink voice-optimized profile parameters for the 802.11a or 802.11b/g network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Choose this option when voice services other than SpectraLink are deployed on your network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- svp-voice— Enables SpectraLink voice priority parameters for the 802.11a or 802.11b/g network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- wmm-default— Enables the Wi-Fi Multimedia (WMM) default parameters for the 802.11a or 802.11b/g network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is the default value. Choose this option when voice or video services are not deployed on your network.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>`show ap dot11 {5ghz</td>
<td>24ghz} network`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>show ap dot11 5ghz network</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>`no ap dot11 {5ghz</td>
<td>24ghz} shutdown`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Controller(config)# <code>no ap dot11 5ghz shutdown</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong></td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Controller(config)# end</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring EDCA Parameters (GUI)

**Step 1** Choose **Configuration > Wireless > 802.11a/n/ac > EDCA Parameters** or **Configuration > Wireless > 802.11b/g/n > EDCA Parameters** to open EDCA Parameters page.

**Step 2** Choose one of the following options from the **EDCA Profile** drop-down list:

- **wmm-default**—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- **svp-voice**—Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
- **optimized-voice**—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
- **optimized-video-voice**—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
- **custom-voice**—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

**Note** If you deploy video services, admission control (ACM) must be disabled.

**Step 3** If you want to enable MAC optimization for voice, select the **Enable Low Latency MAC** check box. Otherwise, leave this check box unselected, which is the default value. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point.

**Note** We do not recommend you to enable low latency MAC. You should enable low latency MAC only if the WLAN allows WMM clients. If WMM is enabled, then low latency MAC can be used with any of the EDCA profiles.

**Step 4** Click **Apply** to commit your changes.

**Step 5** To reenable the radio network, choose **Network** under 802.11a/n or 802.11b/g/n, select the **802.11a/n/ac** (or **802.11b/g/n** **Network Status** check box, and click **Apply**.

**Step 6** Click **Save Configuration**.
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 17: Monitoring Voice Parameters Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ap dot11 {5ghz</td>
<td>24ghz} network</td>
</tr>
<tr>
<td>show ap name ap_name dot11 24ghz tsm all</td>
<td>Displays the TSM voice metrics and current status of MAC optimization for voice.</td>
</tr>
<tr>
<td>show ap name apname cac voice</td>
<td>Displays the information about CAC for a particular access point.</td>
</tr>
<tr>
<td>show client detail client_mac</td>
<td>Displays the U-APSD status for a particular client.</td>
</tr>
<tr>
<td>show policy-map interface wireless client</td>
<td>Displays the video client policy details.</td>
</tr>
<tr>
<td>show access-list</td>
<td>Displays the video client dynamic access-list from the controller.</td>
</tr>
<tr>
<td>show wireless client voice diag status</td>
<td>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. <strong>Note</strong> To work on voice diagnostics CLIs, you need to enter the following command: <code>debug voice-diagnostic mac-addr client_mac_01 client_mac_02</code></td>
</tr>
<tr>
<td>show wireless client voice diag tspec</td>
<td>Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.</td>
</tr>
<tr>
<td>show wireless client voice diag qos-map</td>
<td>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.</td>
</tr>
<tr>
<td>show wireless client voice diag rssi</td>
<td>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.</td>
</tr>
<tr>
<td>show client voice-diag roam-history</td>
<td>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.</td>
</tr>
</tbody>
</table>
You can monitor the video parameters using the following commands.

### Table 18: Monitoring Video Parameters Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show policy-map interface wireless mac</strong> mac-address</td>
<td>Displays information about the voice and video data packet statistics.</td>
</tr>
<tr>
<td><strong>show wireless media-stream client summary</strong></td>
<td>Displays a summary of the media stream and video client information.</td>
</tr>
<tr>
<td>**show controllers d0</td>
<td>b queue**</td>
</tr>
<tr>
<td><strong>show platform qos queue stats interface</strong></td>
<td>Displays which queue packets are going through from the controller.</td>
</tr>
</tbody>
</table>

**Table 18: Monitoring Video Parameters Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ap join stats summary ap_mac</strong></td>
<td>Displays the last join error detail for a specific access point.</td>
</tr>
<tr>
<td><strong>show ip igmp snooping wireless mgid</strong></td>
<td>Displays the TSM voice metrics and current status of MAC optimization for voice.</td>
</tr>
<tr>
<td><strong>show wireless media-stream multicast-direct state</strong></td>
<td>Displays the media stream multicast-direct parameters.</td>
</tr>
<tr>
<td><strong>show wireless media-stream group summary</strong></td>
<td>Displays the summary of the media stream and client information.</td>
</tr>
<tr>
<td><strong>show wireless media-stream group detail</strong> group_name</td>
<td>Displays the details of a specific media-stream group.</td>
</tr>
<tr>
<td><strong>show wireless media-stream client summary</strong></td>
<td>Displays the details for a set of media-stream clients.</td>
</tr>
<tr>
<td><strong>show wireless media-stream client detail</strong> group_name</td>
<td>Displays the details for a set of media-stream clients.</td>
</tr>
<tr>
<td>**show ap dot11 {5ghz</td>
<td>24ghz} media-stream rrc**</td>
</tr>
<tr>
<td><strong>show wireless media-stream message details</strong></td>
<td>Displays information about the message configuration.</td>
</tr>
<tr>
<td>**show ap name ap-name auto-rf dot11 5ghz</td>
<td>i Util**</td>
</tr>
<tr>
<td>**show controllers d0</td>
<td>b queue**</td>
</tr>
<tr>
<td>**show controllers d1</td>
<td>b queue**</td>
</tr>
</tbody>
</table>
**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:

```plaintext
table-map egressssid_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
  queue-buffers ratio 0
  service-policy ssid-child-cac

policy-map ssid-child-cac
class voice
  priority level 1
  police 50000000
  conform-action transmit
  exceed-action drop
  admit cac wmm-tspec
  rate 1000
  wlan-up 6 7

class video
  priority level 2
  police 100000000
  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:

```plaintext
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

<table>
<thead>
<tr>
<th>Related Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Topic</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Multicast configuration</td>
</tr>
<tr>
<td>VideoStream configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standards and RFCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard/RFC</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>None</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Voice and Video Parameters Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 12

Configuring RFID Tag Tracking

• Finding Feature Information, page 181
• Information About Configuring RFID Tag Tracking, page 181
• How to Configure RFID Tag Tracking, page 182
• Monitoring RFID Tag Tracking Information, page 183
• Additional References RFID Tag Tracking, page 183
• Feature History and Information For Performing RFID Tag Tracking Configuration, page 184

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 Controller 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables RFID tag tracking.</td>
</tr>
<tr>
<td>location rfid status</td>
<td>By default, RFID tag tracking is enabled.</td>
</tr>
<tr>
<td>Example: Controller(config)# location rfid status</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Disables RFID tag tracking.</td>
</tr>
<tr>
<td>(Optional) no location rfid status</td>
<td></td>
</tr>
<tr>
<td>Example: Controller(config)# no location rfid status</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies a static timeout value (between 60 and 7200 seconds).</td>
</tr>
<tr>
<td>location rfid timeout seconds</td>
<td>The static timeout value is the amount of time that the controller 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.</td>
</tr>
<tr>
<td>Example: Controller(config)# location rfid timeout 1500</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables RFID tag mobility for specific tags. When you enter the location rfid mobility vendor-name command, tags are unable to obtain a DHCP address for client mode when attempting to select and/or download a configuration.</td>
</tr>
<tr>
<td>location rfid mobility vendor-name name</td>
<td>Note: These commands can be used only for Pango tags. Therefore, the only valid entry for vendor_name is &quot;pango&quot; in all lowercase letters.</td>
</tr>
<tr>
<td>Example: Controller(config)# location rfid mobility vendor-name Aerosct</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Disables RFID tag mobility for specific tags. When you enter the no location rfid mobility 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.</td>
</tr>
<tr>
<td>(Optional) no location rfid mobility name</td>
<td></td>
</tr>
<tr>
<td>Example: Controller(config)# no location rfid mobility test</td>
<td></td>
</tr>
</tbody>
</table>
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 controller.

Table 19: Monitoring RFID Tag Tracking Information Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show location rfid config</td>
<td>Displays the current configuration for RFID tag tracking.</td>
</tr>
<tr>
<td>show location rfid detail mac_address</td>
<td>Displays the detailed information for a specific RFID tag.</td>
</tr>
<tr>
<td>show location rfid summary</td>
<td>Displays a list of all RFID tags currently connected to the controller.</td>
</tr>
<tr>
<td>show location rfid client</td>
<td>Displays a list of RFID tags that are associated to the controller as clients.</td>
</tr>
</tbody>
</table>

Additional References RFID Tag Tracking

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing RFID Tag Tracking Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 13

Configuring Location Settings

- Finding Feature Information, page 185
- Information About Configuring Location Settings, page 185
- How to Configure Location Settings, page 186
- Monitoring Location Settings and NMS Settings, page 190
- Examples: Location Settings Configuration, page 191
- Examples: NMS Settings Configuration, page 191
- Additional References for Location Settings, page 192
- Feature History and Information For Performing Location Settings Configuration, page 193

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 controller determines the location of client devices by gathering Received Signal Strength Indication (RSSI) measurements from access points all around the client of interest. The controller 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>`location plm {calibrating [multiband</td>
<td>uniband]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# location plm client 100</td>
<td></td>
</tr>
</tbody>
</table>

The path loss measurement request improves the location accuracy. You can configure the `burst_interval` parameter for the normal, non-calibrating client from zero through 3600 seconds, and the default value is 60 seconds.

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.

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 `location plm` command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the Controller 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.
### Configuring Location Settings

**Purpose**
Configure the RSSI half life for the clients, calibrating clients, RFID tags, and rogue access points.

**Step 3**
- **Command or Action:** `location rssi-half-life \{calibrating-client | client | rogue-aps | tags \} seconds`
- **Example:**
  ```
  Controller(config)# location rssi-half-life calibrating-client 60
  ```

**Purpose**
You can enter the `location rssi-half-life` 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.

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 `location rssi-half-life` command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or halflife).

**Note**
We recommend that you do not use or modify the `location rssi-half-life` command.

**Step 4**
- **Command or Action:** `location expiry \{calibrating-client | client | rogue-aps | tags \} timeout`
- **Example:**
  ```
  Controller(config)# location expiry calibrating-client 50
  ```

**Purpose**
You can enter the RSSI timeout value for the clients, calibrating clients, RFID tags, and rogue access points from 5 through 3600 seconds, and the default value is 5 seconds.

For the calibrating clients, you can enter the RSSI timeout value from 0 through 3600 seconds, and the default value is 5 seconds.

Ensuring that recent, strong RSSIs are retained by the CPU is critical to location accuracy. The `location expiry` command enables you to specify the length of time after which old RSSI averages expire.

**Note**
We recommend that you do not use or modify the `location expiry` command.

**Step 5**
- **Command or Action:** `location algorithm \{rssi-average | simple\}`
- **Example:**
  ```
  Controller(config)# location algorithm rssi-average
  ```

**Purpose**
You can enter the `location algorithm rssi-average` command to specify a more accurate algorithm but requires more CPU overhead or the `location algorithm simple` command to specify a faster algorithm that requires low CPU overhead but provides less accuracy.

**Note**
We recommend that you do not use or modify the `location algorithm` command.

**Step 6**
- **Command or Action:** `location admin-tag string`
- **Example:**
  ```
  Controller(config)# location admin-tag
  ```

**Purpose**
Sets administrative tag or site information for the location of client devices.

**Step 7**
- **Command or Action:** `location civic-location identifier \{identifier | host\}`
- **Example:**
  ```
  Controller(config)# location civic-location identifier host
  ```

**Purpose**
Specifies civic location information.
You can set the civic location identifier either as a string or host.
## 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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong>&lt;br&gt;location custom-location identifier {identifier</td>
<td>host}</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Controller(config)# location custom-location identifier host</td>
<td>You can set the custom location identifier either as a string or host.</td>
</tr>
<tr>
<td><strong>Step 9</strong>&lt;br&gt;location geo-location identifier {identifier</td>
<td>host}</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Controller(config)# location geo-location identifier host</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong>&lt;br&gt;location prefer {cdp</td>
<td>lldp-med</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Controller(config)# location prefer weight cdp 50</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong>&lt;br&gt;location rfid {status</td>
<td>timeout</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Controller(config)# location rfid timeout 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong>&lt;br&gt;end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Controller(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> nmsp notification interval {attachment seconds</td>
<td>location seconds</td>
</tr>
<tr>
<td>Example: Controller(config)# nmsp notification interval rssi rfid 50</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td>Example: Controller(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

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

Example: Controller(config)# location notify-threshold rssi 50
DETAILED STEPS

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

| **Step 2** | Configures the NMSP notification threshold for clients, RFID tags, and rogue clients and access points. |
| location notify-threshold {clients | rogues ap | tags} threshold | You can enter the RSSI threshold value from zero through 10 db. |
| Example: Controller(config)# location notify-threshold clients 5 |         |

| **Step 3** | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
| end |         |
| Example: Controller(config)# end |         |

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 controller.

Table 20: Monitoring Location Settings Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show location summary</td>
<td>Displays the current location configuration values.</td>
</tr>
<tr>
<td>show location statistics rfid</td>
<td>Displays the location-based RFID statistics.</td>
</tr>
<tr>
<td>show location detail client_mac_addr</td>
<td>Displays the RSSI table for a particular client.</td>
</tr>
</tbody>
</table>

Monitoring NMSP Settings (CLI)

This section describes the new commands for NMSP settings.
The following commands can be used to monitor NMSP settings on the controller.
Table 21: Monitoring NMSP Settings Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show nmsp attachment suppress interfaces</td>
<td>Displays the attachment suppress interfaces.</td>
</tr>
<tr>
<td>show nmsp capability</td>
<td>Displays the NMSP capabilities.</td>
</tr>
<tr>
<td>show nmsp notification interval</td>
<td>Displays the NMSP notification intervals.</td>
</tr>
<tr>
<td>show nmsp statistics connection</td>
<td>Displays the connection-specific NMSP counters.</td>
</tr>
<tr>
<td>show nmsp statistics summary</td>
<td>Displays the common NMSP counters.</td>
</tr>
<tr>
<td>show nmsp status</td>
<td>Displays the status of active NMSP connections.</td>
</tr>
<tr>
<td>show nmsp subscription detail</td>
<td>Displays all of the mobility services to which the controller is subscribed.</td>
</tr>
<tr>
<td>show nmsp subscription detail ip_addr</td>
<td>Displays details only for the mobility services subscribed to by a specific IP address.</td>
</tr>
<tr>
<td>show nmsp subscription summary</td>
<td>Displays details for all of the mobility services to which the controller is subscribed.</td>
</tr>
</tbody>
</table>

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:

```
Controller# configure terminal
Controller(config)# location plm calibrating uniband
Controller(config)# end
Controller# show location summary
```

This example shows how to configure the RSSI half life for a rouge access point:

```
Controller# configure terminal
Controller(config)# location rssi-half-life rogue-aps 20
Controller(config)# end
Controller# show location summary
```

Examples: NMSP Settings Configuration

This example shows how to configure the NMSP notification interval for RFID tags:

```
Controller# configure terminal
Controller(config)# nmsp notification interval rssi rfid 50
```
Controller(config)# end
Controller# show nmsp notification interval

This example shows how to configure the NMSP notification threshold for clients:

Controller# configure terminal
Controller(config)# nmsp notify-threshold 5
Controller(config)# end
Controller# show nmsp statistics summary

Additional References for Location Settings

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Location Settings Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Monitoring Flow Control

- Finding Feature Information, page 195
- Information About Flow Control, page 195
- Monitoring Flow Control, page 195
- Examples: Monitoring Flow Control, page 196
- Additional References for Monitoring Flow Control, page 197
- Feature History and Information For Monitoring Flow Control, page 198

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 controller.

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 controller.
Table 22: Monitoring Flow Control

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless flow-control channel-id</td>
<td>Displays information about flow control on a particular channel.</td>
</tr>
<tr>
<td>show wireless flow-control channel-id statistics</td>
<td>Displays statistical information about flow control on a particular channel.</td>
</tr>
</tbody>
</table>

Examples: Monitoring Flow Control

This example shows how to view information pertaining to any channel:

Controller# show wireless flow-control 3
Controller#

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:

Controller# show wireless flow-control 3
Controller#

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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

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

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
## Feature History and Information For Monitoring Flow Control

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 15

Configuring System Message Logs

- Information About Configuring System Message Logs, page 199
- How to Configure System Message Logs, page 202
- Monitoring and Maintaining System Message Logs, page 211
- Configuration Examples for System Message Logs, page 211
- Feature History and Information For System Message Logs, page 212

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

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

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

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer on a standalone switch, and in the case of a switch stack, on the . If a standalone switch or the stack master fails, the log is lost unless you had saved it to flash memory.
You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet, through the console port, or through the Ethernet management port. In a switch stack, all stack member consoles provide the same console output.

Note

The syslog format is compatible with 4.3 BSD UNIX.

### System Log Message Format

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

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

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

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

#### Table 23: System Log Message Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seq no:</code></td>
<td>Stamps log messages with a sequence number only if the <code>service sequence-numbers</code> global configuration command is configured.</td>
</tr>
<tr>
<td><code>timestamp formats:</code></td>
<td>Date and time of the message or event. This information appears only if the `service timestamps log [datetime</td>
</tr>
<tr>
<td><code>mm/dd h:mm:ss</code></td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><code>hh:mm:ss</code> (short uptime)</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><code>d h</code> (long uptime)</td>
<td></td>
</tr>
<tr>
<td><code>facility</code></td>
<td>The facility to which the message refers (for example, SNMP, SYS, and so forth).</td>
</tr>
<tr>
<td><code>severity</code></td>
<td>Single-digit code from 0 to 7 that is the severity of the message.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MNEMONIC</td>
<td>Text string that uniquely describes the message.</td>
</tr>
<tr>
<td>description</td>
<td>Text string containing detailed information about the event being reported.</td>
</tr>
<tr>
<td>hostname-n</td>
<td>Hostname of a stack member and its switch number in the stack. Though the is a stack member, it does not append its hostname to system messages.</td>
</tr>
</tbody>
</table>

### Default System Message Logging Settings

**Table 24: Default System Message Logging Settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>System message logging to the console</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Console severity</td>
<td>Debugging.</td>
</tr>
<tr>
<td>Logging file configuration</td>
<td>No filename specified.</td>
</tr>
<tr>
<td>Logging buffer size</td>
<td>4096 bytes.</td>
</tr>
<tr>
<td>Logging history size</td>
<td>1 message.</td>
</tr>
<tr>
<td>Time stamps</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Synchronous logging</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Logging server</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Syslog server IP address</td>
<td>None configured.</td>
</tr>
<tr>
<td>Server facility</td>
<td>Local7</td>
</tr>
<tr>
<td>Server severity</td>
<td>Informational.</td>
</tr>
</tbody>
</table>

### Syslog Message Limits

If you enabled syslog message traps to be sent to an SNMP network management station by using the `snmp-server enable trap` global configuration command, you can change the level of messages sent and stored in the switch history table. You also can change the number of messages that are stored in the history table.
Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels are stored in the history table even if syslog traps are not enabled.

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

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

## How to Configure System Message Logs

### Setting the Message Display Destination Device

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

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| **configure terminal** | Enters global configuration mode. |
| **Example:**
| Controller# `configure terminal` | |
| **Step 2**
| `logging buffered [size]` | Logs messages to an internal buffer on the switch or on a standalone switch or, in the case of a switch stack, on the . The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes.
If a standalone switch or the fails, the log file is lost unless you previously saved it to flash memory. See Step 4.
| **Note** Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the `show memory` privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should not be set to this amount. | |
| **Example:**
| Controller(config)# `logging buffered 8192` | |
### Configuring System Message Logs

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** | Logs messages to a UNIX syslog server host.  
*host* 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. |
| `logging host` |  |
| **Example:** |  |
| `Controller(config)# logging host 125.1.1.100` |  |
| **Step 4** | Stores log messages in a file in flash memory on a standalone switch or, in the case of a switch stack, on the .  
- *filename*—Enters the log message filename.  
- *(Optional)* **max-file-size** —Specifies the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes.  
- *(Optional)* **min-file-size**—Specifies the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes.  
- *(Optional)* **severity-level-number** |  |
| `logging file flash: filename` |  |
| *max-file-size [min-file-size]] [severity-level-number | type] |  |
| **Example:** |  |
| `Controller(config)# logging file flash:log_msg.txt 40960 4096 3` |  |
| **Step 5** | Returns to privileged EXEC mode. |
| `end` |  |
| **Example:** |  |
| `Controller(config)# end` |  |
| **Step 6** | Logs messages to a non-console terminal during the current session.  
Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages. |
| `terminal monitor` |  |
| **Example:** |  |
| `Controller# terminal monitor` |  |

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| `configure terminal` | Enters global configuration mode. |
| **Example:** |
| `Controller# configure terminal` |

| **Step 2**
| `line [console | vty] line-number [ending-line-number]` | Specifies the line to be configured for synchronous logging of messages. |
| **Example:** |
| `Controller(config)# line console` | • `console` — Specifies configurations that occur through the switch console port or the Ethernet management port. |
| | • `line vty line-number` — Specifies which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet session. The range of line numbers is from 0 to 15. |
| | You can change the setting of all 16 vty lines at once by entering: |
| | `line vty 0 15` |
| | 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: |
| | `line vty 2` |
| | When you enter this command, the mode changes to line configuration. |

| **Step 3**
| **Example:** |
| `Controller(config)# logging synchronous level 3 limit 1000` | • (Optional) `level severity-level` — Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers mean greater severity and high numbers mean lesser severity. The default is 2. |
| | • (Optional) `level all` — Specifies that all messages are printed asynchronously regardless of the severity level. |
| | • (Optional) `limit number-of-buffers` — 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. |
Disabling Message Logging

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

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

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

To reenable message logging after it has been disabled, use the `logging on` global configuration command. This task is optional.

**SUMMARY STEPS**

1. configure terminal
2. no logging console
3. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>no logging console</td>
<td>Disables message logging.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# no logging console</td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables log time stamps.</td>
</tr>
<tr>
<td>Use one of these commands:</td>
<td><code>log uptime</code>—Enables time stamps on log messages, showing the time since the system was rebooted.</td>
</tr>
<tr>
<td>- <code>service timestamps log uptime</code></td>
<td><code>log datetime</code>—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.</td>
</tr>
<tr>
<td>- `service timestamps log datetime[msec</td>
<td>localtime</td>
</tr>
</tbody>
</table>

Example:

Controller(config)# end

Returns to privileged EXEC mode.
Enabling and Disabling Sequence Numbers in Log Messages

If there is more than one log message with the same timestamp, 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> service sequence-numbers</td>
<td>Enables sequence numbers.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# service sequence-numbers</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>entry global configuration mode</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>limits messages logged to the console.</td>
</tr>
<tr>
<td>logging console level</td>
<td>By default, the console receives debugging messages and numerically lower levels.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# logging console 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>limits messages logged to the terminal lines.</td>
</tr>
<tr>
<td>logging monitor level</td>
<td>By default, the terminal receives debugging messages and numerically lower levels.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# logging monitor 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>limits messages logged to the syslog servers.</td>
</tr>
<tr>
<td>logging trap level</td>
<td>By default, syslog servers receive informational messages and numerically lower levels.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Controller(config)# logging trap 3</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Controller# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>logging history level</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Controller(config)# logging history 3</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>logging history size number</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Controller(config)# logging history size 200</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Add a line to the file <code>/etc/syslog.conf</code></td>
<td>• local7—Specifies the logging facility.</td>
</tr>
<tr>
<td>Example:</td>
<td>• debug—Specifies the syslog level. The file must already exist, and the syslog daemon must have permission to write to it.</td>
</tr>
<tr>
<td><code>local7.debug /usr/adm/logs/cisco.log</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Enter these commands at the UNIX shell prompt.</td>
<td>Creates the log file. The syslog daemon sends messages at this level or at a more severe level to this file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>touch /var/log/cisco.log</code></td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring and Maintaining System Message Logs

#### Monitoring Configuration Archive Logs

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show archive log config {all</td>
<td>number [end-number]</td>
</tr>
</tbody>
</table>

#### Configuration Examples for System Message Logs

**Example: Stacking System Message**

This example shows a partial switch system message for and a stack member (hostname Switch-2):

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, 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)
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, 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 up (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-channel1, 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
*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)

Feature History and Information For System Message Logs

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Online Diagnostics

- Information About Configuring Online Diagnostics, page 213
- How to Configure Online Diagnostics, page 214
- Monitoring and Maintaining Online Diagnostics, page 218
- Configuration Examples for Online Diagnostic Tests, page 219
- Additional References for Online Diagnostics, page 221
- Feature History and Information for Configuring Online Diagnostics, page 222

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Starts the diagnostic tests.</td>
</tr>
<tr>
<td>`diagnostic start switch number test {name</td>
<td>test-id</td>
</tr>
<tr>
<td>Example: Controller# diagnostic start switch 2 test basic</td>
<td>• <code>name</code>—Enters the name of the test.</td>
</tr>
<tr>
<td></td>
<td>• <code>test-id</code>—Enters the ID number of the test.</td>
</tr>
<tr>
<td></td>
<td>• <code>test-id-range</code>—Enters the range of test IDs by using integers separated by a comma and a hyphen.</td>
</tr>
<tr>
<td></td>
<td>• <code>all</code>—Starts all of the tests.</td>
</tr>
<tr>
<td></td>
<td>• <code>basic</code>—Starts the basic test suite.</td>
</tr>
<tr>
<td></td>
<td>• <code>complete</code>—Starts the complete test suite.</td>
</tr>
<tr>
<td></td>
<td>• <code>minimal</code>—Starts the minimal bootup test suite.</td>
</tr>
<tr>
<td></td>
<td>• <code>non-disruptive</code>—Starts the non-disruptive test suite.</td>
</tr>
<tr>
<td></td>
<td>• <code>per-port</code>—Starts the per-port test suite.</td>
</tr>
</tbody>
</table>

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

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

**Example:**

Controller# configure terminal

**Step 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}

**Example:**

Controller(config)# diagnostic schedule switch 3 test 1-5 on July 3 2013 23:10

Schedules on-demand diagnostic tests for a specific day and time.

The switch number keyword is supported only on stacking switches. The range is from 1 to 4.

When specifying the tests to be scheduled, use these options:

- **name**—Name of the test that appears in the show diagnostic content command output.
- **test-id**—ID number of the test that appears in the show diagnostic content command output.
- **test-id-range**—ID numbers of the tests that appear in the show diagnostic content command output.
- **all**—All test IDs.
- **basic**—Starts the basic on-demand diagnostic tests.
- **complete**—Starts the complete test suite.
- **minimal**—Starts the minimal bootup test suite.
- **non-disruptive**—Starts the non-disruptive test suite.
- **per-port**—Starts the per-port test suite.

You can schedule the tests as follows:

- Daily—Use the daily *hh:mm* parameter.
- Specific day and time—Use the on *mm dd yyyy hh:mm* parameter.
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.

### SUMMARY STEPS

1. configure terminal
2. diagnostic monitor interval switch number test {name | test-id | test-id-range | all} hh:mm:ss milliseconds day
3. diagnostic monitor syslog
4. diagnostic monitor threshold switch number test {name | test-id | test-id-range | all} failure count count
5. diagnostic monitor switch number test {name | test-id | test-id-range | all}
6. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> diagnostic monitor interval switch number test {name</td>
<td>test-id</td>
</tr>
<tr>
<td><strong>Example:</strong> Controller(config)# diagnostic monitor interval switch 2 test 1 12:30:00 750 5</td>
<td>• name—Name of the test that appears in the show diagnostic content command output.</td>
</tr>
<tr>
<td></td>
<td>• test-id—ID number of the test that appears in the show diagnostic content command output.</td>
</tr>
<tr>
<td></td>
<td>• test-id-range—ID numbers of the tests that appear in the show diagnostic content command output.</td>
</tr>
<tr>
<td></td>
<td>• all—All of the diagnostic tests.</td>
</tr>
</tbody>
</table>
When specifying the interval, set these parameters:

- **hh:mm:ss**—Monitoring interval in hours, minutes, and seconds. The range for hh is 0 to 24, and the range for mm and ss is 0 to 60.
- **milliseconds**—Monitoring interval in milliseconds (ms). The range is from 0 to 999.
- **day**—Monitoring interval in the number of days. The range is from 0 to 20.

### Step 3: Diagnostic Monitor Syslog

**Example:**

```
Controller(config)# diagnostic monitor syslog
```

(Optional) Configures the switch to generate a syslog message when a health-monitoring test fails.

### Step 4: Diagnostic Monitor Threshold Switch

**Example:**

```
Controller(config)# diagnostic monitor threshold switch number test {name | test-id | test-id-range | all} failure count count
```

(Optional) Sets the failure threshold for the health-monitoring tests.

When specifying the tests, use one of these parameters:

- **name**—Name of the test that appears in the `show diagnostic content` command output.
- **test-id**—ID number of the test that appears in the `show diagnostic content` command output.
- **test-id-range**—ID numbers of the tests that appear in the `show diagnostic content` command output.
- **all**—All of the diagnostic tests.

The range for the failure threshold `count` is 0 to 99.

### Step 5: Diagnostic Monitor Switch

**Example:**

```
Controller(config)# diagnostic monitor switch number test {name | test-id | test-id-range | all}
```

Enables the specified health-monitoring tests.

The `switch number` keyword is supported only on stacking switches. The range is from 1 to 9.

When specifying the tests, use one of these parameters:

- **name**—Name of the test that appears in the `show diagnostic content` command output.
- **test-id**—ID number of the test that appears in the `show diagnostic content` command output.
- **test-id-range**—ID numbers of the tests that appear in the `show diagnostic content` command output.
- **all**—All of the diagnostic tests.
**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 25: Commands for Diagnostic Test Configuration and Results

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show diagnostic content switch [number</td>
<td>all]`</td>
</tr>
<tr>
<td></td>
<td>The `switch [number</td>
</tr>
<tr>
<td><code>show diagnostic status</code></td>
<td>Displays the currently running diagnostic tests.</td>
</tr>
<tr>
<td>`show diagnostic result switch [number</td>
<td>all] [detail</td>
</tr>
<tr>
<td></td>
<td>The `switch [number</td>
</tr>
<tr>
<td>`show diagnostic switch [number</td>
<td>all] [detail]`</td>
</tr>
<tr>
<td></td>
<td>The `switch [number</td>
</tr>
<tr>
<td>`show diagnostic schedule switch [number</td>
<td>all]`</td>
</tr>
<tr>
<td></td>
<td>The `switch [number</td>
</tr>
</tbody>
</table>
### Configuration Examples for Online Diagnostic Tests

#### Examples: Start Diagnostic Tests

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

```plaintext
Controller# diagnostic start switch 2 test TestInlinePwrCtlr
```

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

```plaintext
Controller# diagnostic start switch 1 test all
```

#### Example: Configure a Health Monitoring Test

This example shows how to configure a health-monitoring test:

```plaintext
Controller(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
Controller(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:

```plaintext
Controller(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:

```plaintext
Controller(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:

```plaintext
Controller# show diagnostic ondemand settings
Test iterations = 1
```
Action on test failure = continue

This example shows how to display diagnostic events for errors:

Controller# **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:

Controller# **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.

Controller#

This example shows how to display the boot up level:

Controller# **show diagnostic bootup level**

Current bootup diagnostic level: minimal

Controller#
Additional References for Online Diagnostics

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management commands</td>
<td>System Management Command Reference (Cisco WLC 5700 Series)</td>
</tr>
<tr>
<td>Platform-independent command reference</td>
<td>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
<tr>
<td>Platform-independent configuration information</td>
<td>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information for Configuring Online Diagnostics

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Predownloading an Image to Access Points

- Finding Feature Information, page 223
- Predownloading an Image to an Access Point, page 223
- Restrictions for Predownloading an Image to an Access Point, page 224
- How to Predownload an Image to an Access Point, page 224
- Monitoring Access Point Predownload Process, page 225
- Examples: Access Point Predownload Process, page 226
- Additional References for Predownloading an Image to an Access Point, page 226
- Feature History and Information For Performing Predownloading an Image to an Access Point, page 227

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.

Predownloading an Image to an Access Point

To minimize network outages, you can now download an upgrade image to the access point from the controller without resetting the access point or losing network connectivity. Previously, you would download an upgrade image to the controller and reset it, which causes the access point to go into discovery mode. After the access point discovers the controller with the new image, the access point downloads the new image, resets, goes into discovery mode, and rejoins the controller.

You can now download the upgrade image to the controller and then download the image to the access point while the network is still up. When both devices are up, the access point discovers and rejoins the controller.
Restrictions for Predownloading an Image to an Access Point

The following are the restrictions for predownloading an image to an access point:

- The maximum number of concurrent predownloads is limited to half the number of concurrent normal image downloads. This limitation allows new access points to join the controller during image downloading.

  If you reach the predownload limit, then the access points that cannot get an image sleep for a time between 180 to 600 seconds and then reattempt the predownload.

- Access points with 16-MB total available memory may not have enough free memory to download an upgrade image and may automatically delete crash info files, radio files, and any backup images to free up space. However, this limitation does not affect the predownload process because the predownload image replaces any backup image on the access point.

- All of the primary, secondary, and tertiary controllers should run the same images or the feature will not be effective.

- At the time of reset, you must make sure that all of the access points have downloaded the image.

- The access point can store only two software images.

How to Predownload an Image to an Access Point

Predownloading an Image to Access Points (CLI)

Before You Begin

There are some prerequisites that you must keep in mind while predownloading an image to an access point:

- Predownloading can be done only when the controller is booted in the install mode.
- You can copy the new image either from the TFTP server, flash image, or USB.
- Before predownloading the new image, you must install the new software using the `software install` command and select `no` to the `reload` option.

SUMMARY STEPS

1. `ap image predownload` or `ap ap-name predownload`
2. `show ap image`
3. `ap image swap`
4. `ap image reset`
5. `reload`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ap image predownload</code> or <code>ap ap-name predownload</code></td>
<td>Downloads the new image to all access points or a specific access point connected to the controller.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# <code>ap image predownload</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller# <code>ap ap1 predownload</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show ap image</code></td>
<td>Verifies the access points predownload process.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# <code>show ap image</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ap image swap</code></td>
<td>Specifies to swap the backup image to the primary image.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# <code>ap image swap</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ap image reset</code></td>
<td>Resets the access points.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# <code>ap image reset</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>reload</code></td>
<td>Resets the system.</td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# <code>reload</code></td>
<td></td>
</tr>
</tbody>
</table>

Monitoring Access Point Predownload Process

This section describes the command for monitoring the access point predownload process.

The following command can be used to monitor the access point predownload process.

Table 26: Monitoring Access Point Predownload Process Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ap image</code></td>
<td>Verifies the access points predownload process.</td>
</tr>
</tbody>
</table>

Displaying Access Point Predownload Status

While downloading the access point predownload image, you can simultaneously enter the `show ap image` command to verify the predownload progress on the access points:

```
Controller# `show ap image`
Total number of APs : 1
Number of APs
```
Examples: Access Point Predownload Process

This example shows how to predownload an image to an access point AP1:

```
Controller# ap image predownload
Controller# show ap image
Controller# ap image swap
Controller# show ap image
Controller# ap image reset
Controller# reload
```

Additional References for Predownloading an Image to an Access Point

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lightweight access points configuration</td>
<td></td>
</tr>
<tr>
<td>Lightweight Access Point commands</td>
<td></td>
</tr>
</tbody>
</table>
## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>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></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

## Feature History and Information For Performing Predownloading an Image to an Access Point

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Troubleshooting the Software Configuration

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the switch. Depending on the nature of the problem, you can use the command-line interface (CLI), Device Manager, or Network Assistant to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

- Information About Troubleshooting the Software Configuration, page 229
- How to Troubleshoot the Software Configuration, page 237
- Verifying Troubleshooting of the Software Configuration, page 248
- Scenarios for Troubleshooting the Software Configuration, page 250
- Configuration Examples for Troubleshooting Software, page 253
- Feature History and Information for Troubleshooting Software Configuration, page 255

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 237
Lost or Forgotten Password on a Controller

The default configuration for the controller allows an end user with physical access to the controller 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 controller.

Note

On these controllers, 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.

Related Topics

Recovering from a Lost or Forgotten Password, on page 238

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 Configuration Guide (Cisco WLC 5700 Series).

Related Topics

Scenarios to Troubleshoot Power over Ethernet (PoE), on page 250

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 244
- Example: Pinging an IP Host, on page 253

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 switches 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 switches 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 switches 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 switches 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 switches 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 246
- Example: Performing a Traceroute to an IP Host, on page 253

**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 only on 10/100/1000 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and 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.

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 246
- Example: Enabling All System Diagnostics, on page 254

### 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:

```
Controller# dir crashinfo?
crashinfo-1: crashinfo-2: crashinfo-3: crashinfo:
Controller#
```

For example, to access the crashinfo directory for switch 1, enter

```
Controller dir crashinfo-1
```

From the ROMMON prompt, you can view the crashinfo files by using the `dir` command:

```
Controller: dir sdal
```
The following is sample output of a crashinfo file

Controller# 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)

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.

Controller#

System Reports

When a controller 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 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 stack member.

• Power over Ethernet (PoE)—Record of the power consumption of PoE ports on a standalone switch or a stack member.

• Temperature—Temperature of a standalone switch or a stack member.

• Uptime data—Time when a standalone switch or a 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 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 247
- Displaying OBFL Information, on page 248

## 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:

- Spanning tree topology changes
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_ADDR ip_address subnet_mask

   Example:
   
   
   
   
   switch: set IP_ADDR 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.
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: dir sda9:
Directory of sda9:/
  2 drwx 1024 .
  2 drwx 1024 ..
  11 -rw- 18923068 c3850-recovery.bin
```

36939776 bytes available (20830208 bytes used)

**Related Topics**

- Software Failure on a Switch, on page 229

---

**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 . Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until all the system LEDs turn on and remain solid; then release the **Mode** button.
5. After recovering the password, reload the switch or the .
6. Power on the remaining switches in the stack.
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. If you are recovering the password for a switch stack, connect to the console port of the or
- Connect a PC to the Ethernet management port. If you are recovering the password for a switch stack, connect to the Ethernet management port of a stack member.

Step 2 Set the linespeed 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 . Within 15 seconds, press the Mode button while the System LED is still flashing green. Continue pressing the Mode button until all the system LEDs turn on and remain solid; 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 .
On a switch:
Switch> reload
Proceed with reload? [confirm] y

On the active switch:
Switch> reload slot <stack-active-member-number>
Proceed with reload? [confirm] y

Step 6 Power on the remaining switches in the stack.

Related Topics
Lost or Forgotten Password on a Controller, on page 230
**Procedure with Password Recovery Enabled**

If the password-recovery operation is enabled, this message appears:

### Step 1
Ignore the startup configuration with the following command:

Controller: `SWITCH_IGNORE_STARTUP_CFG=1`

### Step 2
Boot the switch with the `packages.conf` file from flash.

Controller: `boot flash:packages.conf`

### Step 3
Terminate the initial configuration dialog by answering **No**.

Would you like to enter the initial configuration dialog? [yes/no]: **No**

### Step 4
At the switch prompt, enter privileged EXEC mode.

Controller>` enable
Switch#`

### Step 5
Copy the startup configuration to running configuration.

Controller>` copy startup-config running-config Destination filename [running-config]?

Press Return in response to the confirmation prompts. The configuration file is now reloaded, and you can change the password.

### Step 6
Enter global configuration mode and change the **enable** password.

Controller>` configure terminal
Controller(config)#`

### Step 7
Write the running configuration to the startup configuration file.

Controller>` copy running-config startup-config`

### Step 8
Confirm that manual boot mode is enabled.

Controller>` show boot

```plaintext
BOOT variable = flash:packages.conf;
Manual Boot = yes
Enable Break = yes
```
Step 9  Reload the controller.

Controller# reload

Step 10  Return the Bootloader parameters (previously changed in Steps 2 and 3) to their original values.

Controller: switch: SWITCH_IGNORE_STARTUP_CFG=0

Step 11  Boot the controller with the packages.conf file from flash.

Controller: boot flash:packages.conf

Step 12  After the controller boots up, disable manual boot on the controller.

Controller(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:

Controller: `dir flash:

The switch file system appears.

### Step 3
Boot up the system:

Controller: `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:

Controller> `enable

### Step 5
Enter global configuration mode:

Controller# `configure terminal

### Step 6
Change the password:

Controller(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:

Controller(config)# `exit

Controller#

**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:

Controller# `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 switches 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 CLI. 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 switches in the stack can make it easier to remotely troubleshoot the switch stack. However, you need to remember that the switches have manually assigned numbers if you add, remove, or rearrange switches 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 switches.

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.

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.

---

**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 switches.
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping ip host \ address</td>
<td>Pings a remote host through IP or by supplying the hostname or network address.</td>
</tr>
</tbody>
</table>

Controller# ping 172.20.52.3

Related Topics
- Ping, on page 231
- Example: Pinging an IP Host, on page 253

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.

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 27: Monitoring the Physical Path

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>tracetroute mac \ [interface interface-id]</td>
<td>Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.</td>
</tr>
<tr>
<td>\ {source-mac-address} \ [interface interface-id]</td>
<td></td>
</tr>
<tr>
<td>\ {destination-mac-address} \ [vlan vlan-id] \ [detail]</td>
<td></td>
</tr>
<tr>
<td>tracetroute mac ip \ {source-ip-address</td>
<td>source-hostname} \ {destination-ip-address</td>
</tr>
</tbody>
</table>
Executing IP Traceroute

Note

Though other protocol keywords are available with the traceroute privileged EXEC command, they are not supported in this release.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute ip host</td>
<td>Traces the path that packets take through the network.</td>
</tr>
<tr>
<td>Controller# traceroute ip 192.51.100.1</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- IP Traceroute, on page 232
- Example: Performing a Traceroute to an IP Host, on page 253

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.

Related Topics

- Debug Commands, on page 234
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.

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 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.

Related Topics

Onboard Failure Logging on the Switch, on page 235
Displaying OBFL Information, on page 248
Verifying Troubleshooting of the Software Configuration

Displaying OBFL Information

Table 28: Commands for Displaying OBFL Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show onboard switch switch-number clilog</code></td>
<td>Displays the OBFL CLI commands that were entered on a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Controller# show onboard switch 1 clilog</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number environment</code></td>
<td>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.</td>
</tr>
<tr>
<td>Controller# show onboard switch 1 environment</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number message</code></td>
<td>Displays the hardware-related messages generated by a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Controller# show onboard switch 1 message</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number counter</code></td>
<td>Displays the counter information on a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Controller# show onboard switch 1 counter</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number temperature</code></td>
<td>Displays the temperature of a standalone switch or the specified switch stack members.</td>
</tr>
<tr>
<td>Controller# show onboard switch 1 temperature</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number uptime</code></td>
<td>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.</td>
</tr>
<tr>
<td>Controller# show onboard switch 1 uptime</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number voltage</code></td>
<td>Displays the system voltages of a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Controller# show onboard switch 1 voltage</td>
<td></td>
</tr>
<tr>
<td><code>show onboard switch switch-number status</code></td>
<td>Displays the status of a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td>Controller# show onboard switch 1 status</td>
<td></td>
</tr>
</tbody>
</table>
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.

```
Controller# 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 29: Troubleshooting CPU Utilization Problems

<table>
<thead>
<tr>
<th>Type of Problem</th>
<th>Cause</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interrupt percentage value is almost as high as total CPU utilization value.</td>
<td>The CPU is receiving too many packets from the network.</td>
<td>Determine the source of the network packet. Stop the flow, or change the switch configuration. See the section on “Analyzing Network Traffic.”</td>
</tr>
<tr>
<td>Total CPU utilization is greater than 50% with minimal time spent on interrupts.</td>
<td>One or more Cisco IOS process is consuming too much CPU time. This is usually triggered by an event that activated the process.</td>
<td>Identify the unusual event, and troubleshoot the root cause. See the section on “Debugging Active Processes.”</td>
</tr>
</tbody>
</table>
Scenarios for Troubleshooting the Software Configuration

Scenarios to Troubleshoot Power over Ethernet (PoE)

Table 30: Power over Ethernet Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Symptom or Problem</th>
<th>Possible Cause and Solution</th>
</tr>
</thead>
</table>
| Only one port does not have PoE. Trouble is on only one switch port. PoE and non-PoE devices do not work on this port, but do on other ports. | Verify that the powered device works on another PoE port. Use the `show run`, or `show interface status` user EXEC commands to verify that the port is not shut down or error-disabled.  
  **Note** Most switches turn off port power when the port is shut down, even though the IEEE specifications make this optional.  
  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.  
  Verify that the total cable length from the switch front panel to the powered device is not more than 100 meters.  
  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.  
  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 `show inline power` command to verify the amount of available power. |
<table>
<thead>
<tr>
<th>Symptom or Problem</th>
<th>Possible Cause and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No PoE on all ports or a group of ports. Trouble is on all switch ports. Nonpowered Ethernet devices cannot establish an Ethernet link on any port, and PoE devices do not power on.</td>
<td>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. 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. Use the <strong>show log</strong> privileged EXEC command to review alarms or system messages that previously reported PoE conditions or status changes. If there are no alarms, use the <strong>show interface status</strong> command to verify that the ports are not shut down or error-disabled. If ports are error-disabled, use the <strong>shut</strong> and <strong>no shut</strong> interface configuration commands to reenable the ports. Use the <strong>show env power</strong> and <strong>show power inline</strong> privileged EXEC commands to review the PoE status and power budget (available PoE). Review the running configuration to verify that <strong>power inline never</strong> is not configured on the ports. 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 <strong>shut</strong> and <strong>no shut</strong> 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. 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. Use the <strong>show power inline</strong> 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. If a powered device can power on when only one powered device is connected to the switch, enter the <strong>shut</strong> and <strong>no shut</strong> interface configuration commands on the remaining ports, and then reconnect the Ethernet cables one at a time to the switch PoE ports. Use the <strong>show interface status</strong> and <strong>show power inline</strong> privileged EXEC commands to monitor inline power statistics and port status. 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.</td>
</tr>
<tr>
<td>Symptom or Problem</td>
<td>Possible Cause and Solution</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Cisco IP Phone disconnects or resets. After working normally, a Cisco phone or wireless access point intermittently reloads or disconnects from PoE.</td>
<td>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. Verify that the cable length is not more than 100 meters from the switch port to the powered device. Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs. Notice whether any error messages appear at the same time a disconnect occurs. Use the <code>show log</code> privileged EXEC command to review error messages. 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.) 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.</td>
</tr>
<tr>
<td>Non-Cisco powered device does not work on Cisco PoE switch. 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.</td>
<td>Use the <code>show power inline</code> 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. Use the <code>show interface status</code> command to verify that the switch detects the connected powered device. Use the <code>show log</code> 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 <code>inrush</code>) current that exceeds a current-limit threshold for the port.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Power over Ethernet Ports](#) on page 230
Configuration Examples for Troubleshooting Software

Example: Pinging an IP Host

This example shows how to ping an IP host:

Controller# 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
Controller#

Table 31: Ping Output Display Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point means receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period means the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error PDU was received.</td>
</tr>
<tr>
<td>C</td>
<td>A congestion experienced packet was received.</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime exceeded.</td>
</tr>
</tbody>
</table>

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 231
Executing Ping, on page 244

Example: Performing a Traceroute to an IP Host

This example shows how to perform a traceroute to an IP host:

Controller# traceroute ip 192.0.2.10
Type escape sequence to abort.
Tracing the route to 192.0.2.10
192.0.2.1 0 msec 0 msec 4 msec
192.0.2.203 12 msec 8 msec 0 msec
192.0.2.100 4 msec 0 msec 0 msec
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 32: Traceroute Output Display Characters**

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output means that an access list is blocking traffic.</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench.</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable.</td>
</tr>
</tbody>
</table>

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 232](#)
- [Executing IP Traceroute, on page 246](#)

**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:

```
Controller# 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 234

### Feature History and Information for Troubleshooting Software Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
INDEX

11n Mode parameter 93
802.11a (or 802.11b/g) Global Parameters page 89
802.11a (or 802.11b/g) Network Status parameter 89, 95
802.11g Support parameter 89
802.11h Global Parameters page 95
802.11h, described 85
802.11n 84
devices 84

banners (continued)
default configuration 25
Beacon Period parameter 89
broadcast traffic 231

C
CCX Layer 2 client roaming 113
described 113
Channel Announcement parameter 95
clock 21
See system clock 21
corrupted software, recovery steps with Xmodem 237
crashinfo file 234
crashinfo, description 234

D
Data Rates parameter 89
daylight saving time 29
debugging 234, 246, 254
enabling all system diagnostics 254
redirecting error message output 246
using commands 234
default configuration 25, 26
banners 25
DNS 25
MAC address table 26
described 213, 231, 235
directed roam request 114
displaying 248
displaying crash information 234
DNS 25, 31
default configuration 25
overview 25
setting up 31
Domain Name System 25
See DNS 25

A
access points 113
assisted roaming 113
address resolution 27
addresses 26, 27, 40
dynamic 26
defined 26
learning 26
MAC, discovering 27
static 40
adding and removing 40
aging time 34
MAC address table 34
and ARP 231
and CDP 231
ARP 27
defined 27
table 27
address resolution 27
authoritative time source, described 22
autonegotiation 243
mismatches 243

B
banners 25, 32, 33
configuring 32, 33
login 33
message-of-the-day login 32

System Management Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)
domain names 25
  DNS 25
DTPC Support parameter 89
dynamic transmit power control, configuring 89

E
EDCA Profile parameter 174
enable 247
Enable Low Latency MAC parameter 174
enabling all system diagnostics 254
enhanced neighbor list 114
  request (E2E) 114
described 114
Example for Performing a Traceroute to an IP Host command 253
Example for Pinging an IP Host command 253
executing 244, 246
extended crashinfo file 234

F
files 234
  crashinfo, description 234
flash memory 235
Fragmentation Threshold parameter 89

I
ICMP 232
  time-exceeded messages 232
  traceroute and 232
ICMP ping 231, 244
oxecuting 244
overview 231
inter-subnet roaming 113
described 113
IP addresses 27
discovering 27
IP addresses and subnets 231
IP traceroute 232, 246
oxecuting 246
overview 232

L
Layer 2 traceroute (continued)
described 231
IP addresses and subnets 231
MAC addresses and VLANs 231
multicast traffic 231
multiple devices on a port 231
unicast traffic 231
usage guidelines 231
login banners 25

M
MAC addresses 26, 27, 34, 40
  aging time 34
  and VLAN association 26
  building the address table 26
default configuration 26
discovering 27
dynamic 26
  learning 26
static 40
  characteristics of 40
MAC addresses and VLANs 231
MCS data rates 93
messages, to users through banners 25
mismatches 243
mismatches, autonegotiation 243
monitoring 244
  SFP status 244
monitoring status of 244
multicast traffic 231
multiple devices on a port 231

N
Network Mobility Services Protocol (NMSP) 188
  modifying the notification interval for clients, RFID tags, and rogues 188
NTP 22, 24
  associations 24
defined 24
overview 22
time 24
  services 24

O
OBFL 235, 247, 248
  configuring 247
described 235
OBFL (continued)
displaying 248
on-board failure logging 235
online diagnostics 213
 des cribed 213
 overview 213
 overview 213, 231, 232

P
partitioned 243
passwords 230
 recovery of 230
ping 231, 244, 253
 character output description 253
 executing 244
 overview 231
PoE ports 230
 Policy Map 144

Q
QoS 139
 marked-down actions 139
 policers 139
 configuring 139

R
recovery of 230
recovery procedures 237
 redirecting error message output 246
RFC 22
 1305, NTP 22
 roam reason report 114

S
security and identification 244
See also downloading and uploading[software images 237
See also IP traceroute 232
 setting packet forwarding 247
SFP security and identification 244
SFP status 244
SFPs 244
 monitoring status of 244
 security and identification 244
 status, displaying 244
 show forward command 247
 show platform forward command 247
SNMP 35, 37, 38
 traps 35, 37, 38
 enabling MAC address notification 35, 37, 38
 software images 237
 recovery procedures 237
 See also downloading and uploading[software images 237
 SSID and client policy statistics 150
 monitoring using GUI 150
 stacks, switch 243
 partitioned 243
 static addresses 26
 See also addresses 26
 status, displaying 244
 stratum, NTP 23
 summer time 29
 switch stack 247
 system clock 21, 27, 28, 29
 configuring 27, 28, 29
 daylight saving time 29
 manually 27
 summer time 29
time zones 28
 overview 21
 system name 30
 manual configuration 30

T
time 21
 See also NTP and system clock 21
time zones 28
time-exceeded messages 232
 traceroute and 232
trace route command 232
 See also IP trace route 232
trace route, Layer 2 231
 and ARP 231
 and CDP 231
 broadcast traffic 231
described 231
 IP addresses and subnets 231
 MAC addresses and VLANs 231
 multicast traffic 231
 multiple devices on a port 231
 unicast traffic 231
 usage guidelines 231
traffic stream metrics (TSM) 161
described 161
 traps 35, 37, 38
 configuring MAC address notification 35, 37, 38
 enabling 35, 37, 38
troubleshooting 231, 232, 234, 244, 247
  displaying crash information 234
  setting packet forwarding 247
  SFP security and identification 244
  show forward command 247
  with debug commands 234
  with ping 231
  with traceroute 232
Troubleshooting Examples command 253

usage guidelines 231
using commands 234

V
VLAN ID, discovering 27
voice-over-IP (VoIP) telephone roaming 113

W
with debug commands 234
with ping 231
with traceroute 232
WMM parameter 174
world mode 89

U
U-APSD 161
  described 161
unicast MAC address filtering 41
    configuration 41
unicast traffic 231