Consolidated Platform Configuration Guide for Wireless Technologies, Cisco IOS XE 3.2SE (Catalyst 3850 Switches)

First Published: April 09, 2013

Last Modified: April 09, 2013

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

Text Part Number: OL-29469-01

CONTENTS

Preface — Preface xvii

Document Conventions xvii

Related Documentation xix

Obtaining Documentation and Submitting a Service Request xix

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 4

No and Default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 5

How to Use the CLI to Configure Features 5

Configuring the Command History 5

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 8

Editing Command Lines That Wrap 9

Searching and Filtering Output of show and more Commands 10

Accessing the CLI on a Switch Stack 11

Accessing the CLI Through a Console Connection or Through Telnet 11

PART I — VideoStream 13

CHAPTER 2 Configuring VideoStream 15

Finding Feature Information 15

Prerequisites for VideoStream 15

Restrictions for Configuring VideoStream 15

Information about VideoStream 16

How to Configure VideoStream 16

Configuring Multicast-Direct Globally for Media-Stream 16

Configuring Media-Stream for 802.11 bands 18

Configuring WLAN to Stream Video 19

Deleting a Media-Stream 20

Monitoring Media Streams 21

PART II WLAN 23

CHAPTER 3 Configuring WLANs 25

Finding Feature Information 25

Prerequisites for WLANs 25

Restrictions for WLANs 26

Information About WLANs 27

Band Selection 27

Off-Channel Scanning Defer 28

DTIM Period 28

Session Timeouts 29

Cisco Client Extensions 29

Peer-to-Peer Blocking 29

Diagnostic Channel 30

Per-WLAN Radius Source Support 30

How to Configure WLANs 30

Creating WLANs (CLI) 30

Deleting WLANs 31

Searching WLANs 32

Enabling WLANs (CLI) 33

Disabling WLANs (CLI) 34

Configuring General WLAN Properties (CLI) 34

Configuring Advanced WLAN Properties (CLI) 37
Monitoring WLAN Properties (CLI) 39
Where to Go Next 40
Additional References 40
Feature Information for WLANs 41

CHAPTER 4 Configuring DHCP for WLANs 43
Finding Feature Information 43
Prerequisites for Configuring DHCP for WLANs 43
Restrictions for Configuring DHCP for WLANs 44
Information About the Dynamic Host Configuration Protocol 44
Internal DHCP Servers 44
External DHCP Servers 45
DHCP Assignments 45
Information About DHCP Option 82 46
Configuring DHCP Scopes 47
Information About DHCP Scopes 47
How to Configure DHCP for WLANs 48
Configuring DHCP for WLANs (CLI) 48
Configuring DHCP Scopes (CLI) 50
Additional References 51
Feature Information for DHCP for WLANs 52

CHAPTER 5 Configuring WLAN Security 53
Finding Feature Information 53
Prerequisites for Layer 2 Security 53
Information About AAA Override 54
How to Configure WLAN Security 54
Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI) 54
Configuring Static WEP Layer 2 Security Parameters (CLI) 56
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI) 57
Configuring 802.1X Layer 2 Security Parameters (CLI) 58
Additional References 59
Feature Information about WLAN Layer 2 Security 60

CHAPTER 6 Configuring Access Point Groups 61

Finding Feature Information 61

Prerequisites for Configuring AP Groups 61

Restrictions for Configuring Access Point Groups 62

Information About Access Point Groups 62

How to Configure Access Point Groups 64

Creating Access Point Groups 64

Assigning an Access Point to an AP Group 65

Viewing Access Point Group 65

Additional References 66

Feature History and Information for Access Point Groups 67

PART III Radio Resource Management 69

CHAPTER 7 Configuring Radio Resource Management 71

Finding Feature Information 71

Prerequisites for Configuring Radio Resource Management 71

Restrictions for Radio Resource Management 72

Information About Radio Resource Management 72

Radio Resource Monitoring 72

Information About RF Groups 73

RF Group Leader 73

RF Group Name 75

Mobility Controller 75

Mobility Agent 76

Information About Rogue Access Point Detection in RF Groups 76

Transmit Power Control 76

Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings 77

Dynamic Channel Assignment 77

Coverage Hole Detection and Correction 78

How to Configure RRM 79

Configuring Advanced RRM CCX Parameters (CLI) 79

Configuring Neighbor Discovery Type (CLI) 80

Configuring RRM Profile Thresholds, Monitoring Channels, and Monitoring Intervals (GUI) 80
Configuring RF Groups 81
Configuring the RF Group Mode (GUI) 82
Configuring RF Group Selection Mode (CLI) 83
Configuring an RF Group Name (CLI) 83
Configuring an RF Group Name (GUI) 84
Configuring Members in a 802.11 Static RF Group (CLI) 84
Configuring Transmit Power Control 85
Configuring the Tx-Power Control Threshold (CLI) 85
Configuring the Tx-Power Level (CLI) 86
Configuring Transmit Power Control (GUI) 87
Configuring 802.11 RRM Parameters 88
Configuring Advanced 802.11 Channel Assignment Parameters (CLI) 88
Configuring Dynamic Channel Assignment (GUI) 90
Configuring 802.11 Coverage Hole Detection (CLI) 92
Configuring Coverage Hole Detection (GUI) 93
Configuring 802.11 Event Logging (CLI) 95
Configuring 802.11 Statistics Monitoring (CLI) 96
Configuring the 802.11 Performance Profile (CLI) 97
Configuring Rogue Access Point Detection in RF Groups 98
Configuring Rogue Access Point Detection in RF Groups (CLI) 98
Enabling Rogue Access Point Detection in RF Groups (GUI) 100
Monitoring RRM Parameters and RF Group Status 100
Monitoring RRM Parameters 100
Monitoring RF Group Status (CLI) 102
Monitoring RF Group Status (GUI) 102
Examples: RF Group Configuration 103
Additional References for Radio Resource Management 103
Feature History and Information For Performing Radio Resource Management Configuration 104

PART IV **Lightweight Access Points** 105

CHAPTER 8 **Configuring the Switch for Access Point Discovery** 107

Finding Feature Information 107
Prerequisites for Configuring the Switch for Access Point Discovery 107
Restrictions for Configuring the Switch for Access Point Discovery 108
Information About Configuring the Switch for Access Point Discovery 108
Access Point Communication Protocols 108
Viewing Access Point Join Information 109
Troubleshooting the Access Point Join Process 109
How to Configure Access Point Discovery 110
Configuring the Syslog Server for Access Points (CLI) 110
Monitoring Access Point Join Information (CLI) 111
Configuration Examples for Configuring the Switch for Access Point Discovery 112
Displaying the MAC Addresses of all Access Points: Example 112
DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example 113

CHAPTER 9 Configuring Data Encryption 115
Finding Feature Information 115
Prerequisites for Configuring Data Encryption 115
Restrictions for Configuring Data Encryption 115
Information About Data Encryption 116
How to Configure Data Encryption 116
Configuring Data Encryption (CLI) 116
Configuration Examples for Configuring Data Encryption 117
Displaying Data Encryption States for all Access Points: Examples 117

CHAPTER 10 Configuring Retransmission Interval and Retry Count 119
Finding Feature Information 119
Prerequisites for Configuring the Access Point Retransmission Interval and Retry Count 119
Information About Retransmission Interval and Retry Count 120
How to Configure Access Point Retransmission Interval and Retry Count 120
Configuring the Access Point Retransmission Interval and Retry Count (CLI) 120
Viewing CAPWAP Maximum Transmission Unit Information (CLI) 121
Configuration Examples for Configuring Access Point Retransmission Interval and Retry Count 122

Viewing the CAPWAP Retransmission Details: Example 122
Viewing Maximum Transmission Unit Information: Example 122

CHAPTER 11 Configuring Adaptive Wireless Intrusion Prevention System 123
Finding Feature Information 123
Prerequisites for Configuring wIPS 123
How to Configure wIPS on Access Points 124
Configuring wIPS on an Access Point (CLI) 124
Monitoring wIPS Information 125
Configuration Examples for Configuring wIPS on Access Points 126
Displaying the Monitor Configuration Channel Set: Example 126
Displaying wIPS Information: Examples 127

CHAPTER 12 Configuring Authentication for Access Points 129
Finding Feature Information 129
Prerequisites for Configuring Authentication for Access Points 129
Restrictions for Configuring Authentication for Access Points 130
Information about Configuring Authentication for Access Points 130
How to Configure Authentication for Access Points 131
Configuring Global Credentials for Access Points (CLI) 131
Configuring Global Credentials for Access Points (GUI) 132
Configuring Authentication for Access Points (CLI) 133
Configuring the Switch for Authentication (CLI) 135
Configuration Examples for Configuring Authentication for Access Points 137
Displaying the Authentication Settings for Access Points: Examples 137

CHAPTER 13 Converting Autonomous Access Points to Lightweight Mode 139
Finding Feature Information 139
Prerequisites for Converting Autonomous Access Points to Lightweight Mode 139
Information About Autonomous Access Points Converted to Lightweight Mode 140
Reverting from Lightweight Mode to Autonomous Mode 140
Using DHCP Option 43 and DHCP Option 60 140
How Converted Access Points Send Crash Information to the Switch 141
Uploading Memory Core Dumps from Converted Access Points 141
Displaying MAC Addresses for Converted Access Points 141

Configuring a Static IP Address for a Lightweight Access Point 141
How to Convert a Lightweight Access Point Back to an Autonomous Access Point 142
Converting a Lightweight Access Point Back to an Autonomous Access Point (CLI) 142
Converting a Lightweight Access Point Back to an Autonomous Access Point (Using the Mode Button and a TFTP Server) 142
Authorizing Access Points (CLI) 143
Disabling the Reset Button on Converted Access Points (CLI) 144
Monitoring the AP Crash Log Information 145
How to Configure a Static IP Address on an Access Point 146
Configuring a Static IP Address on an Access Point (CLI) 146
Recovering the Access Point Using the TFTP Recovery Procedure 148
Configuration Examples for Converting Autonomous Access Points to Lightweight Mode 148
Displaying the IP Address Configuration for Access Points: Example 148
Displaying Access Point Crash File Information: Example 148

CHAPTER 14 **Using Cisco Workgroup Bridges 149**
Finding Feature Information 149
Information About Cisco Workgroup Bridges and non-Cisco Workgroup bridges 149
Monitoring the Status of Workgroup Bridges 150
Debugging WGB Issues (CLI) 150
Configuration Examples for Configuring Workgroup Bridges 152
WGB Configuration: Example 152

CHAPTER 15 **Configuring Backup Switches and Failover Priority for Access Points 153**
Finding Feature Information 153
Prerequisites for Configuring Backup Switchs and Failover Priority for Access Points 153
Restrictions for Configuring Backup Switchs and Failover Priority for Access Points 154
Information About Configuring Backup Switchs 154
Configuring Failover Priority for Access Points 155
Optimizing RFID Tracking on Access Points 155
Retrieving the Unique Device Identifier on Switchs and Access Points 155
How to Configure Backup Switches for Access Points 156
Configuring Backup Switches for Access Points (CLI) 156

How to Configure Failover Priority for Access Points 158
Configuring Failover Priority for Access Points (CLI) 158
Retrieving Unique Device Identifier on Switches (CLI) 159
Monitoring Failover Priority Settings (CLI) 160
Configuration Examples for Configuring Backup Switchs and Failover Priority for Access Points 160
Displaying Access Point Configuration Information: Examples 160
Displaying Wireless Client Timer Information 161
Displaying Access Point CAPWAP Summary: Example 161

CHAPTER 16 Configuring Probe Request Forwarding 163
Finding Feature Information 163
Information About Configuring Probe Request Forwarding 163
How to Configure Probe Request Forwarding (CLI) 163

CHAPTER 17 Optimizing RFID Tracking 165
Finding Feature Information 165
Optimizing RFID Tracking on Access Points 165
How to Optimize RFID Tracking on Access Points 166
Optimizing RFID Tracking on Access Points (CLI) 166
Configuration Examples for Optimizing RFID Tracking 167
Displaying all the Access Points in Monitor Mode: Example 167

CHAPTER 18 Configuring Country Codes 169
Finding Feature Information 169
Prerequisites for Configuring Country Codes 169
Information About Configuring Country Codes 170
How to Configure Country Codes (CLI) 170
Configuration Examples for Configuring Country Codes 173
Displaying Channel List for Country Codes: Example 173

CHAPTER 19 Configuring Link Latency 175
Finding Feature Information 175
Prerequisites for Configuring Link Latency 175
Restrictions for Configuring Link Latency 176

Information About Configuring Link Latency 176
TCP MSS 176
Link Tests 176
How to Configure Link Latency 177
Configuring Link Latency (CLI) 177
How to Configure TCP MSS 179
Configuring TCP MSS (CLI) 179
Performing a Link Test (CLI) 179
Configuration Examples for Configuring Link Latency 180
Running a Link Test: Example 180
Displaying Link Latency Information: Example 181
Displaying TCP MSS Settings: Example 182

CHAPTER 20 Configuring Power over Ethernet 183
Finding Feature Information 183
Information About Configuring Power over Ethernet 183
How to Configure Power over Ethernet 184
Configuring Power over Ethernet (CLI) 184
Configuration Examples for Configuring Power over Ethernet 185
Displaying Power over Ethernet Information: Example 185

PART V CleanAir 187

CHAPTER 21 Configuring Cisco CleanAir 189
Finding Feature Information 189
Prerequisites for CleanAir 189
Restrictions for CleanAir 190
Information About CleanAir 191
Cisco CleanAir Components 191
Terms Used in Cisco CleanAir 193
Interference Types that Cisco CleanAir can Detect 193
Interference Device Merging 195
Persistent Devices 195
Persistent Devices Detection 195
Persistent Device Avoidance 195

EDRRM and AQR Update Mode 195
CleanAir High Availability 196
How to Configure CleanAir 196
Enabling CleanAir for 2.4-GHz Band 196
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices 197
Configuring Interference Reporting for 2.4-GHz Devices 198
Enabling CleanAir for 5-GHz Band 200
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices 201
Configuring Interference Reporting for 5-GHz devices 202
Configuring EDRRM for CleanAir-Events 203
Configuring Persistent Device Avoidance 204
Configuring Cisco CleanAir using the Controller GUI 205
Configuring Cisco Spectrum Expert 205
Configuring Spectrum Expert (CLI) 205
Monitoring CleanAir Parameters 206
Monitoring the Interference Devices 209
Configuration Examples for Configuring CleanAir 209
CleanAir FAQs 210
Additional References 212

PART VI **Mobility** 215

CHAPTER 22 **Information About Mobility** 217
Overview 217
Wired and Wireless Mobility 218
Features of Mobility 218
Sticky Anchoring for Low Latency Roaming 220
Bridge Domain ID and L2/L3 Roaming 220
Link Down Behavior 220
Platform Specific Scale Requirement for the Mobility Controller 220

CHAPTER 23 **Mobility Network Elements** 223
Mobility Agent 223
Mobility Controller 224
Mobility Oracle 225

Guest Controller 225

CHAPTER 24 Mobility Control Protocols 227

About Mobility Control Protocols 227

Initial Association and Roaming 227

Initial Association 228

Intra Switch Handoff 229

Intra Switch Peer Group Handoff 229

Inter Switch Peer Group Handoff 230

Inter Sub Domain Handoff 232

Inter Mobility Group Handoff 233

CHAPTER 25 Intra Sub Domain Mobility 235

Overview 235

Layer 2 Roaming 235

Layer 3 Roaming 236

Point of Presence at Access Switch 236

CHAPTER 26 Inter Sub Domain Mobility 239

Introduction 239

Point of Presence at Anchor Switch 240

CHAPTER 27 Mobility Controller and Mobility Tunnel Endpoint Redundancy 243

About MC and MTE Redundancy 243

CHAPTER 28 Configuring Mobility 245

Configuring Mobility Controller 245

Configuring Converged Access Controllers 245

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI) 245

Configuring Local Mobility Group (CLI) 247

Adding a Peer Mobility Group (CLI) 248

Configuring Optional Parameters for Roaming Behavior 248

Pointing the Mobility Controller to a Mobility Oracle (CLI) 249

Configuring Guest Controller 250

Configuring Guest Anchor 251

Configuring Mobility Agent 251
Configuring Mobility Agent by Pointing to Mobility Controller (CLI) 251
Configuring the Mobility Controller for the Mobility Agent (CLI) 252
Configuring Optional Parameters on a Mobility Agent (CLI) 253

Preface

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

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^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.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier` font	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

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

Reader Alert Conventions

This document may use the following conventions for reader alerts:

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

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

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

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

Warning **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

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

- Cisco Catalyst 3850 Switch documentation, located at:

  http://www.cisco.com/go/cat3850_docs

- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- Cisco Validated Designs documents, located at:

  http://www.cisco.com/go/designzone

- Error Message Decoder, located at:

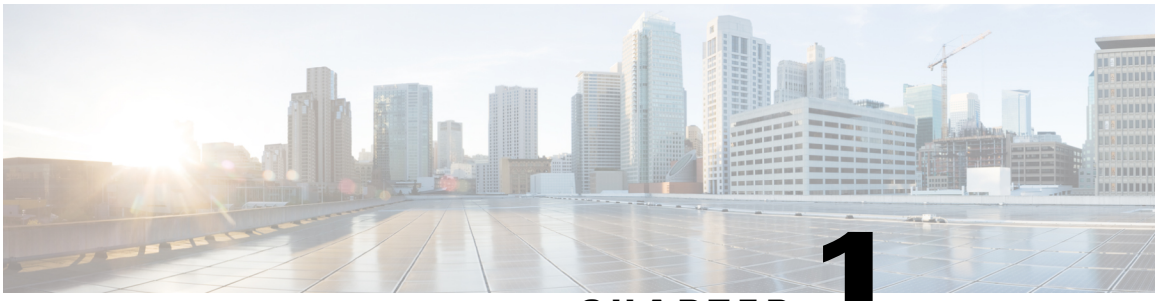
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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



CHAPTER 1

Using the Command-Line Interface

- Information About Using the Command-Line Interface, page 1
- How to Use the CLI to Configure Features, page 5

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 switch reboots.

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

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

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

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	`Switch>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Switch#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Switch(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Switch(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports.

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

Using the Help System

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**help** **Example:** `Switch# help`	Obtains a brief description of the help system in any command mode.

Step 2	*abbreviated-command-entry* **?**
	Example:
	`Switch# di?`
	`dir disable disconnect`
		Obtains a list of commands that begin with a particular character string.

Step 3	*abbreviated-command-entry* <Tab>
	Example:
	`Switch# sh conf<tab>`
	`Switch# show configuration`
		Completes a partial command name.

	Command or Action	Purpose
Step 4	**?** **Example:** `Switch> ?`	Lists all commands available for a particular command mode.
Step 5	*command* **?** **Example:** `Switch> show ?`	Lists the associated keywords for a command.

Step 6	*command keyword* **?**
	
	Example:
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`
		Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

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

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

```
Switch# show conf
```

No and Default Forms of Commands

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

Table 2: Common CLI Error Messages

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

Configuration Logging

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

Note Only CLI or HTTP changes are logged.

How to Use the CLI to Configure Features

Configuring the Command History

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

Changing the Command History Buffer Size

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

SUMMARY STEPS

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

DETAILED STEPS

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

Recalling Commands

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Ctrl-P** or use the **up arrow** key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Step 2	**Ctrl-N** or use the **down arrow** key	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.

	Command or Action	Purpose
Step 3	**show history** **Example:** `Switch# show history`	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.

Disabling the Command History Feature

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

SUMMARY STEPS

1. **terminal no history**

DETAILED STEPS

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

Enabling and Disabling Editing Features

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal editing** **Example:** `Switch# terminal editing`	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.

	Command or Action	Purpose
Step 2	**terminal no editing** **Example:** `Switch# terminal no editing`	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

Editing Commands Through Keystrokes

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

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

Table 3: Editing Commands

Editing Commands	Description
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 switch suddenly sends a message to your screen.

Editing Command Lines That Wrap

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	**access-list**
	
	Example:
	`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		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.

Step 2	**Ctrl-A** **Example:** `Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	Checks the complete syntax. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right.
Step 3	**Return** key	Execute the commands. 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.

Searching and Filtering Output of show and more Commands

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*	Searches and filters the output.

	Command or Action	Purpose

	Example:
	`Switch# 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`
		Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain **output** are not displayed, but the lines that contain **output** appear.

Accessing the CLI on a Switch Stack

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

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

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

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

Accessing the CLI Through a Console Connection or Through Telnet

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

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

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

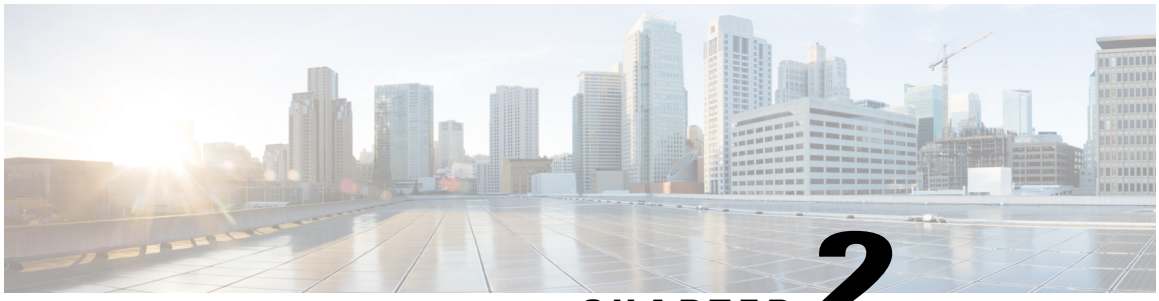
- Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH)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

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

PART I

VideoStream

- Configuring VideoStream, page 15



CHAPTER 2

Configuring VideoStream

- Finding Feature Information, page 15
- Prerequisites for VideoStream, page 15
- Restrictions for Configuring VideoStream, page 15
- Information about VideoStream, page 16
- How to Configure VideoStream, page 16
- Monitoring Media Streams, page 21

Finding Feature Information

Your software release may not support all 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 VideoStream

Make sure that the multicast feature is enabled. We recommend configuring IP multicast on the controller with multicast-multicast mode.

Check for the IP address on the client machine. The machine should have an IP address from the respective VLAN.

Verify that the access points have joined the controllers.

Restrictions for Configuring VideoStream

IGMP snooping is required to switch ON for this MC2UC feature to be functional.

Information about VideoStream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. The multicast frame packets are sent at a predetermined rate irrespective of the wireless client optimal data rate. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable. Also if the packets are delivered faster, the packets get congested.

The VideoStream feature makes the IP multicast stream delivery reliable over the air, by converting the multicast frame to a unicast frame over the air. Each VideoStream client acknowledges receiving a video IP multicast stream.

How to Configure VideoStream

Configuring Multicast-Direct Globally for Media-Stream

SUMMARY STEPS

1. **configure terminal**
2. **wireless multicast**
3. **IP igmp snooping**
4. **IP igmp snooping querier**
5. **wireless media-stream multicast-direct**
6. **wireless media-stream message**
7. **wireless media-stream group**<*name*><*startIp*><*endIp*>
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast**	Enables multicast for wireless forwarding.
Step 3	**IP igmp snooping**	Enables IGMP snooping on a per-VLAN basis. If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.
Step 4	**IP igmp snooping querier**	Configures a snooping querier on an interface when there is no multicast router in the VLAN to generate queries.

	Command or Action	Purpose
Step 5	**wireless media-stream multicast-direct** **Example:** `Switch(config)#wireless media-stream multicast-direct`	Configures the global multicast-direct feature for the controller.

Step 6	**wireless media-stream message**
	
	Example:
	`Switch(config)#wireless media-stream message ?`
	`  Email  Configure Session Announcement Email`
	`  Notes  Configure Session Announcement notes`
	`  URL  Configure Session Announcement URL`
	`  phone  Configure Session Announcement Phone number`
	`  <cr>`
		Configures various message configuration parameters like phone, URL, email and notes. That is, when a media stream is refused (due to bandwidth constraints), a message can be sent to the user. These parameters configure the messages to send IT support email address, notes (message to display explaining why the stream was refused), URL to which the user can be redirected and the phone number that the user can call about the refused stream.

Step 7	**wireless media-stream group**<*name*><*startIp*><*endIp*>
	
	Example:
	`Switch(config)#wireless media-stream group grp1 231.1.1.1 239.1.1.3`
	`Switch(config-media-stream)#?`
	
	`  avg-packet-size  Configures average packet size`
	`  default  Set a command to its defaults`
	
	`  exit  Exit sub-mode`
	`  max-bandwidth  Configures maximum Expected Stream Bandwidth in Kbps`
	`  no  Negate a command or set its defaults`
	`  policy  Configure media stream admission policy`
	`  qos  Configure  Over the AIR QoS class, <'video'> ONLY`
	
	`  <cr>`
		configures each media stream and its parameters like expected multicast destination addresses, stream bandwidth consumption and stream priority parameters.

Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Media-Stream for 802.11 bands

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz media-stream multicast-direct**
3. **ap dot11 24ghz | 5ghz media-stream video-redirect**
4. **ap dot11 24ghz | 5ghz media-stream multicast-direct admission-besteffort**
5. **ap dot11 24ghz | 5ghz media-stream multicast-direct client-maximum [<value >]**
6. **ap dot11 24ghz | 5ghz media-stream multicast-direct radio-maximum 20**
7. **ap dot11 24ghz | 5ghz cac multimedia max-bandwidth [<bandwidth>]**
8. **ap dot11 24ghz | 5ghz cac media-stream multicast-direct min_client_rate [<dot11_rate>]**
9. **ap dot11 5ghz cac media-stream**
10. **ap dot11 5ghz cac multimedia**
11. **ap dot11 5ghz cac video**
12. **ap dot11 5ghz cac voice**
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz media-stream multicast-direct** **Example:** `Switch(config)#ap dot11 24ghz media-stream multicast-direct`	Configures if media stream (mc2uc) is allowed for 802.11 band
Step 3	**ap dot11 24ghz | 5ghz media-stream video-redirect** **Example:** `Switch(config)#ap dot11 24ghz media-stream video-redirect`	Configures to redirect unicast video traffic to best effort queue.
Step 4	**ap dot11 24ghz | 5ghz media-stream multicast-direct admission-besteffort** **Example:** `Switch(config)#ap dot11 24ghz media-stream multicast-direct admission-besteffort`	Configures the media stream to still be sent through the best effort queue if a media stream cannot be prioritized due to bandwidth availability limitations. Add **no** in the command to drop the stream if the media stream cannot be prioritized due to bandwidth availability limitations.

	Command or Action	Purpose
Step 5	**ap dot11 24ghz | 5ghz media-stream multicast-direct client-maximum [<value >]** **Example:** `Switch(config)#ap dot11 24ghz media-stream multicast-direct client-max 15`	Configures maximum number of allowed media streams per individual client. The maximum is 15 and the default is 0. Value 0 denotes unlimited streams.
Step 6	**ap dot11 24ghz | 5ghz media-stream multicast-direct radio-maximum 20**	Configures maximum number of radio streams. The range is from 1 to 20. Default is 0. Value 0 denotes unlimited streams.
Step 7	**ap dot11 24ghz | 5ghz cac multimedia max-bandwidth [<bandwidth>]** **Example:** `Switch(config)#ap dot11 24ghz cac multimedia max-bandwidth 60`	Configure maximum media (voice + video) bandwidth in %. The range is between 5% and 85%.
Step 8	**ap dot11 24ghz | 5ghz cac media-stream multicast-direct min_client_rate [<dot11_rate>]** **Example:** `Switch(config)#ap dot11 24ghz cac media-stream multicast-direct min_client_rate`	Configures the minimum PHY rate needed for a client to send media-stream as unicast. Clients communicating below this rate will not receive the media stream as a unicast flow. Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.
Step 9	**ap dot11 5ghz cac media-stream**	Configures CAC parameters for media stream access category.
Step 10	**ap dot11 5ghz cac multimedia**	Configures CAC parameters for media access category, used for voice and video.
Step 11	**ap dot11 5ghz cac video**	Configures CAC parameters for video access category, used for voice signaling.
Step 12	**ap dot11 5ghz cac voice**	Configures CAC parameters for voice access category.
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring WLAN to Stream Video

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan_name*
3. **shutdown**
4. **media-stream multicast-direct**
5. **no shutdown**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan_name* **Example:** `Switch(config)#wlan wlan50`	Enters the WLAN configuration mode.
Step 3	**shutdown** **Example:** `Switch(config-wlan)#shutdown`	Disables the WLAN for configuring it parameters.
Step 4	**media-stream multicast-direct** **Example:** `Switch(config)#media-stream multicast-direct`	Configures the multicast-direct feature on media-stream for the WLAN.
Step 5	**no shutdown** **Example:** `Switch(config-wlan)#no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Deleting a Media-Stream

Before You Begin

The media-stream should be enabled and configured for it to be deleted.

SUMMARY STEPS

1. **configure terminal**
2. **no wireless media-stream group media_stream_name**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**no wireless media-stream group media_stream_name** **Example:** `Switch(config)#no wireless media-stream grp1`	Deletes the media-stream which bears the name mentioned in the command.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Media Streams

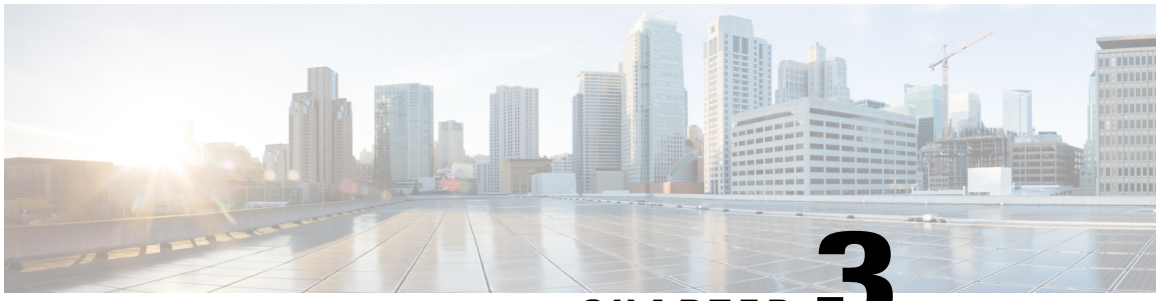
Table 4: Commands for monitoring media streams

Commands	Description
show wireless media-stream client detail *group name*	Displays media stream client details of the particular group.
show wireless media-stream client summary	Displays the media stream information of all the clients.
show wireless media-stream group detail *group name*	Displays the media stream configuration details of the particular group.
show wireless media-stream group summary	Displays the media stream configuration details of all the groups.
show wireless media-stream message details	Displays the session announcement message details.
show wireless multicast	Displays the multicast-direct configuration state.
show ap dot11 24ghz | 5ghz media-stream rrc	Displays 802.11 media Resource-Reservation-Control configurations.

PART II

WLAN

- Configuring WLANs, page 25
- Configuring DHCP for WLANs, page 43
- Configuring WLAN Security, page 53
- Configuring Access Point Groups, page 61



CHAPTER 3

Configuring WLANs

- Finding Feature Information, page 25
- Prerequisites for WLANs, page 25
- Restrictions for WLANs, page 26
- Information About WLANs, page 27
- How to Configure WLANs, page 30
- Monitoring WLAN Properties (CLI), page 39
- Where to Go Next, page 40
- Additional References, page 40
- Feature Information for WLANs, page 41

Finding Feature Information

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

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 WLANs

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point (AP) does not advertise disabled WLANs in its access point group or WLANs that belong to another group.
- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that switches properly route VLAN traffic.

- The switch uses different attributes to differentiate between WLANs with the same Service Set Identifier (SSID).
  - WLANs with the same SSID and same Layer 2 policy cannot be created if the WLAN ID is lower than 17.
  - Two WLANs with IDs that are greater than 17 and that have the same SSID and same Layer 2 policy is allowed if WLANs are added in different AP groups.

Note This requirement ensures that clients never detect the SSID present on the same access point radio.

Related Topics

Creating WLANs (CLI), on page 30
Configuring General WLAN Properties (CLI), on page 34
Deleting WLANs, on page 31
Configuring Advanced WLAN Properties (CLI), on page 37
Band Selection, on page 27
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 29
Peer-to-Peer Blocking, on page 29
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 33
Disabling WLANs (CLI), on page 34

Restrictions for WLANs

- Peer-to-peer blocking does not apply to multicast traffic.
- You can configure a maximum up to of 2000 clients.
- The WLAN name and SSID can have up to 32 characters. Spaces are not allowed in the WLAN profile name and SSID.
- You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.

Caution Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this feature with care.

Related Topics

Creating WLANs (CLI), on page 30
Configuring General WLAN Properties (CLI), on page 34
Deleting WLANs, on page 31
Configuring Advanced WLAN Properties (CLI), on page 37
Band Selection, on page 27
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 29
Peer-to-Peer Blocking, on page 29
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 33
Disabling WLANs (CLI), on page 34

Information About WLANs

This feature enables you to control up to 64 WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All switches publish up to 16 WLANs to each connected access point, but you can create up to the maximum number of WLANs supported and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the switch to access.

Band Selection

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

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

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 37

Prerequisites for WLANs, on page 25
Restrictions for WLANs, on page 26

Off-Channel Scanning Defer

In deployments with certain power-save clients, you sometimes need to defer the Radio Resource Management's (RRM) normal off-channel scanning to avoid missing critical information from low-volume clients (for example, medical devices that use power-save mode and periodically send telemetry information). This feature improves the way that Quality of Service (QoS) interacts with the RRM scan defer feature.

You can use a client's Wi-Fi Multimedia (WMM) UP marking to configure the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP.

Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitoring access points, or other access points in the same location that do not have this WLAN assigned.

You can assign a QoS policy (bronze, silver, gold, and platinum) to a WLAN to affect how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon) if all 802.11 clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently which results in a longer battery life. For example, if the beacon period is 100 ms and you set the DTIM value to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds. This rate allows the

power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, which results in a longer battery life.

Note A beacon period, which is specified in milliseconds on the switch, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. On Cisco's 802.11n access points, this value is rounded to the nearest multiple of 17 TUs. For example, a configured beacon period of 100 ms results in an actual beacon period of 104 ms.

Many applications cannot tolerate a long time between broadcast and multicast messages, which results in poor protocol and application performance. We recommend that you set a low DTIM value for 802.11 networks that support such clients.

Session Timeouts

You can configure a WLAN with a session timeout. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

Cisco Client Extensions

The Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features that are related to increased security, enhanced performance, fast roaming, and power management.

- The software supports CCX versions 1 through 5, which enables switches and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the switch and cannot be disabled. However, you can configure Aironet information elements (IEs).
- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the switch sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the switch and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 37

Prerequisites for WLANs, on page 25

Restrictions for WLANs, on page 26

Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the switch, dropped by the switch, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with the local switching WLAN.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 37

Prerequisites for WLANs, on page 25

Restrictions for WLANs, on page 26

Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the switch GUI or CLI to enable the diagnostic channel, and you can use the switch CLI to run the diagnostic tests.

Note We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface.

Per-WLAN Radius Source Support

By default, the switch sources all RADIUS traffic from the IP address on its management interface, which means that even if a WLAN has specific RADIUS servers configured instead of the global list, the identity used is the management interface IP address.

If you want to filter WLANs, you can use the callStationID that is set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

When you enable the per-WLAN RADIUS source support, the switch sources all RADIUS traffic for a particular WLAN by using the dynamic interface that is configured. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the switch on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in deployments that integrate with ACS Network Access Restrictions and Network Access Profiles.

You can combine per-WLAN RADIUS source support with the normal RADIUS traffic source and some WLANs that use the management interface and others using the per-WLAN dynamic interface as the address source.

How to Configure WLANs

Creating WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name wlan-id* [*ssid*]
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*] **Example:** `Switch(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID: • For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters. • For the *wlan-id*, enter the WLAN ID. The range is from 1 to 512. • For the *ssid*, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** By default, the WLAN is disabled.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 25

Restrictions for WLANs, on page 26

Deleting WLANs

SUMMARY STEPS

1. **configure terminal**
2. **no wlan** *wlan-name wlan-id ssid*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**no wlan** *wlan-name wlan-id ssid* **Example:** `Switch(config)# no wlan test2`	Deletes the WLAN. The arguments are as follows: • The *wlan-name* is the WLAN profile name. • The *wlan-id* is the WLAN ID. • The *ssid* is the WLAN SSID name configured for the WLAN. **Note** If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 25

Restrictions for WLANs, on page 26

Searching WLANs

SUMMARY STEPS

1. **show wlan summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show wlan summary** **Example:** `Switch# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

```
Switch# show wlan summary
Number of WLANs: 4
```

```
WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test1                            test1-ssid                     137  UP
3    test2                            test2-ssid                     136  UP
2    test3                            test3-ssid                     1    UP
45   test4                            test4-ssid                     1    DOWN
```

You can also use wild cards to search WLANs. For example **show wlan summary include** | *variable*. Where variable is any search string in the output.

```
Switch# show wlan summary | include test-wlan-ssid
1    test-wlan                       test-wlan-ssid                  137   UP
```

Enabling WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **no shutdown**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 25

Restrictions for WLANs, on page 26

Disabling WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **end**
5. **show wlan summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch(config-wlan)# shutdown`	Disables the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**show wlan summary** **Example:** `Switch# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

Related Topics

Prerequisites for WLANs, on page 25

Restrictions for WLANs, on page 26

Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Call Snooping
- Radio
- Interface
- Status

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **broadcast-ssid**
5. **radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**}
6. **client vlan** *vlan-identifier*
7. **ip multicast vlan** *vlan-name*
8. **media-stream multicast-direct**
9. **call-snoop**
10. **no shutdown**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch# shutdown`	Disables the WLAN before configuring the parameters.
Step 4	**broadcast-ssid** **Example:** `Switch(config-wlan)# broadcast-ssid`	Broadcasts the SSID for this WLAN. This field is enabled by default.

	Command or Action	Purpose
Step 5	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**} **Example:** `Switch# radio all`	Enables radios on the WLAN. The keywords are as follows: • **all**—Configures the WLAN on all radio bands. • **dot1a**—Configures the WLAN on only 802.11a radio bands. • **dot11g**—Configures the WLAN on 802.11ag radio bands. • **dot11bg**—Configures the WLAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled). • **dot11ag**— Configures the wireless LAN on 802.11g radio bands only.
Step 6	**client vlan** *vlan-identifier* **Example:** `Switch# client vlan test-vlan`	Enables an interface group on the WLAN. *vlan-identifier*—Specifies the VLAN identifier. This can be the VLAN name, VLAN ID, or VLAN group name.
Step 7	**ip multicast vlan** *vlan-name* **Example:** `Switch(config-wlan)# ip multicast vlan test`	Enables IP multicast on a WLAN. The keywords are as follows: • **vlan**—Specifies the VLAN ID. • *vlan-name*—Specifies the VLAN name.
Step 8	**media-stream multicast-direct** **Example:** `Switch(config-wlan)# media-stream multicast-direct`	Enables multicast VLANs on this WLAN.
Step 9	**call-snoop** **Example:** `Switch(config-wlan)# call-snoop`	Enables call-snooping support.
Step 10	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 25

Restrictions for WLANs, on page 26

Configuring Advanced WLAN Properties (CLI)

You can configure the following advanced properties:

- AAA Override
- Coverage Hole Detection
- Session Timeout
- Cisco Client Extensions
- Diagnostic Channels
- Interface Override ACLs
- P2P Blocking
- Client Exclusion
- Maximum Clients Per WLAN
- Off Channel Scan Defer

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **aaa-override**
4. **chd**
5. **session-timeout** *time-in-seconds*
6. **ccx aironet-iesupport**
7. **diag-channel**
8. **ip access-group** [web] *acl-name*
9. **peer-blocking** [**drop** | **forward-upstream**]
10. **exclusionlist** *time-in-seconds*
11. **client association limit** *max-number-of-clients*
12. **channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}}
13. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**aaa-override** **Example:** `Switch(config-wlan)# aaa-override`	Enables AAA override.
Step 4	**chd** **Example:** `Switch(config-wlan)# chd`	Enables coverage hole detection for this WLAN. This field is enabled by default.
Step 5	**session-timeout** *time-in-seconds* **Example:** `Switch(config-wlan)# session-timeout 450`	Sets the session timeout in seconds. The range and default values vary according to the security configuration. If the WLAN security is configured to dot1x, the range is 300 to 86400 seconds and the default value is 1800 seconds. For all other WLAN security configurations, the range is 1 to 65535 seconds and the default value is 0 seconds. A value of 0 indicates no session timeout.
Step 6	**ccx aironet-iesupport** **Example:** `Switch(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet IEs for this WLAN. This field is enabled by default.
Step 7	**diag-channel** **Example:** `Switch(config-wlan)# diag-channel`	Enables diagnostic channel support to troubleshoot client communication issues on a WLAN.
Step 8	**ip access-group** [web] *acl-name* **Example:** `Switch(config)# ip access-group test-acl-name`	Configures the WLAN ACL group. The variable *acl-name* specifies the user-defined IPv4 ACL name. The keyword **web** specifies the IPv4 web ACL.
Step 9	**peer-blocking** [**drop** | **forward-upstream**] **Example:** `Switch(config)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **drop—**Enables peer-to-peer blocking on the drop action. • **forward-upstream—**Enables peer-to-peer blocking on the forward upstream action.
Step 10	**exclusionlist** *time-in-seconds* **Example:** `Switch(config)# exclusionlist 10`	Specifies the timeout in seconds. The valid range is from 0 to 2147483647. Enter 0 for no timeout. A zero (0) timeout indicates that the client is permanently added to the exclusion list.

	Command or Action	Purpose
Step 11	**client association limit** *max-number-of-clients* **Example:** `Switch(config)# client association limit 200`	Sets the maximum number of clients that can be configured on a WLAN.
Step 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} **Example:** `Switch(config)# channel-scan defer-priority 6`	Sets the channel scan defer priority and defer time. The arguments are as follows: • **defer-priority—**Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3. • **defer-time—**Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Band Selection, on page 27
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 29
Peer-to-Peer Blocking, on page 29
Diagnostic Channel
Client Count Per WLAN
Prerequisites for WLANs, on page 25
Restrictions for WLANs, on page 26
Information About AAA Override, on page 54
Prerequisites for Layer 2 Security, on page 53

Monitoring WLAN Properties (CLI)

Command	Description
show wlan id *wlan-id*	Displays WLAN properties based on the WLAN ID.
show wlan name *wlan-name*	Displays WLAN properties based on the WLAN name.

Command	Description
show wlan all	Displays WLAN properties of all configured WLANs.
show wlan summary	Displays a summary of all WLANs. The summary details includes the following information: • WLAN ID • Profile name • SSID • VLAN • Status
show running-config wlan *wlan-name*	Displays the running configuration of a WLAN based on the WLAN name.
show running-config *wlan*	Displays the running configuration of all WLANs.

Where to Go Next

Proceed to configure DHCP for WLANs.

Additional References

Related Documents

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Mobility Anchor configuration	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
WebAuth Configuration	*Security Configuration Guide (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

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

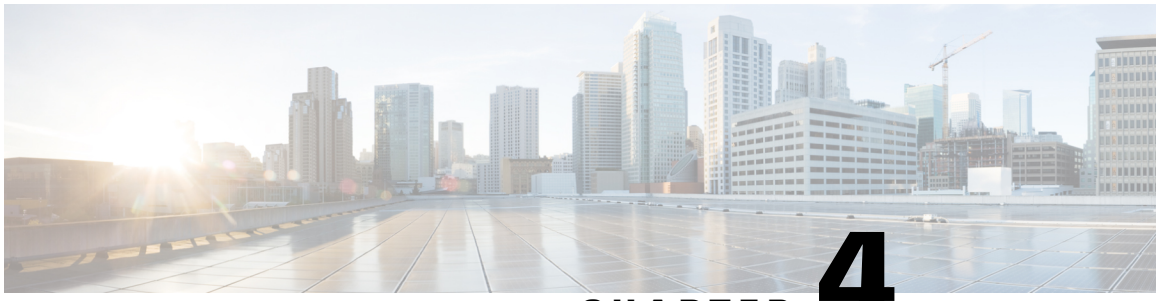
Technical Assistance

Description	Link
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.	http://www.cisco.com/support

Feature Information for WLANs

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
WLAN Functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 4

Configuring DHCP for WLANs

- Finding Feature Information, page 43
- Prerequisites for Configuring DHCP for WLANs, page 43
- Restrictions for Configuring DHCP for WLANs, page 44
- Information About the Dynamic Host Configuration Protocol, page 44
- How to Configure DHCP for WLANs, page 48
- Additional References, page 51
- Feature Information for DHCP for WLANs, page 52

Finding Feature Information

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

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 DHCP for WLANs

- To be able to use the DHCP option 82, you must configure DHCP on Cisco IOS software. By default, DHCP option 82 is enabled for all clients. You can control the wireless client behavior using the WLAN suboptions.

Related Topics

Configuring DHCP for WLANs (CLI), on page 48

Information About the Dynamic Host Configuration Protocol, on page 44

Internal DHCP Servers, on page 44

External DHCP Servers, on page 45
DHCP Assignments, on page 45
Information About DHCP Option 82, on page 46
Configuring DHCP Scopes, on page 47
Information About DHCP Scopes, on page 47

Restrictions for Configuring DHCP for WLANs

- If you override the DHCP server in a WLAN, you must ensure that you configure the underlying Cisco IOS configuration to make sure that the DHCP server is reachable.
- WLAN DHCP override works only if DHCP service is enabled on the switch.

  You can configure DHCP service in the following ways:

  - Configuring the DHCP pool on the switch.
  - Configuring a DHCP relay agent on the SVI. Note: the VLAN of the SVI must be mapped to the WLAN where DHCP override is configured.

Related Topics

Configuring DHCP for WLANs (CLI), on page 48
Information About the Dynamic Host Configuration Protocol, on page 44
Internal DHCP Servers, on page 44
External DHCP Servers, on page 45
DHCP Assignments, on page 45
Information About DHCP Option 82, on page 46
Configuring DHCP Scopes, on page 47
Information About DHCP Scopes, on page 47

Information About the Dynamic Host Configuration Protocol

You can configure WLANs to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available: internal and external.

Related Topics

Configuring DHCP for WLANs (CLI), on page 48
Prerequisites for Configuring DHCP for WLANs, on page 43
Restrictions for Configuring DHCP for WLANs, on page 44

Internal DHCP Servers

The switches contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The wireless network generally contains a maximum of 10 access points or fewer, with the access points on the same IP subnet as the switch. The internal server provides DHCP addresses to wireless clients, direct-connect access points, and DHCP requests that are relayed from access points. Only

lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the switch as the DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the switch, such as local subnet broadcast, Domain Name System (DNS), or priming.

An internal DHCP server pool only serves the wireless clients of that switch, not clients of other switches. Also, an internal DHCP server can serve only wireless clients, not wired clients.

When clients use the internal DHCP server of the switch, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned with the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one. Wired guest clients are always on a Layer 2 network connected to a local or foreign switch.

Note DHCPv6 is not supported in the internal DHCP servers.

Related Topics

Configuring DHCP for WLANs (CLI), on page 48

Prerequisites for Configuring DHCP for WLANs, on page 43

Restrictions for Configuring DHCP for WLANs, on page 44

External DHCP Servers

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay, which means that each switch appears as a DHCP Relay agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

Because the switch captures the client IP address that is obtained from a DHCP server, it maintains the same IP address for that client during intra switch, inter switch, and inter-subnet client roaming.

Note External DHCP servers can support DHCPv6.

Related Topics

Configuring DHCP for WLANs (CLI), on page 48

Prerequisites for Configuring DHCP for WLANs, on page 43

Restrictions for Configuring DHCP for WLANs, on page 44

DHCP Assignments

You can configure DHCP on a per-interface or per-WLAN basis. We recommend that you use the primary DHCP server address that is assigned to a particular interface.

You can assign DHCP servers for individual interfaces. You can configure the management interface, AP-manager interface, and dynamic interface for a primary and secondary DHCP server, and you can configure

the service-port interface to enable or disable DHCP servers. You can also define a DHCP server on a WLAN. In this case, the server overrides the DHCP server address on the interface assigned to the WLAN.

Security Considerations

For enhanced security, we recommend that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all WLANs with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not allowed on the network. The switch monitors DHCP traffic because it acts as a DHCP proxy for the clients.

Note WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server.

If slightly less security is tolerable, you can create WLANs with DHCP Addr. Assignment Required disabled. Clients then have the option of using a static IP address or obtaining an IP address from a designated DHCP server.

Note DHCP Addr. Assignment Required is not supported for wired guest LANs.

You can create separate WLANs with DHCP Addr. Assignment Required configured as disabled. This is applicable only if DHCP proxy is enabled for the switch. You must not define the primary/secondary configuration DHCP server you should disable the DHCP proxy. These WLANs drop all DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

Related Topics

Configuring DHCP for WLANs (CLI), on page 48

Prerequisites for Configuring DHCP for WLANs, on page 43

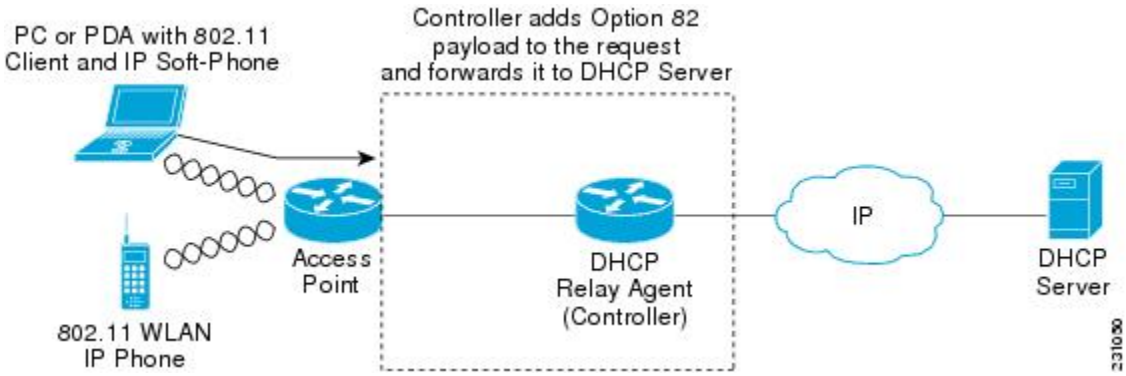
Restrictions for Configuring DHCP for WLANs, on page 44

Information About DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the switch to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can

configure the switch to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.

Figure 1: DHCP Option 82



The access point forwards all DHCP requests from a client to the switch. The switch adds the DHCP option 82 payload and forwards the request to the DHCP server. The payload can contain the MAC address or the MAC address and SSID of the access point, depending on how you configure this option.

Note Any DHCP packets that already include a relay agent option are dropped at the switch.

For DHCP option 82 to operate correctly, DHCP proxy must be enabled.

Related Topics

Configuring DHCP for WLANs (CLI), on page 48
Prerequisites for Configuring DHCP for WLANs, on page 43
Restrictions for Configuring DHCP for WLANs, on page 44

Configuring DHCP Scopes

Related Topics

Configuring DHCP for WLANs (CLI), on page 48
Prerequisites for Configuring DHCP for WLANs, on page 43
Restrictions for Configuring DHCP for WLANs, on page 44

Information About DHCP Scopes

Switches have built-in DHCP relay agents. However, when you desire network segments that do not have a separate DHCP server, the switches can have built-in DHCP scopes that assign IP addresses and subnet masks to wireless clients. Typically, one switch can have one or more DHCP scopes that each provide a range of IP addresses.

DHCP scopes are needed for internal DHCP to work. Once DHCP is defined on the switch, you can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to the switch's management interface.

Related Topics

Configuring DHCP for WLANs (CLI), on page 48
Prerequisites for Configuring DHCP for WLANs, on page 43
Restrictions for Configuring DHCP for WLANs, on page 44
Configuring DHCP Scopes (CLI), on page 50

How to Configure DHCP for WLANs

Configuring DHCP for WLANs (CLI)

Use this procedure to configure the following DHCP parameters on a WLAN:

- DHCP Option 82 Payload
- DHCP Required
- DHCP Override

Before You Begin

- You must have admin privileges for configuring the WLAN.
- To configure the DHCP override, you must have the IP address of the DHCP server.

SUMMARY STEPS

1. **configure terminal**
2. **shutdown**
3. **wlan** *profile-name*
4. **ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**}
5. **ip dhcp required**
6. **ip dhcp server** *ip-address*
7. **no shutdown**
8. **end**
9. **show wlan** *wlan-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**shutdown** **Example:** `Switch(config)# shutdown`	Shut down the WLAN.
Step 3	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

Step 4	**ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**}
	
	Example:
	`Switch(config)# ip dhcp opt82 format add-ssid`
		Specifies the DHCP82 payload on the WLAN. The keyword and arguments are as follows:
		• **ascii—**Configures ASCII for DHCP Option 82. If this is not configured, the option 82 format is set to ASCII format.
		• **format—**Specifies the DHCP option 82 format. The following options are available:
		  • *add-ssid***—**Set RemoteID format that is the AP radio MAC address and SSID.
		  • *ap-ethmac***—**Set RemoteID format that is the AP Ethernet MAC address.
		Note If the format option is not configured, only the AP radio MAC address is used.
		• **rid—**Adds the Cisco 2 byte RID for DHCP option 82.

Step 5	**ip dhcp required** **Example:** `Switch(config-wlan)# ip dhcp required`	Makes it mandatory for clients to get their IP address from the DHCP server. Static clients are not allowed.
Step 6	**ip dhcp server** *ip-address* **Example:** `Switch(config-wlan)# ip dhcp server 200.1.1.2`	Defines a DHCP server on the WLAN that overrides the DHCP server address on the interface assigned to the WLAN.
Step 7	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Restarts the WLAN.

	Command or Action	Purpose
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show wlan** *wlan-name* **Example:** `Switch(config-wlan)# show wlan test-wlan`	Verifies the DHCP configuration.

Related Topics

Information About the Dynamic Host Configuration Protocol, on page 44
Internal DHCP Servers, on page 44
External DHCP Servers, on page 45
DHCP Assignments, on page 45
Information About DHCP Option 82, on page 46
Configuring DHCP Scopes, on page 47
Information About DHCP Scopes, on page 47
Prerequisites for Configuring DHCP for WLANs, on page 43
Restrictions for Configuring DHCP for WLANs, on page 44

Configuring DHCP Scopes (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp pool** *pool-name*
3. **network** *network-name mask-address*
4. **dns-server** *hostname*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**ip dhcp pool** *pool-name* **Example:** `Switch(config)#ip dhcp pool test-pool`	Configures the DHCP pool address.
Step 3	**network** *network-name mask-address* **Example:** `Switch(dhcp-config)#network 209.165.200.224 255.255.255.0`	Specifies the network number in dotted-decimal notation and the mask address.
Step 4	**dns-server** *hostname* **Example:** `Switch(dhcp-config)#dns-server example.com`	Specifies the DNS name server. You can specify an IP address or a hostname.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Information About DHCP Scopes, on page 47

Additional References

Related Documents

Related Topic	Document Title
System Management	*System Management Configuration Guide (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

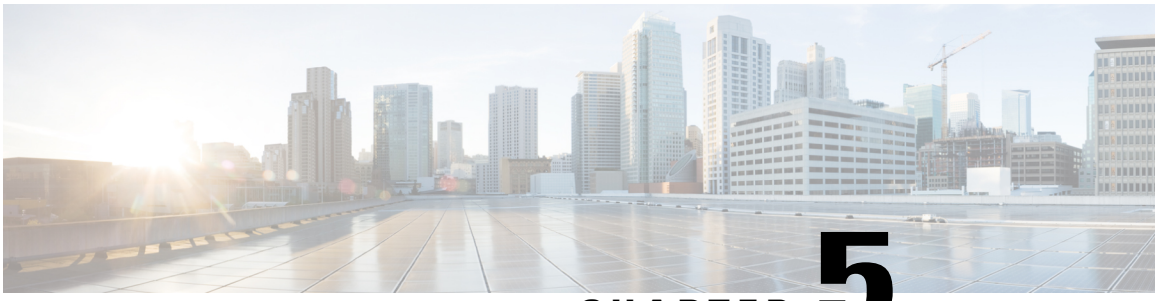
MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://cisco.com/go/mibs

Technical Assistance

Description	Link
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.	http://www.cisco.com/support

Feature Information for DHCP for WLANs

Feature Name	Release	Feature Information
DHCP functionality for WLAN	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 5

Configuring WLAN Security

- Finding Feature Information, page 53
- Prerequisites for Layer 2 Security, page 53
- Information About AAA Override, page 54
- How to Configure WLAN Security, page 54
- Additional References, page 59
- Feature Information about WLAN Layer 2 Security, page 60

Finding Feature Information

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

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 Layer 2 Security

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- Static WEP or 802.1X

Note Because static WEP and 802.1X are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.

- WPA/WPA2

Note Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.

Related Topics

Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI), on page 54
Configuring Static WEP Layer 2 Security Parameters (CLI), on page 56
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI), on page 57
Configuring 802.1X Layer 2 Security Parameters (CLI), on page 58
Configuring Advanced WLAN Properties (CLI), on page 37
Information About AAA Override, on page 54

Information About AAA Override

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 37
Prerequisites for Layer 2 Security, on page 53

How to Configure WLAN Security

Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI)

Before You Begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** {**authentication** {**open** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0**|**8**}} *wep-key wep-key-index1-4*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security static-wep-key** {**authentication** {**open**	**sharedkey**}	**encryption** {**104**	**40**} [**ascii**	**hex**] {**0**|**8**}} *wep-key wep-key-index1-4* **Example:** `Switch(config-wlan)# security static-wep-key encryption 40 hex 0 test 2`	Configures static WEP security on a WLAN. The keywords and arguments are as follows: • **authentication—**Configures 802.11 authentication. • **encryption—**Sets the static WEP keys and indices. • **open—**Configures open system authentication. • **sharedkey—**Configures shared key authentication. • **104, 40—**Specifies the WEP key size. • **hex, ascii—**Specifies the input format of the key. • *wep-key-index* , *wep-key-index1-4*—Type of password that follows. A value of 0 indicates that an unencrypted password follows. A value of 8 indicates that an AES encrypted follows.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 53

Configuring Static WEP Layer 2 Security Parameters (CLI)

Before You Begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** [**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security static-wep-key** [**authentication** {**open**	**shared**}	**encryption** {**104**	**40**} {**ascii**	**hex**} [**0**	**8**]] **Example:** `Switch(config-wlan)# security static-wep-key authentication open`	The keywords are as follows: • **static-wep-key—**Configures Static WEP Key authentication. • **authentication—**Specifies the authentication type you can set. The values are open and shared. • **encryption—**Specifies the encryption type that you can set. The valid values are 104 and 40. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters • **ascii—**Specifies the key format as ASCII. • **hex—**Specifies the key format as HEX.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 53

Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

Note The default security policy is WPA2.

Before You Begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security wpa**
4. **security wpa wpa1**
5. **security wpa wpa1 ciphers** [**aes** | **tkip**]
6. **security wpa wpa2**
7. **security wpa wpa2 ciphers** [**aes** | **tkip**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security wpa** **Example:** `Switch(config-wlan)# security wpa`	Enables WPA.
Step 4	**security wpa wpa1** **Example:** `Switch(config-wlan)# security wpa wpa1`	Enables WPA1.
Step 5	**security wpa wpa1 ciphers** [**aes**	**tkip**] **Example:** `Switch(config-wlan)# security wpa wpa1 ciphers aes`	Specifies the WPA1 cipher. Choose one of the following encryption types: • **aes—**Specifies WPA/AES support. • **tkip—**Specifies WPA/TKIP support.

	Command or Action	Purpose
Step 6	**security wpa wpa2** **Example:** `Switch(config-wlan)# security wpa`	Enables WPA 2.
Step 7	**security wpa wpa2 ciphers** [**aes** | **tkip**] **Example:** `Switch(config-wlan)# security wpa wpa2 ciphers tkip`	Configure WPA2 cipher. Choose one of the following encryption types: • **aes—**Specifies WPA/AES support. • **tkip—**Specifies WPA/TKIP support.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 53

Configuring 802.1X Layer 2 Security Parameters (CLI)

Before You Begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security dot1x**
4. **security** [**authentication-list** *auth-list-name* | **encryption** {**0** | **104** | **40**}
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security dot1x** **Example:** `Switch(config-wlan)# security dot1x`	Specifies 802.1X security.
Step 4	**security** [**authentication-list** *auth-list-name* | **encryption** {**0** | **104** | **40**} **Example:** `Switch(config-wlan)# security encryption 104`	The keywords and arguments are as follows: • **authentication-list—**Specifies the authentication list for IEEE 802.1X. • **encryption—**Specifies the length of the CKIP encryption key. The valid values are 0, 40, and 104. Zero (0) signifies no encryption. This is the default. **Note** All keys within a WLAN must be of the same size.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 53

Additional References

Related Documents

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Security configuration guide	*Security Configuration Guide (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

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

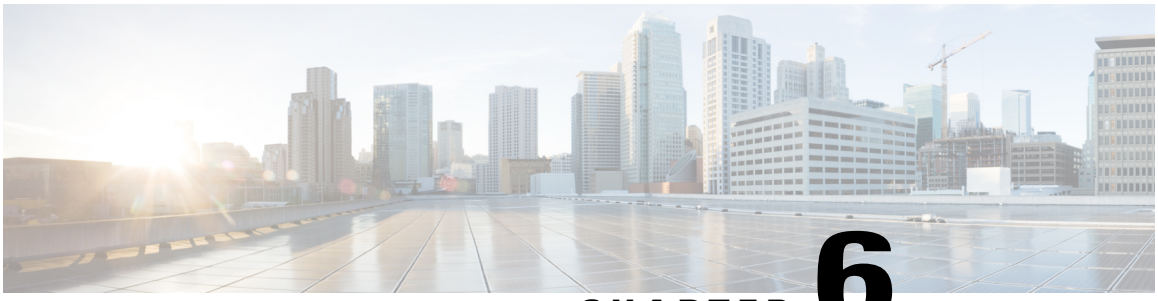
Technical Assistance

Description	Link
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.	http://www.cisco.com/support

Feature Information about WLAN Layer 2 Security

This table lists the features in this module and provides links to specific configuration information.

Feature Name	Release	Feature Information
WLAN Security functionality	Cisco IOS XE 3.2SE	This feature was introduced.



CHAPTER 6

Configuring Access Point Groups

- Finding Feature Information, page 61
- Prerequisites for Configuring AP Groups, page 61
- Restrictions for Configuring Access Point Groups, page 62
- Information About Access Point Groups, page 62
- How to Configure Access Point Groups, page 64
- Additional References, page 66
- Feature History and Information for Access Point Groups, page 67

Finding Feature Information

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

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 AP Groups

The following are the prerequisites for creating access point groups on a switch:

- The required access control list (ACL) must be defined on the router that serves the VLAN or subnet.
- Multicast traffic is supported with access point group VLANs. However, if the client roams from one access point to another, the client might stop receiving multicast traffic, unless IGMP snooping is enabled.

Related Topics

Information About Access Point Groups, on page 62

Restrictions for Configuring Access Point Groups, on page 62

Restrictions for Configuring Access Point Groups

- Suppose that the interface mapping for a WLAN in the AP group table is the same as the WLAN interface. If the WLAN interface is changed, the interface mapping for the WLAN in the AP group table also changes to the new WLAN interface.

  Suppose that the interface mapping for a WLAN in the AP group table is different from the one defined for the WLAN. If the WLAN interface is changed, then the interface mapping for the WLAN in the AP group table does not change to the new WLAN interface.

- If you clear the configuration on the switch, all of the access point groups disappear except for the default access point group "default-group," which is created automatically.

- The default access point group can have up to 16 WLANs associated with it. The WLAN IDs for the default access point group must be less than or equal to 16. If a WLAN with an ID greater than 16 is created in the default access point group, the WLAN SSID will not be broadcasted. All WLAN IDs in the default access point group must have an ID that is less than or equal to 16. WLANs with IDs greater than 16 can be assigned to custom access point groups.

Related Topics

Information About Access Point Groups, on page 62
Prerequisites for Configuring AP Groups, on page 61

Information About Access Point Groups

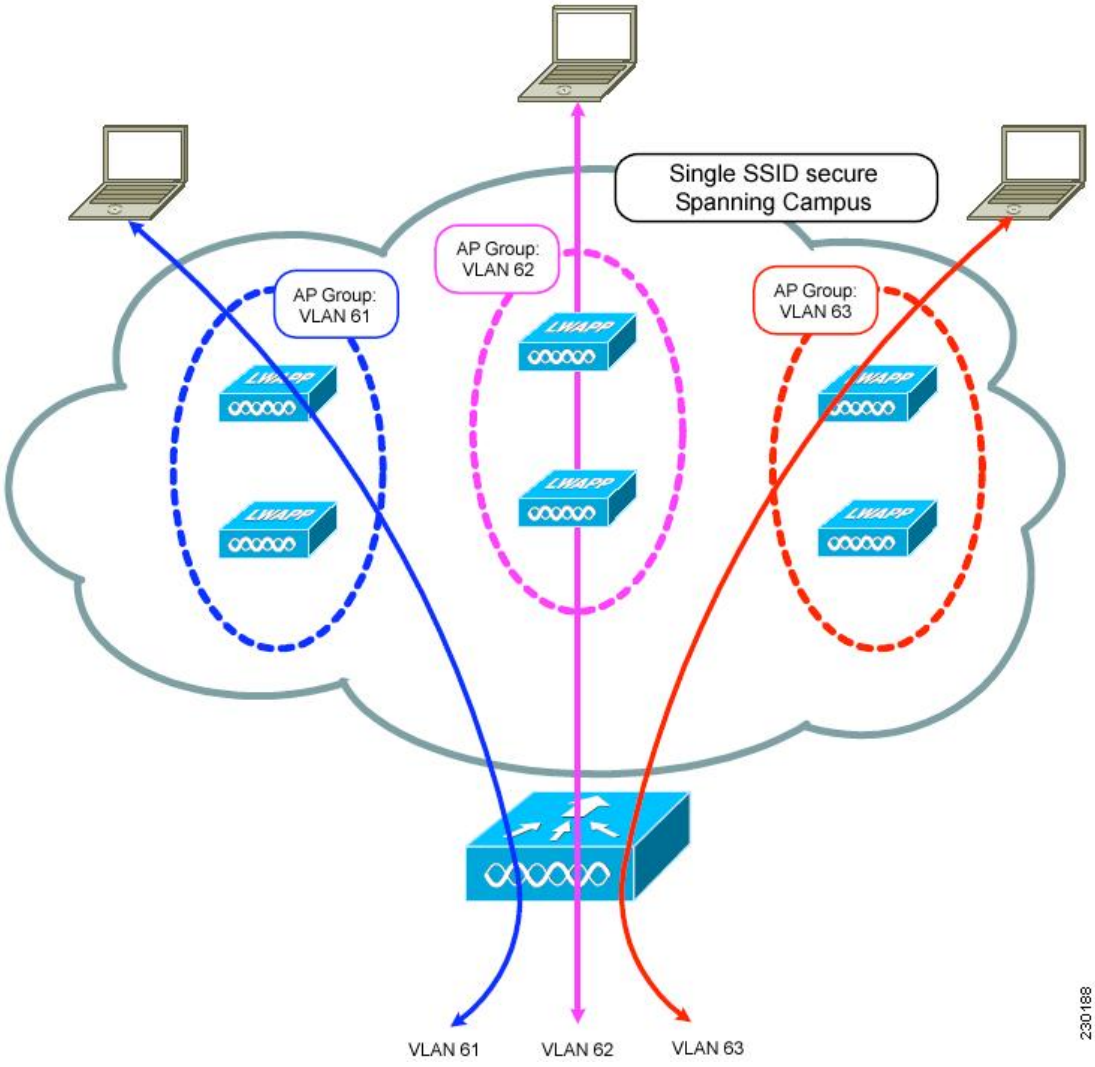
After you create up to 512 WLANs on the switch, you can selectively publish them (using access point groups) to different access points to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the switch. Therefore, all users that are associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration.

In the figure, three configured dynamic interfaces are mapped to three different VLANs (VLAN 61, VLAN 62, and VLAN 63). Three access point groups are defined, and each is a member of a different VLAN, but all are members of the same SSID. A client within the wireless SSID is assigned an IP address from the VLAN subnet on which its access point is a member. For example, any user that associates with an access point that is a member of access point group VLAN 61 is assigned an IP address from that subnet.

In the figure, the switch internally treats roaming between access points as a Layer 3 roaming event. In this way, WLAN clients maintain their original IP addresses.

After all access points have joined the switch, you can create access point groups and assign up to 16 WLANs to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group.

Figure 2: Access Point Groups



Related Topics

Creating Access Point Groups, on page 64

Viewing Access Point Group, on page 65

Assigning an Access Point to an AP Group, on page 65

Prerequisites for Configuring AP Groups, on page 61

Restrictions for Configuring Access Point Groups, on page 62

How to Configure Access Point Groups

Creating Access Point Groups

Before You Begin

You must have administrator privileges to perform this operation.

SUMMARY STEPS

1. **configure terminal**
2. **ap group** *ap-group-name*
3. **wlan** *wlan-name*
4. (Optional) **vlan** *vlan-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap group** *ap-group-name* **Example:** `Switch(config)# ap group my-ap-group`	Creates an access point group.
Step 3	**wlan** *wlan-name* **Example:** `Switch(config-apgroup)# wlan wlan-name`	Associates the AP group to a WLAN.
Step 4	**vlan** *vlan-name* **Example:** `Switch(config-apgroup)# vlan test-vlan`	(Optional) Assigns the access point group to a VLAN.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

This example shows how to create an AP group:

```
Switch# configure terminal
Switch(config-apgroup)# ap group test-ap-group-16
```

```
Switch(config-wlan-apgroup)# wlan test-ap-group-16
Switch(config-wlan-apgroup)# vlan VLAN1300
```

Related Topics

Information About Access Point Groups, on page 62

Assigning an Access Point to an AP Group

Before You Begin

You must have administrator privileges to perform this operation.

SUMMARY STEPS

1. **ap name** *ap-name* **ap-group-name** *ap-group*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **ap-group-name** *ap-group* **Example:** `Switch# ap name 1240-101 ap-groupname apgroup_16`	Assigns the access point to the access point group. The keywords and arguments are as follows: • **name—**Specifies that the argument following this keyword is the name of an AP that is associated to the switch. • *ap-name*—AP that you want to associate to the AP group. • **ap-group-name—**Specifies that the argument following this keyword is the name of the AP group that is configured on the switch. • *ap-group*—Name of the access point group that is configured on the switch.

Related Topics

Information About Access Point Groups, on page 62

Viewing Access Point Group

Before You Begin

You must have administrator privileges to perform this operation.

SUMMARY STEPS

1. **show ap groups** [**extended**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ap groups** [**extended**] **Example:** `Switch# show ap groups`	Displays the AP groups configured on the switch. The **extended** keyword displays all AP Groups information defined in the system in detail.

Related Topics

Information About Access Point Groups, on page 62

Additional References

Related Documents

Related Topic	Document Title
WLAN commands	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Lightweight Access Point configuration	*Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Lightweight Access Point commands	*Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

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

Technical Assistance

Description	Link
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.	http://www.cisco.com/support

Feature History and Information for Access Point Groups

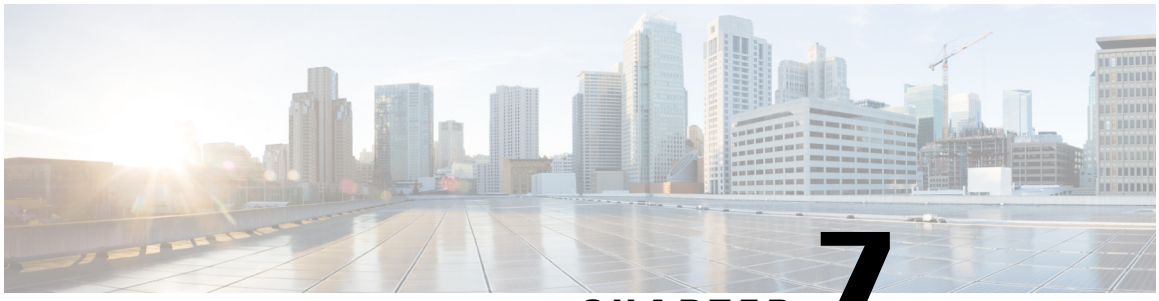
This table lists the features in this modules and provides links to specific configuration information.

Feature Name	Release	Feature Information
AP Groups	Cisco IOS XE 3.2SE	This feature was introduced.

PART III

Radio Resource Management

- Configuring Radio Resource Management, page 71



CHAPTER 7

Configuring Radio Resource Management

- Finding Feature Information, page 71
- Prerequisites for Configuring Radio Resource Management, page 71
- Restrictions for Radio Resource Management, page 72
- Information About Radio Resource Management, page 72
- How to Configure RRM, page 79
- Monitoring RRM Parameters and RF Group Status, page 100
- Examples: RF Group Configuration, page 103
- Additional References for Radio Resource Management, page 103
- Feature History and Information For Performing Radio Resource Management Configuration, page 104

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 Radio Resource Management

The switch should be configured as a mobility controller and not a mobility anchor to configure Radio Resource Management. It may require dynamic channel assignment functionality for the home APs to be supported.

The new mobility architecture that involves mobility controller and mobility agent must be configured on the switch or controllers for RRM to work.

Note Refer Mobility Configuration Guide for configuring mobility controller and mobility agent.

Restrictions for Radio Resource Management

The number of APs in a RF-group is limited to 500.

If an AP tries to join the RF-group that already holds the maximum number of APs it can support, the device rejects the application and throws an error.

Information About Radio Resource Management

The Radio Resource Management (RRM) software embedded in the switch acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables switches to continually monitor their associated lightweight access points for the following information:

- Traffic load—The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.
- Interference—The amount of traffic coming from other 802.11 sources.
- Noise—The amount of non-802.11 traffic that is interfering with the currently assigned channel.
- Coverage—The Received Signal Strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.
- Other —The number of nearby access points.

RRM performs these functions:

- Radio resource monitoring
- Transmit power control
- Dynamic channel assignment
- Coverage hole detection and correction
- RF grouping

Radio Resource Monitoring

RRM automatically detects and configures new switches and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can scan all valid channels for the country of operation as well as for channels available in other locations. The access points in local mode go “off-channel” for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

Note In the presence of voice traffic or other critical traffic (in the last 100 ms), the access points can defer off-channel measurements. It also defers based on WLAN scan defer priority configurations.

Each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance.

RRM supports new mobility architecture for RF grouping that involves Mobility Controller (MC) and Mobility Agent (MA).

- Mobility Controller (MC)—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.
- Mobility Agent (MA)—The Mobility Agent is the component that maintains client mobility state machine for a mobile client.

Information About RF Groups

An RF group is a logical collection of Cisco WLCs that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering Cisco WLCs into a single RF group enable the RRM algorithms to scale beyond the capabilities of a single Cisco WLC.

RF group is created based on following parameters:

- User-configured RF network name.
- Neighbor discovery performed at the radio level.
- Country list configured on MC.

RF grouping runs between MCs.

Lightweight access points periodically send out neighbor messages over the air. Access points using the the same RF group name validate messages from each other.

When access points on different Cisco WLCs hear validated neighbor messages at a signal strength of –80 dBm or stronger, the Cisco WLCs dynamically form an RF neighborhood in auto mode. In static mode, the leader is manually selected and the members are added to the RF Group. To know more about RF Group modes, RF Group Leader.

Note RF groups and mobility groups are similar in that they both define clusters of Cisco WLCs, but they are different in terms of their use. An RF group facilitates scalable, system-wide dynamic RF management while a mobility group facilitates scalable, system-wide mobility and Cisco WLC redundancy.

RF Group Leader

Starting in the 7.0.116.0 release, the RF Group Leader can be configured in two ways as follows:

- Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).
- Static Mode—In this mode, the user selects a Cisco WLC as an RF group leader manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF group, the reason is indicated. The leader tries to establish a connection with a member every 1 minute if the member has not joined in the previous attempt.

The RF group leader analyzes real-time radio data collected by the system, calculates the power and channel assignments, and sends them to each of the Cisco WLCs in the RF group. The RRM algorithms ensure system-wide stability and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

In Cisco WLC software releases prior to 6.0, the dynamic channel assignment (DCA) search algorithm attempts to find a good channel plan for the radios associated to Cisco WLCs in the RF group, but it does not adopt a new channel plan unless it is considerably better than the current plan. The channel metric of the worst radio in both plans determines which plan is adopted. Using the worst-performing radio as the single criterion for adopting a new channel plan can result in pinning or cascading problems.

Pinning occurs when the algorithm could find a better channel plan for some of the radios in an RF group but is prevented from pursuing such a channel plan change because the worst radio in the network does not have any better channel options. The worst radio in the RF group could potentially prevent other radios in the group from seeking better channel plans. The larger the network, the more likely pinning becomes.

Cascading occurs when one radio's channel change results in successive channel changes to optimize the remaining radios in the RF neighborhood. Optimizing these radios could lead to their neighbors and their neighbors' neighbors having a suboptimal channel plan and triggering their channel optimization. This effect could propagate across multiple floors or even multiple buildings, if all the access point radios belong to the same RF group. This change results in considerable client confusion and network instability.

The main cause of both pinning and cascading is the way in which the search for a new channel plan is performed and that any potential channel plan changes are controlled by the RF circumstances of a single radio. In Cisco WLC software release 6.0, the DCA algorithm has been redesigned to prevent both pinning and cascading. The following changes have been implemented:

- Multiple local searches—The DCA search algorithm performs multiple local searches initiated by different radios within the same DCA run rather than performing a single global search driven by a single radio. This change addresses both pinning and cascading while maintaining the desired flexibility and adaptability of DCA and without jeopardizing stability.
- Multiple channel plan change initiators (CPCIs)—Previously, the single worst radio was the sole initiator of a channel plan change. Now each radio within the RF group is evaluated and prioritized as a potential initiator. Intelligent randomization of the resulting list ensures that every radio is eventually evaluated, which eliminates the potential for pinning.
- Limiting the propagation of channel plan changes (Localization)—For each CPCI radio, the DCA algorithm performs a local search for a better channel plan, but only the CPCI radio itself and its one-hop neighboring access points are actually allowed to change their current transmit channels. The impact of an access point triggering a channel plan change is felt only to within two RF hops from that access point, and the actual channel plan changes are confined to within a one-hop RF neighborhood. Because this limitation applies across all CPCI radios, cascading cannot occur.

- Non-RSSI-based cumulative cost metric—A cumulative cost metric measures how well an entire region, neighborhood, or network performs with respect to a given channel plan. The individual cost metrics of all access points in that area are considered in order to provide an overall understanding of the channel plan's quality. These metrics ensure that the improvement or deterioration of each single radio is factored into any channel plan change. The objective is to prevent channel plan changes in which a single radio improves but at the expense of multiple other radios experiencing a considerable performance decline.

The RRM algorithms run at a specified updated interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keepalive messages to each of the RF group members and collects real-time RF data.

Note Several monitoring intervals are also available. See the Configuring RRM section for details.

RF Group Name

A Cisco WLC is configured with an RF group name, which is sent to all access points joined to the Cisco WLC and used by the access points as the shared secret for generating the hashed MIC in the neighbor messages. To create an RF group, you configure all of the Cisco WLCs to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a Cisco WLC may hear RF transmissions from an access point on a different Cisco WLC, you should configure the Cisco WLCs with the same RF group name. If RF transmissions between access points can be heard, then system-wide RRM is recommended to avoid 802.11 interference and contention as much as possible.

Mobility Controller

An MC can either be a group leader or a group member. One of the MCs can act as a RF group leader based on RF grouping and RF group election with other MCs. The order of priority to elect the RF leader is based on the maximum number of APs the controller or switch can support. The highest priority being 1 and the least being 5.

1 WiSM 2 Controllers

2 Cisco WLC 5700 Series Controllers

3 WiSM 1 Controllers

4 Catalyst 3850 Series Switches

5 Catalyst 3650 Series Switches

When one of the MCs becomes the RRM group leader, the remaining MCs become RRM group members. RRM group members send their RF information to the Group Leader. The group leader determines a channel and Tx power plan for the network and passes the information back to the RF group members. The MCs push the power plan to MA for the radios that belong to MA. These channel and power plans are ultimately pushed down to individual radios.

Note MC has MA functionality within it.

Mobility Agent

The MA communicates with the MC. The MC includes MAC or IP address of the switch/controller while communicating with the MA.

The MA provides the following information when polled by the MC:

- Interference or noise data.
- Neighbor data.
- Radio capabilities (supported channels, power levels).
- Radio configuration (power, channel, channel width).
- Radar data.

The MC exchanges the following information with the switch/controller (MA). The message includes:

- Configurations (channel/power/channel width) for individual radios.
- Polling requests for current configurations and RF measurements for individual radios
- Group Leader Update

In turn, the MA communicates the following messages with the MC:

- RF measurements from radios (e.g. load, noise and neighbor information)
- RF capabilities and configurations of individual radios

The MA sets channel, power, and channel width on the radios when directed by the MC. The DFS, coverage hole detection/mitigation, static channel/power configurations are performed by the MA.

Information About Rogue Access Point Detection in RF Groups

After you have created an RF group of Cisco WLCs, you need to configure the access points connected to the Cisco WLCs to detect rogue access points. The access points will then select the beacon/probe-response frames in neighboring access point messages to see if they contain an authentication information element (IE) that matches that of the RF group. If the select is successful, the frames are authenticated. Otherwise, the authorized access point reports the neighboring access point as a rogue, records its BSSID in a rogue table, and sends the table to the Cisco WLC.

Transmit Power Control

The switch dynamically controls access point transmit power based on real-time wireless LAN conditions.

The Transmit Power Control (TPC) algorithm both increases and decreases an access point's power in response to changes in the RF environment. In most instances, TPC seeks to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm balances RF power in many diverse RF environments. However, it is possible that automatic power control will not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions—for example, when all access points must be mounted in a central hallway, placing the access points close together, but requiring coverage out to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply to all access points through RF profiles in a RF network.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment, enter the maximum and minimum transmit power used by RRM in the text boxes in the Tx Power Control page. The range for these parameters is -10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point attached to the switch to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually.

Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading e-mail in a café affects the performance of the access point in a neighboring business. Even though these are completely separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Switches can dynamically allocate access point channel assignments to avoid conflict and to increase capacity and performance. Channels are “reused” to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the café, which is more effective than not using channel 1 altogether.

The switch’s Dynamic Channel Assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot both simultaneously use 11/54 Mbps. By effectively reassigning channels, the switch keeps adjacent channels separated.

Note We recommend that you use only non-overlapping channels (1, 6, 11, and so on).

The switch examines a variety of real-time RF characteristics to efficiently handle channel assignments as follows:

- Access point received energy—The received signal strength measured between each access point and its nearby neighboring access points. Channels are optimized for the highest network capacity.
- Noise—Noise can limit signal quality at the client and access point. An increase in noise reduces the effective cell size and degrades user experience. By optimizing channels to avoid noise sources, the switch can optimize coverage while maintaining system capacity. If a channel is unusable due to excessive noise, that channel can be avoided.

- 802.11 Interference—Interference is any 802.11 traffic that is not part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all channels looking for sources of interference. If the amount of 802.11 interference exceeds a predefined configurable threshold (the default is 10 percent), the access point sends an alert to the switch. Using the RRM algorithms, the switch may then dynamically rearrange channel assignments to increase system performance in the presence of the interference. Such an adjustment could result in adjacent lightweight access points being on the same channel, but this setup is preferable to having the access points remain on a channel that is unusable due to an interfering foreign access point.

  In addition, if other wireless networks are present, the switch shifts the usage of channels to complement the other networks. For example, if one network is on channel 6, an adjacent wireless LAN is assigned to channel 1 or 11. This arrangement increases the capacity of the network by limiting the sharing of frequencies. If a channel has virtually no capacity remaining, the switch may choose to avoid this channel. In very dense deployments in which all nonoverlapping channels are occupied, the switch does its best, but you must consider RF density when setting expectations.

- Load and utilization—When utilization monitoring is enabled, capacity calculations can consider that some access points are deployed in ways that carry more traffic than other access points (for example, a lobby versus an engineering area). The switch can then assign channels to improve the access point with the worst performance reported. The load is taken into account when changing the channel structure to minimize the impact on clients currently in the wireless LAN. This metric keeps track of every access point's transmitted and received packet counts to determine how busy the access points are. New clients avoid an overloaded access point and associate to a new access point. This parameter is disabled by default.

The switch combines this RF characteristic information with RRM algorithms to make system-wide decisions. Conflicting demands are resolved using soft-decision metrics that guarantee the best choice for minimizing network interference. The end result is optimal channel configuration in a three-dimensional space, where access points on the floor above and below play a major factor in an overall wireless LAN configuration.

Note Radios using 40-MHz channels in the 2.4-GHz band or or 80MHz channels are not supported by DCA.

The RRM startup mode is invoked in the following conditions:

- In a single-switch environment, the RRM startup mode is invoked after the switch is rebooted.
- In a multiple-switch environment, the RRM startup mode is invoked after an RF Group leader is elected.

You can trigger RRM startup mode from CLI.

RRM startup mode runs for 100 minutes (10 iterations at 10-minute intervals). The duration of the RRM startup mode is independent of the DCA interval, sensitivity, and network size. The startup mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady state channel plan. After the startup mode is finished, DCA continues to run at the specified interval and sensitivity.

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a “coverage hole” alert to the switch. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The switch discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the switch mitigates the coverage hole by increasing the transmit power level for that specific access point. The switch does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

How to Configure RRM

Configuring Advanced RRM CCX Parameters (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm ccx location-measurement** *interval*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm ccx location-measurement** *interval* **Example:** `Switch(config)# ap dot11 24ghz rrm ccx location-measurement 15`	Configures the interval for 802.11 CCX client location measurements. The range is from 10 to 32400 seconds.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Neighbor Discovery Type (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm ndp-type** {**protected | transparent**}
3. **end**

DETAILED STEPS

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

Step 2	**ap dot11 24ghz | 5ghz rrm ndp-type** {**protected | transparent**}
	
	Example:
	`Switch(config)#ap dot11 24ghz rrm ndp-type protected`
	`Switch(config)#ap dot11 24ghz rrm ndp-type transparent`
		Configures the neighbor discovery type. By default, the mode is set to "transparent".
		• **protected—**Sets the neighbor discover type to protected. Packets are encrypted.
		• **transparent—**Sets the neighbor discover type to transparent. Packets are sent as is.

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

Configuring RRM Profile Thresholds, Monitoring Channels, and Monitoring Intervals (GUI)

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

Step 2 Configure profile thresholds used for alarming as follows:

Note The profile thresholds have no bearing on the functionality of the RRM algorithms. Switches send an SNMP trap (or an alert) to the Cisco Prime Infrastructure or another trap receiver when individual APs values set for these threshold parameters are exceeded.

a) In the **Interference** text box, enter the percentage of interference (802.11 traffic from sources outside of your wireless network) on a single access point. The valid range is 0 to 100%, and the default value is 10%.

b) In the **Clients** text box, enter the number of clients on a single access point. The valid range is 1 to 75, and the default value is 12.

c) In the **Noise** text box, enter the level of noise (non-802.11 traffic) on a single access point. The valid range is –127 to 0 dBm, and the default value is –70 dBm.

d) In the **Utilization** text box, enter the percentage of RF bandwidth being used by a single access point. The valid range is 0 to 100%, and the default value is 80%.

e) In the **Throughput** text box, enter the level of Throughput being used by a single access point. The valid range is 1000 to 10000000, and the default value is 1000000.

Step 3 From the **Channel List** drop-down list, choose one of the following options to specify the set of channels that the access point uses for RRM scanning:

- **All Channels—**RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.
- **Country Channels—**RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
- **DCA Channels—**RRM channel scanning occurs only on the channel set used by the DCA algorithm, which by default includes all of the non-overlapping channels allowed in the country of operation. However, you can specify the channel set to be used by DCA if desired. To do so, follow instructions in the Dynamic Channel Assignment.

Step 4 Configure monitor intervals as follows:

1 In the **Channel Scan Interval** text box, enter (in seconds) the sum of the time between scans for each channel within a radio band. The entire scanning process takes 50 ms per channel, per radio and runs at the interval configured here. The time spent listening on each channel is determined by the non-configurable 50-ms scan time and the number of channels to be scanned. For example, in the U.S. all 11 802.11b/g channels are scanned for 50 ms each within the default 180-second interval. So every 16 seconds, 50 ms is spent listening on each scanned channel (180/11 = ~16 seconds). The Channel Scan Interval parameter determines the interval at which the scanning occurs. The valid range is 60 to 3600 seconds, and the default value for 802.11a/n/ac and 802.11b/g/n radios is 180 seconds.

2 In the **Neighbor Packet Frequency** text box, enter (in seconds) how frequently neighbor packets (messages) are sent, which eventually builds the neighbor list. The valid range is 60 to 3600 seconds, and the default value is 60 seconds.

Note If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes, the Cisco WLC deletes that neighbor from the neighbor list.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Note Click **Set to Factory Default** if you want to return all of the Cisco WLC's RRM parameters to their factory-default values.

Configuring RF Groups

This section describes how to configure RF groups through either the GUI or the CLI.

Note The RF group name is generally set at deployment time through the Startup Wizard. However, you can change it as necessary.

Note When the multiple-country feature is being used, all Cisco WLCs intended to join the same RF group must be configured with the same set of countries, configured in the same order.

Note You can also configure RF groups using the Cisco Prime Infrastructure.

Configuring the RF Group Mode (GUI)

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **RF Grouping** or or **Configuration** > **Wireless** > **802.11b/g/n** > **RRM** > **RF Grouping** to open the RF Grouping page.

Step 2 From the **Group Mode** drop-down list, choose the mode that you want to configure for this Cisco WLC.
You can configure RF grouping in the following modes:

- auto—Sets the RF group selection to automatic update mode.

  Note A configured static leader cannot become a member of another RF group until its mode is set to "auto".

- leader—Sets the RF group selection to static mode, and sets this Cisco WLC as the group leader.
- off—Sets the RF group selection off. Every Cisco WLC optimizes its own access point parameters.

  Note A Cisco WLC with a lower priority cannot assume the role of a group leader if a Cisco WLC with a higher priority is available. Here, priority is related to the processing power of the Cisco WLC.

  Note We recommend that Cisco WLCs participate in automatic RF grouping. You can override RRM settings without disabling automatic RF group participation.

Step 3 Click **Apply** to save the configuration and click **Restart** to restart the RRM RF Grouping algorithm.

Step 4 If you configured RF Grouping mode for this Cisco WLC as a static leader, you can add group members from the Group Members section as follows:

1. In the switch Name text box, enter the Cisco WLC that you want to add as a member to this group.
2. In the IP Address text box, enter the IP address of the Cisco WLC.
3. Click **Add** to add the member to this group.

   Note If the member has not joined the static leader, the reason of the failure is shown in parentheses.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring RF Group Selection Mode (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm group-mode**{**auto | leader | off**}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz	5ghz rrm group-mode**{**auto	leader	off**} **Example:** `Switch(config)#ap dot11 24ghz rrm group-mode leader`	Configures RF group selection mode for 802.11 bands. • **auto—**Sets the 802.11 RF group selection to automatic update mode. • **leader—**Sets the 802.11 RF group selection to leader mode. • **off—**Disables the 802.11 RF group selection.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RF Group Name (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wireless rf-network** *name*
3. **end**
4. **show network profile** *profile_number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless rf-network** *name* **Example:** `Switch (config)# wireless rf-network test1`	Creates an RF group. The group name should be ASCII String up to 19 characters and is case sensitive. **Note** Repeat this procedure for each controller that you want to include in the RF group.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 4	**show network profile** *profile_number*	Displays the RF group. **Note** You can view the network profile number from 1 to 4294967295.

Configuring an RF Group Name (GUI)

Step 1 Choose **Configuration** > **Controller** > **General** to open the General page.

Step 2 Enter a name for the RF group in the RF Group Name text box. The name can contain up to 19 ASCII characters and is case sensitive.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Step 5 Repeat this procedure for each controller that you want to include in the RF group.

Configuring Members in a 802.11 Static RF Group (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr* **Example:** `Switch(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1`	Configures members in a 802.11 static RF group. The group mode should be set as leader for the group member to be active.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Transmit Power Control

Configuring the Tx-Power Control Threshold (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm tpc-threshold -60`	Configures the Tx-power control threshold used by RRM for auto power assignment. The range is from –80 to –50.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the Tx-Power Level (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm txpower**{*trans_power_level* | **auto** | **max** | **min** | **once**}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm txpower**{*trans_power_level* | **auto** | **max** | **min** | **once**} **Example:** `Switch(config)#ap dot11 24ghz rrm txpower auto`	Configures the 802.11 tx-power level • **trans_power_level—**Sets the transmit power level. • **auto—**Enables auto-RF. • **max—**Configures the maximum auto-RF tx-power. • **min—**Configures the minimum auto-RF tx-power. • **once—**Enables one-time auto-RF.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Transmit Power Control (GUI)

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **TPC** or **Configuration** > **Wireless** > **802.11b/g/n** > **RRM** > **TPC** to open RRM Tx Power Control (TPC) page.

Step 2 Choose the Transmit Power Control.
Coverage Optimal Mode (TPCv1)— Offers strong signal coverage and stability. In this mode, power can be kept low to gain extra capacity and reduce interference.

Step 3 Choose one of the following options from the Power Level Assignment Method list to specify the Cisco WLC's dynamic power assignment mode:

- **Automatic—**Causes the Cisco WLC to periodically evaluate and, if necessary, update the transmit power for all joined access points. This is the default value.
- **On Demand—**Causes the Cisco WLC to periodically evaluate the transmit power for all joined access points. However, the Cisco WLC updates the power, if necessary, only when you click **Apply** after choosing **On Demand**.

  Note The Cisco WLC does not evaluate and update the transmit power immediately when you click **Apply** after choosing **On Demand**. It waits for the next 600-second interval. This value is not configurable.
- **Fixed—**Prevents the Cisco WLC from evaluating and, if necessary, updating the transmit power for joined access points. The power level is set to the fixed value chosen from the drop-down list. The corresponding option for **Fixed** when you try to configure from CLI is **once**.

  Note The transmit power level is assigned an integer value instead of a value in mW or dBm. The integer corresponds to a power level that varies depending on the regulatory domain, channel, and antennas in which the access points are deployed.

  Note For optimal performance, we recommend that you use the Automatic setting.

Step 4 Enter the maximum and minimum power level assignment values in the Maximum Power Level Assignment and Minimum Power Level Assignment text boxes.
The range for the Maximum Power Level Assignment is –10 to 30 dBm.

The range for the Minimum Power Level Assignment is –10 to 30 dBm.

Step 5 In the Power Threshold text box, enter the cutoff signal level used by RRM when determining whether to reduce an access point's power. The default value for this parameter is –70 dBm for TPCv1, but can be changed when access points are transmitting at higher (or lower) than desired power levels.
The range for this parameter is –80 to –50 dBm. Increasing this value (between –65 and –50 dBm) causes the access points to operate at a higher transmit power. Decreasing the value has the opposite effect.

In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

This page also shows the following nonconfigurable transmit power level parameter settings:

- Power Neighbor Count—The minimum number of neighbors an access point must have for the transmit power control algorithm to run.

- Power Assignment Leader—The MAC address of the RF group leader, which is responsible for power level assignment.
- Last Power Level Assignment—The last time RRM evaluated the current transmit power level assignments.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Configuring 802.11 RRM Parameters

Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm channel cleanair-event sensitivity** {**high | low | medium**}
3. **ap dot11 24ghz | 5ghz rrm channel dca**{*channel number*| **anchor-time | global**{**auto| once**}| **interval | min-metric | sensitivity**{**high | low | medium**}}
4. **ap dot11 5ghz rrm channel dca chan-width-11n** {**20** | **40**}
5. **ap dot11 24ghz | 5ghz rrm channel device**
6. **ap dot11 24ghz | 5ghz rrm channel foreign**
7. **ap dot11 24ghz | 5ghz rrm channel load**
8. **ap dot11 24ghz | 5ghz rrm channel noise**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm channel cleanair-event sensitivity** {**high | low | medium**} **Example:** `Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures CleanAir event-driven RRM parameters. • **High–**Specifies the most sensitivity to non-Wi-Fi interference as indicated by the air quality (AQ) value. • **Low–**Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value. • **Medium–**Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.

	Command or Action	Purpose
Step 3	**ap dot11 24ghz | 5ghz rrm channel dca**{*channel number*| **anchor-time | global**{**auto**| **once**}| **interval | min-metric | sensitivity**{**high | low | medium**}} **Example:** `Switch(config)#ap dot11 24ghz rrm channel dca interval 2`	Configures Dynamic Channel Assignment (DCA) algorithm parameters for the 802.11 band. • ***<1-14>*–**Enter a channel number to be added to the DCA list. • **anchor-time–**Configures the anchor time for the DCA. The range is between 0 and 23 hours. • **global–**Configures the DCA mode for all 802.11 Cisco APs. ◦ **auto–**Enables auto-RF. ◦ **once–**Enables auto-RF only once. • **interval–**Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes. • **min-metric–**Configures the DCA minimum RSSI energy metric. The range is between -100 and -60. • **sensitivity–**Configures the DCA sensitivity level to changes in the environment. ◦ **high–**Specifies the most sensitivity. ◦ **low–**Specifies the least sensitivity. ◦ **medium–**Specifies medium sensitivity.
Step 4	**ap dot11 5ghz rrm channel dca chan-width-11n** {**20** | **40**}	Configures the DCA channel width for all 802.11n radios in the 5-GHz band. • 20 sets the channel width for 802.11n radios to 20 MHz. This is the default value. • 40 sets the channel width for 802.11n radios to 40 MHz.
Step 5	**ap dot11 24ghz | 5ghz rrm channel device** **Example:** `Switch(config)#ap dot11 24ghz rrm channel device`	Configures the persistent non-Wi-Fi device avoidance in the 802.11 channel assignment.
Step 6	**ap dot11 24ghz | 5ghz rrm channel foreign** **Example:** `Switch(config)#ap dot11 24ghz rrm channel foreign`	Configures the foreign AP 802.11 interference avoidance in the channel assignment.

	Command or Action	Purpose
Step 7	**ap dot11 24ghz | 5ghz rrm channel load** **Example:** `Switch(config)#ap dot11 24ghz rrm channel load`	Configures the Cisco AP 802.11 load avoidance in the channel assignment.
Step 8	**ap dot11 24ghz | 5ghz rrm channel noise** **Example:** `Switch(config)#ap dot11 24ghz rrm channel noise`	Configures the 802.11 noise avoidance in the channel assignment.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Dynamic Channel Assignment (GUI)

You can specify the channels that the Dynamic Channel Assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning by using the Cisco WLC GUI.

Note This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

Step 1 Disable the 802.11a/n/ac or 802.11b/g/n network as follows:

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

b) Unselect the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.

c) Click **Apply**.

Step 2 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **DCA** or **Configuration** > **Wireless** > **802.11b/g/n** > **RRM** > **DCA** to open the Dynamic Channel Assignment (DCA) page.

Step 3 Choose one of the following options from the **Channel Assignment Method** drop-down list to specify the Cisco WLC's DCA mode:

- **Automatic—**Causes the Cisco WLC to periodically evaluate and, if necessary, update the channel assignment for all joined access points. This is the default value.
- **Freeze—**Causes the Cisco WLC to evaluate and update the channel assignment for all joined access points, if necessary, only when you click **Apply** after selecting the **Freeze** option.

  Note The Cisco WLC does not evaluate and update the channel assignment immediately when you click **Apply** after selecting the **Freeze** option. It waits for the next interval to elapse.

- **OFF—**Turns off DCA and sets all access point radios to the first channel of the band. If you choose this option, you must manually assign channels on all radios.

  Note For optimal performance, we recommend that you use the Automatic setting. See the Disabling Dynamic Channel and Power Assignment (GUI) section for instructions on how to disable the Cisco WLC's dynamic channel and power settings.

Step 4 From the Interval drop-down list, choose one of the following options to specify how often the DCA algorithm is allowed to run: **10 minutes**, **1 hour**, **2 hours**, **3 hours**, **4 hours**, **6 hours**, **8 hours**, **12 hours**, or **24 hours**. The default value is 10 minutes.

Step 5 From the AnchorTime drop-down list, choose a number to specify the time of day when the DCA algorithm is to start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

Step 6 From the **DCA Channel Sensitivity** drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- **Low—**The DCA algorithm is not particularly sensitive to environmental changes.
- **Medium—**The DCA algorithm is moderately sensitive to environmental changes.
- **High—**The DCA algorithm is highly sensitive to environmental changes.

The default value is Medium. The DCA sensitivity thresholds vary by radio band, as noted in the following table:

Table 5: DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

Step 7 This page also shows the following nonconfigurable channel parameter settings:

- Channel Assignment Leader—The MAC address of the RF group leader, which is responsible for channel assignment.

Step 8 In the DCA Channel List area, the DCA Channels text box shows the channels that are currently selected. To choose a channel, select its check box in the Select column. To exclude a channel, unselect its check box.
The ranges are as follows:

- 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165 (depending on countries).
- 802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 (depending on countries).

The defaults are as follows:

- 802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161

- 802.11b/g—1, 6, 11

Step 9 Click **Apply**.

Step 10 Reenable the 802.11 networks as follows:

1. Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **Network** or **Configuration** > **Wireless** > **802.11b/g/n** > **Network** to open the Global Parameters page.
2. Select the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.
3. Click **Apply**.

Step 11 Click **Save Configuration**.

Configuring 802.11 Coverage Hole Detection (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**}
3. **ap dot11 24ghz | 5ghz rrm coverage exception global** *exception level*
4. **ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min exception level*
5. **ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} **Example:** `Switch(config)#ap dot11 24ghz rrm coverage data fail-percentage 60`	Configures the 802.11 coverage hole detection for data packets. • **fail-percentage**—Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%. • **packet-count**—Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255. • **rssi-threshold**—Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm.

	Command or Action	Purpose
Step 3	**ap dot11 24ghz | 5ghz rrm coverage exception global** *exception level* **Example:** `Switch(config)#ap dot11 24ghz rrm coverage exception global 50`	Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.
Step 4	**ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min exception level* **Example:** `Switch(config)#ap dot11 24ghz rrm coverage level global 10`	Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.
Step 5	**ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} **Example:** `Switch(config)#ap dot11 24ghz rrm coverage voice packet-count 10`	Configures the 802.11 coverage hole detection for voice packets. • **fail-percentage—**Configures the 802.11 coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%. • **packet-count—**Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255. • **rssi-threshold—**Configures the 802.11 minimum receive coverage level for voice packets that range from –90 to –60 dBm.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Coverage Hole Detection (GUI)

Step 1 Disable the 802.11 network as follows:

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

b) Unselect the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.

c) Click **Apply**.

Step 2 Choose **Configuration** > **Wireless** > **802.11a/n/ac** > **RRM** > **Coverage Thresholds** or **Configuration** > **Wireless** > **802.11b/g/n** > **RRM** > **Coverage Thresholds** to open coverage page.

Step 3 Select the **Enable Coverage Hole Detection** check box to enable coverage hole detection, or unselect it to disable this feature. If you enable coverage hole detection, the Cisco WLC automatically determines, based on data received from the access points, if any access points have clients that are potentially located in areas with poor coverage. The default value is selected.

Step 4 In the **Data RSSI** text box, enter the minimum Receive Signal Strength Indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm. The access point takes data RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

Step 5 In the **Voice RSSI** text box, enter the minimum Receive Signal Strength Indication (RSSI) value for voice packets received by the access point. The value that you enter is used to identify coverage holes within your network. If the access point receives a packet in the voice queue with an RSSI value below the value that you enter here, a potential coverage hole has been detected. The valid range is –90 to –60 dBm, and the default value is –80 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.

Step 6 In the **Min Failed Client Count per AP** text box, enter the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The valid range is 1 to 75, and the default value is 3.

Step 7 In the **Coverage Exception Level per AP** text box, enter the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The valid range is 0 to 100%, and the default value is 25%.

Note If both the number and percentage of failed packets exceed the values configured for Failed Packet Count and Failed Packet Percentage (configurable through the Cisco WLC CLI) for a 5-second period, the client is considered to be in a pre-alarm condition. The Cisco WLC uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the Min Failed Client Count per AP and Coverage Exception Level per AP text boxes over two 90-second periods (a total of 180 seconds). The Cisco WLC determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Step 8 Click **Apply**.

Step 9 Reenable the 802.11 network as follows:

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

b) Select the **802.11a/n/ac** (or **802.11b/g/n**) **Network Status** check box.

c) Click **Apply**.

Step 10 Click **Save Configuration**.

Configuring 802.11 Event Logging (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm logging**{**channel | coverage | foreign | load | noise | performance | txpower**}
3. **end**

DETAILED STEPS

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

Step 2	**ap dot11 24ghz | 5ghz rrm logging**{**channel | coverage | foreign | load | noise | performance | txpower**}
	
	Example:
	`Switch(config)#ap dot11 24ghz rrm logging channel`
	`Switch(config)#ap dot11 24ghz rrm logging coverage`
	`Switch(config)#ap dot11 24ghz rrm logging foreign`
	`Switch(config)#ap dot11 24ghz rrm logging load`
	`Switch(config)#ap dot11 24ghz rrm logging noise`
	`Switch(config)#ap dot11 24ghz rrm logging performance`
	`Switch(config)#ap dot11 24ghz rrm logging txpower`
		Configures event-logging for various parameters.
		• **channel—**Configures the 802.11 channel change logging mode.
		• **coverage—**Configures the 802.11 coverage profile logging mode.
		• **foreign—**Configures the 802.11 foreign interference profile logging mode.
		• **load—**Configures the 802.11 load profile logging mode.
		• **noise—**Configures the 802.11 noise profile logging mode.
		• **performance—**Configures the 802.11 performance profile logging mode.
		• **txpower—**Configures the 802.11 transmit power change logging mode.

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

Configuring 802.11 Statistics Monitoring (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**}
3. **ap dot11 24ghz | 5ghz rrm monitor coverage** *interval*
4. **ap dot11 24ghz | 5ghz rrm monitor load** *interval*
5. **ap dot11 24ghz | 5ghz rrm monitor noise** *interval*
6. **ap dot11 24ghz | 5ghz rrm monitor signal** *interval*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} **Example:** `Switch(config)#ap dot11 24ghz rrm monitor channel-list all`	Sets the 802.11 monitoring channel-list for parameters such as noise/interference/rogue. • **all—** Monitors all channels. • **country—** Monitor channels used in configured country code. • **dca—** Monitor channels used by dynamic channel assignment.
Step 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor coverage 600`	Configures the 802.11 coverage measurement interval in seconds that ranges from 60 to 3600.
Step 4	**ap dot11 24ghz | 5ghz rrm monitor load** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor load 180`	Configures the 802.11 load measurement interval in seconds that ranges from 60 to 3600.
Step 5	**ap dot11 24ghz | 5ghz rrm monitor noise** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor noise 360`	Configures the 802.11 noise measurement interval (channel scan interval) in seconds that ranges from 60 to 3600.

	Command or Action	Purpose
Step 6	**ap dot11 24ghz | 5ghz rrm monitor signal** *interval* **Example:** `Switch(config)#ap dot11 24ghz rrm monitor signal 480`	Configures the 802.11 signal measurement interval (neighbor packet frequency) in seconds that ranges from 60 to 3600.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the 802.11 Performance Profile (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value*
3. **ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value*
4. **ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value*
5. **ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value*
6. **ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile clients 20`	Sets the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.

	Command or Action	Purpose
Step 3	**ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile foreign 50`	Sets the threshold value for 802.11 foreign interference that ranges between 0 and 100%.
Step 4	**ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile noise -65`	Sets the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.
Step 5	**ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile throughput 10000`	Sets the threshold value for 802.11 Cisco AP throughput that ranges between 1000 and 10000000 bytes per second.
Step 6	**ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value* **Example:** `Switch(config)#ap dot11 24ghz rrm profile utilization 75`	Sets the threshold value for 802.11 RF utilization that ranges between 0 to 100%.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

Before You Begin

Ensure that each Cisco WLC in the RF group has been configured with the same RF group name.

Note The name is used to verify the authentication IE in all beacon frames. If the Cisco WLCs have different names, false alarms will occur.

SUMMARY STEPS

1. **ap name** *Cisco_AP* **mode** {**local** | **monitor**}
2. **end**
3. **configure terminal**
4. **wireless wps ap-authentication**
5. **wireless wps ap-authentication threshold** *value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode** {**local** | **monitor**} **Example:** `Switch# ap name ap1 mode local`	Configures a particular access point for local (normal) mode or monitor (listen-only) mode. Perform this step for every access point connected to the Cisco WLC.
Step 2	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 4	**wireless wps ap-authentication** **Example:** `Switch (config)# wireless wps ap-authentication`	Enables rogue access point detection.
Step 5	**wireless wps ap-authentication threshold** *value* **Example:** `Switch (config)# wireless wps ap-authentication threshold 50`	Specifies when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period. The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value. **Note** Enable rogue access point detection and threshold value on every Cisco WLC in the RF group. **Note** If rogue access point detection is not enabled on every Cisco WLC in the RF group, the access points on the Cisco WLCs with this feature disabled are reported as rogues.

Enabling Rogue Access Point Detection in RF Groups (GUI)

Step 1 Make sure that each Cisco WLC in the RF group has been configured with the same RF group name.
Note The name is used to verify the authentication IE in all beacon frames. If the Cisco WLCs have different names, false alarms will occur.

Step 2 Choose **Configuration** > **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 3 Click the name of an access point to open the All APs > Edit page.

Step 4 Choose either **local** or **monitor** from the AP Mode drop-down list and click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Step 6 Repeat Step 2 through Step 5 for every access point connected to the Cisco WLC.

Step 7 Choose **Configuration** > **Security** > **Wireless Protection Policies** > **AP Authentication/MFP** to open the AP Authentication Policy page.
The name of the RF group to which this Cisco WLC belongs appears at the top of the page.

Step 8 Choose **AP Authentication** from the Protection Type drop-down list to enable rogue access point detection.

Step 9 Enter a number in the Alarm Trigger Threshold edit box to specify when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.
Note The valid threshold range is from1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Step 12 Repeat this procedure on every Cisco WLC in the RF group.
Note If rogue access point detection is not enabled on every Cisco WLC in the RF group, the access points on the Cisco WLCs with this feature disabled are reported as rogues.

Monitoring RRM Parameters and RF Group Status

Monitoring RRM Parameters

Table 6: Commands for monitoring Radio Resource Management

Commands	Description
show ap dot11 24ghz ccx	Displays the 802.11b CCX information for all Cisco APs.
show ap dot11 24ghz channel	Displays the configuration and statistics of the 802.11b channel assignment.
show ap dot11 24ghz coverage	Displays the configuration and statistics of the 802.11b coverage.

Commands	Description
show ap dot11 24ghz group	Displays the configuration and statistics of the 802.11b grouping.
show ap dot11 24ghz l2roam	Displays 802.11b l2roam information.
show ap dot11 24ghz logging	Displays the configuration and statistics of the 802.11b event logging.
show ap dot11 24ghz monitor	Displays the configuration and statistics of the 802.11b monitoring.
show ap dot11 24ghz profile	Displays 802.11b profiling information for all Cisco APs.
show ap dot11 24ghz receiver	Displays the configuration and statistics of the 802.11b receiver.
show ap dot11 24ghz summary	Displays the configuration and statistics of the 802.11b Cisco APs.
show ap dot11 24ghz txpower	Displays the configuration and statistics of the 802.11b transmit power control.
show ap dot11 5ghz ccx	Displays 802.11a CCX information for all Cisco APs.
show ap dot11 5ghz channel	Displays the configuration and statistics of the 802.11a channel assignment.
show ap dot11 5ghz coverage	Displays the configuration and statistics of the 802.11a coverage.
show ap dot11 5ghz group	Displays the configuration and statistics of the 802.11a grouping.
show ap dot11 5ghz l2roam	Displays 802.11a l2roam information.
show ap dot11 5ghz logging	Displays the configuration and statistics of the 802.11a event logging.
show ap dot11 5ghz monitor	Displays the configuration and statistics of the 802.11a monitoring.
show ap dot11 5ghz profile	Displays 802.11a profiling information for all Cisco APs.
show ap dot11 5ghz receiver	Displays the configuration and statistics of the 802.11a receiver.

Commands	Description
show ap dot11 5ghz summary	Displays the configuration and statistics of the 802.11a Cisco APs.
show ap dot11 5ghz txpower	Displays the configuration and statistics of the 802.11a transmit power control.

Monitoring RF Group Status (CLI)

This section describes the new commands for RF group status.

The following commands can be used to monitor RF group status on the switch.

Table 7: Monitoring Aggressive Load Balancing Command

Command	Purpose
show ap dot11 5ghz group	Displays the Cisco WLC name which is the RF group leader for the 802.11a RF network.
show ap dot11 24ghz group	Displays the Cisco WLC name which is the RF group leader for the 802.11b/g RF network.

Monitoring RF Group Status (GUI)

Step 1 Choose **Configuration** > **Wireless** > **802.11a/n** > **or 802.11b/g/n > RRM** > **RF Grouping** to open the RF Grouping Algorithm page.
This page shows the details of the RF group, displaying the configurable parameter **Group mode**, the **Group role** of this Cisco WLC, the **Group Update Interval** and the Cisco WLC name and IP address of the **Group Leader** to this Cisco WLC.

Note RF grouping mode can be set using the **Group Mode** drop-down list.

Tip Once a Cisco WLC has joined as a static member and you want to change the grouping mode, we recommend that you remove the member from the configured static-leader and also make sure that a member Cisco WLC has not been configured to be a member on multiple static leaders. This is to avoid repeated join attempts from one or more RF static leaders.

Step 2 (Optional) Repeat this procedure for the network type that you did not select (802.11a/n or 802.11b/g/n).

Examples: RF Group Configuration

This example shows how to configure RF group name:

```
Switch# configure terminal
Switch(config)# wireless rf-network test1
Switch(config)# ap dot11 24ghz shutdown
Switch(config)# end
Switch # show network profile 5
```

This example shows how to configure rogue access point detection in RF groups:

```
Switch# ap name ap1 mode local
Switch# end
Switch# configure terminal
Switch(config)# wireless wps ap-authentication
Switch(config)# wireless wps ap-authentication threshold 50
Switch(config)# end
```

Additional References for Radio Resource Management

Related Documents

Related Topic	Document Title
RRM commands and their details	*RRM Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

MIBs

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

Technical Assistance

Description	Link
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.	http://www.cisco.com/support

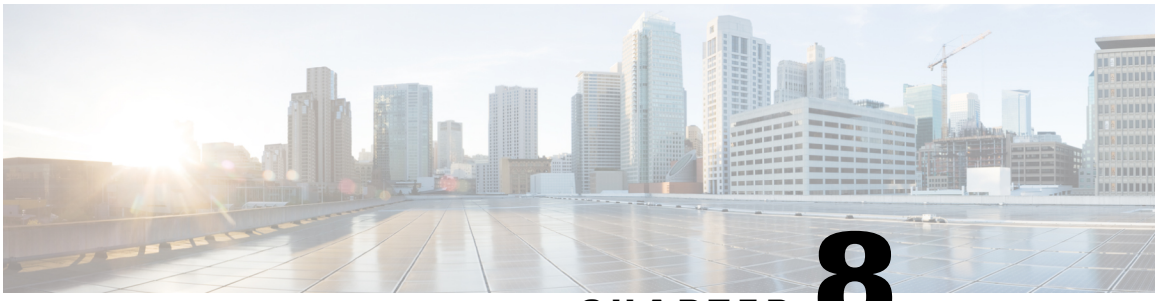
Feature History and Information For Performing Radio Resource Management Configuration

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

PART IV

Lightweight Access Points

- Configuring the Switch for Access Point Discovery, page 107
- Configuring Data Encryption, page 115
- Configuring Retransmission Interval and Retry Count, page 119
- Configuring Adaptive Wireless Intrusion Prevention System, page 123
- Configuring Authentication for Access Points, page 129
- Converting Autonomous Access Points to Lightweight Mode, page 139
- Using Cisco Workgroup Bridges, page 149
- Configuring Backup Switches and Failover Priority for Access Points, page 153
- Configuring Probe Request Forwarding, page 163
- Optimizing RFID Tracking, page 165
- Configuring Country Codes, page 169
- Configuring Link Latency, page 175
- Configuring Power over Ethernet, page 183



CHAPTER 8

Configuring the Switch for Access Point Discovery

- Finding Feature Information, page 107
- Prerequisites for Configuring the Switch for Access Point Discovery, page 107
- Restrictions for Configuring the Switch for Access Point Discovery, page 108
- Information About Configuring the Switch for Access Point Discovery, page 108
- How to Configure Access Point Discovery, page 110
- Configuration Examples for Configuring the Switch for Access Point Discovery, page 112

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 the Switch for Access Point Discovery

- Ensure that the Control and Provisioning of Wireless Access Points (CAPWAP) UDP ports 5246 and 5247 (similar to the Lightweight Access Point Protocol (LWAPP) UDP ports 12222 and 12223) are enabled and are not blocked by an intermediate device that could prevent an access point from joining the switch.
- If access control lists (ACLs) are in the control path between the switch and its access points, you must open new protocol ports to prevent access points from being stranded.
- If an access point is in the UP state and its IP address changes, the access point tears down the existing CAPWAP tunnel and rejoins the switch.

- Access points must be discovered by a switch before they can become an active part of the network. The lightweight access points support the following switch discovery processes:
  - Layer 3 CAPWAP discovery—You can enable this feature on different subnets from the access point. This feature uses IP addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
  - Locally stored switch IP address discovery—If the access point was previously associated to a switch, the IP addresses of the primary, secondary, and tertiary switchs are stored in the access point's nonvolatile memory. This process of storing switch IP addresses on an access point for later deployment is called *priming the access point*.
  - DHCP server discovery—This feature uses DHCP option 43 to provide switch IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.
  - DNS discovery—The access point can discover switchs through your domain name server (DNS). You must configure your DNS to return switch IP addresses in response to CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of switch IP addresses, the access point sends discovery requests to the switchs.

Restrictions for Configuring the Switch for Access Point Discovery

- Ensure that the switchs are configured with the correct date and time. If the date and time configured on the switch precedes the creation and installation date of certificates on the access points, the access point fails to join the switch.
- During the discovery process, access points that are supported by the Cisco switch, such as the 1140, 1260, 3500, 1040,1600, 2600, or 3600 query only for Cisco switchs.

Information About Configuring the Switch for Access Point Discovery

In a CAPWAP environment, a lightweight access point discovers a switch by using CAPWAP discovery mechanisms and then sends a CAPWAP join request to the switch. The switch sends a CAPWAP join response to the access point that allows the access point to join the switch. When the access point joins the switch, the switch manages its configuration, firmware, control transactions, and data transactions.

Access Point Communication Protocols

Cisco lightweight access points use the IETF standard CAPWAP to communicate with the switch and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a switch to manage a collection of wireless access points. CAPWAP is implemented in switch for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices

- To enable switchs to interoperate with third-party access points in the future

Viewing Access Point Join Information

Join statistics for an access point that sends a CAPWAP discovery request to the switch at least once are maintained on the switch even if the access point is rebooted or disconnected. These statistics are removed only when the switch is rebooted or when you choose to clear the statistics.

Troubleshooting the Access Point Join Process

Access points can fail to join a switch for many reasons such as a RADIUS authorization is pending, self-signed certificates are not enabled on the switch, the access point and switch's regulatory domains do not match, and so on.

You can configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the switch because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the switch until it receives a CAPWAP join request from the access point, so it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining issues without enabling CAPWAP debug commands on the switch, the switch collects information for all access points that send a discovery message to this switch and maintains information for any access points that have successfully joined this switch.

The switch collects all join-related information for each access point that sends a CAPWAP discovery request to the switch. Collection begins when the first discovery message is received from the access point and ends when the last configuration payload is sent from the switch to the access point.

When the switch is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

You can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

You can configure the syslog server IP address through the access point CLI, if the access point is not connected to the switch by entering the **capwap ap log-server** *syslog_server_IP_address* command.

When the access point joins a switch for the first time, the switch pushes the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address, until it is overridden by one of the following scenarios:

- The access point is still connected to the same switch, and you changed the global syslog server IP address configuration on the switch by using the **ap syslog host** *Syslog_Server_IP_Address* command. In this case, the switch pushes the new global syslog server IP address to the access point.
- The access point is still connected to the same switch, and you configured a specific syslog server IP address for the access point on the switch by using the **ap name** *Cisco_AP* **syslog host** *Syslog_Host_IP_Address* command. In this case, the switch pushes the new specific syslog server IP address to the access point.
- The access point gets disconnected from the switch, and you configured the syslog server IP address from the access point CLI by using the **capwap ap log-server** *syslog_server_IP_address* command. This command works only if the access point is not connected to any switch.
- The access point gets disconnected from the switch and joins another switch. In this case, the new switch pushes its global syslog server IP address to the access point.

Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address, if the access point can reach the syslog server IP address.

How to Configure Access Point Discovery

Configuring the Syslog Server for Access Points (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap syslog host** *host_ip_address*
4. **end**
5. **show ap config global**
6. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap syslog host** *host_ip_address* **Example:** `Switch(config)# ap syslog host 10.9.9.16`	Configures the global syslog server for all access points that join this switch. **Note** By default, the global syslog server IP address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the switch. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
Step 5	**show ap config global** **Example:** `Switch# show ap config global`	Displays the global syslog server settings for all access points that join the switch.
Step 6	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP03 config general`	Displays the syslog server settings for a specific access point.

Monitoring Access Point Join Information (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **show ap join stats summary**
3. **show ap mac-address** *mac_address* **join stats summary**
4. **show ap mac-address** *mac_address* **join stats detailed**
5. **clear ap join statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show ap join stats summary** **Example:** `Switch# show ap join stats summary`	Displays the MAC addresses of all the access points that are joined to the switch or that have tried to join.
Step 3	**show ap mac-address** *mac_address* **join stats summary** **Example:** `Switch# show ap mac-address 000.2000.0400 join stats summary`	Displays all the statistics for the AP including the last join error detail.

	Command or Action	Purpose
Step 4	**show ap mac-address** *mac_address* **join stats detailed** **Example:** `Switch# show ap mac-address 000.2000.0400 join stats detailed`	Displays all join-related statistics collected for a specific access point.
Step 5	**clear ap join statistics** **Example:** `Switch# clear ap join statistics`	Clears the join statistics for all access points. **Note** To clear the join statistics that correspond to specific access points, enter the **clear ap mac-address** *mac_address* **join statistics** command.

Related Topics

Displaying the MAC Addresses of all Access Points: Example, on page 112

DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example, on page 113

Configuration Examples for Configuring the Switch for Access Point Discovery

Displaying the MAC Addresses of all Access Points: Example

This example shows how to display MAC addresses of all the access points that are joined to the switch:

```
Switch# show ap join stats summary
Number of APs.................................... 4

Base Mac          EthernetMac       AP Name IP Address    Status
----------------- ----------------- ------- ------------- ----------
00:0b:85:57:bc:c0 00:0b:85:57:bc:c0 AP1130  10.10.163.217 Joined
00:1c:0f:81:db:80 00:1c:63:23:ac:a0 AP1140  10.10.163.216 Not joined
00:1c:0f:81:fc:20 00:1b:d5:9f:7d:b2 AP1     10.10.163.215 Joined
00:21:1b:ea:36:60 00:0c:d4:8a:6b:c1 AP2     10.10.163.214 Not joined
```

This example shows how to display the last join error details for a specific access point:

```
Switch# show ap mac-address 000.2000.0400 join stats summary
Is the AP currently connected to controller..... Yes
Time at which the AP joined this
controller last time............................. Aug 21 12:50:36.061
Type of error
that occurred last.................. AP got or has been disconnected
Reason for error
that occurred last........... The AP has been reset by the controller
Time at which the last join error occurred..... Aug 21 12:50:34.374
```

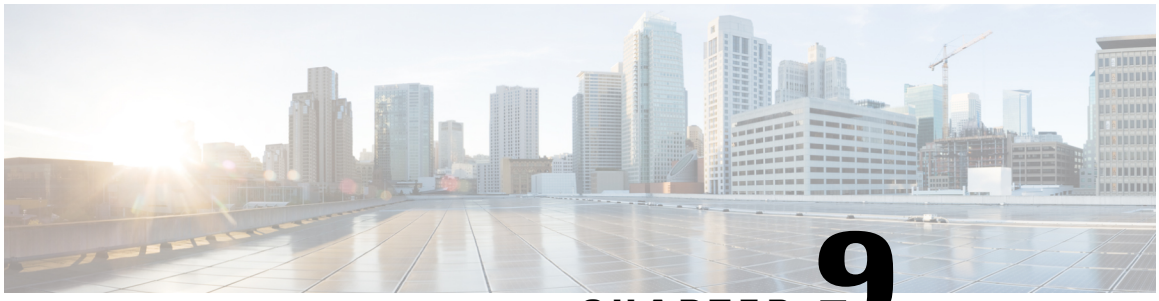
This example shows how to display all join-related statistics collected for a specific access point:

```
Switch# show ap mac-address 000.2000.0400 join stats detailed
Discovery phase statistics
- Discovery requests received..................... 2
- Successful discovery responses sent............. 2
- Unsuccessful discovery request processing....... 0
- Reason for last unsuccessful discovery attempt.... Not applicable
- Time at last successful discovery attempt....... Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt..... Not applicable

Join phase statistics
```

```
- Join requests received.............................. 1
- Successful join responses sent...................... 1
- Unsuccessful join request processing................ 1
- Reason for last unsuccessful join attempt.....      RADIUS authorization
                                                      is pending
                                                      for the AP
- Time at last successful join attempt................ Aug 21 12:50:34.481
- Time at last unsuccessful join attempt.............. Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received..................... 1
- Successful configuration responses sent.............. 1
- Unsuccessful configuration request processing....... 0
- Reason for last unsuccessful configuration attempt.. Not applicable
- Time at last successful configuration attempt....... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt..... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure.......... Not applicable

Last AP disconnect details
- Reason for last AP connection failure............... The AP has been reset by
                                                      the controller
Last join error summary
- Type of error that occurred last.................... AP got or has been
                                                      disconnected
- Reason for error that occurred last................. The AP has been reset
                                                      by the controller
- Time at which the last join error occurred.......... Aug 21 12:50:34.374
```

DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example

For more information about the AP join process, see *DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example* at http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00808714fe.shtml.



CHAPTER 9

Configuring Data Encryption

- Finding Feature Information, page 115
- Prerequisites for Configuring Data Encryption, page 115
- Restrictions for Configuring Data Encryption, page 115
- Information About Data Encryption, page 116
- How to Configure Data Encryption, page 116
- Configuration Examples for Configuring Data Encryption, page 117

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 Data Encryption

- Cisco 1260, 3500, 3600, 801, 1140, 1310, and 1520 series access points support Datagram Transport Layer Security (DTLS) data encryption.
- You can use the switch to enable or disable DTLS data encryption for a specific access point or for all access points.
- Non-Russian customers who use the Cisco switch do not need a data DTLS license.

Restrictions for Configuring Data Encryption

- Encryption limits throughput at both the switch and the access point, and maximum throughput is desired for most enterprise networks.

- If your switch does not have a data DTLS license and if the access point associated with the switch has DTLS enabled, the data path will be unencrypted.
- In images that do not have a DTLS license, the DTLS commands are not available.

Information About Data Encryption

The switch enables you to encrypt Control and Provisioning of Wireless Access Points (CAPWAP) control packets (and optionally, CAPWAP data packets) that are sent between the access point and the switch using DTLS. DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a switch and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

How to Configure Data Encryption

Configuring Data Encryption (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap link-encryption**
3. **end**
4. **show ap link-encryption**
5. **show wireless dtls connections**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap link-encryption** **Example:** `Switch(config)# ap link-encryption`	Enables data encryption for all access points or a specific access point by entering this command. The default value is disabled. Changing the data encryption mode requires the access points to rejoin the switch.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
Step 4	**show ap link-encryption** **Example:** `Switch# show ap link-encryption`	Displays the encryption state of all access points or a specific access point. This command also shows authentication errors, which track the number of integrity check failures and replay errors. Relay errors help in tracking the number of times the access point receives the same packet.
Step 5	**show wireless dtls connections** **Example:** `Switch# show wireless dtls connections`	Displays a summary of all active DTLS connections. **Note** If you experience any problems with DTLS data encryption, enter the **debug dtls ap** {**all** | **event** | **trace**} command to debug all DTLS messages, events, or traces.

Related Topics

Displaying Data Encryption States for all Access Points: Examples, on page 117

Configuration Examples for Configuring Data Encryption

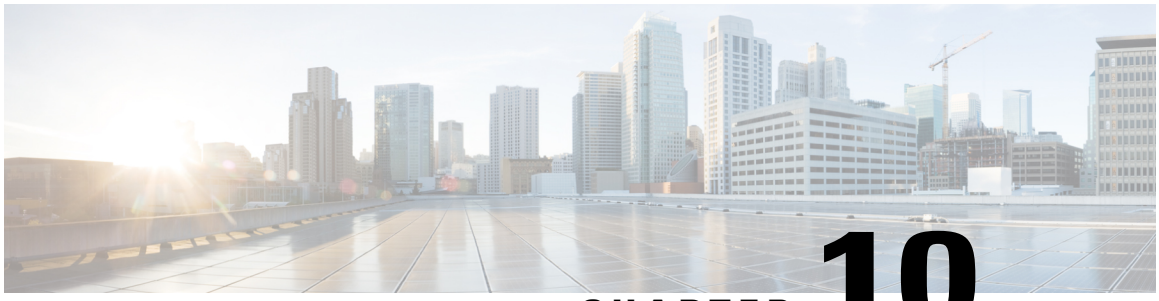
Displaying Data Encryption States for all Access Points: Examples

This example shows how to display the encryption state of all access points or a specific access point. This command also shows authentication errors, which track the number of integrity check failures and replay errors. Relay errors help in tracking the number of times the access point receives the same packet:

```
Switch# show ap link-encryption
                    Encryption  Dnstream  Upstream    Last
AP Name                  State     Count     Count  Update
------------------  ----------  --------  --------  ------
3602a                  Enabled         0         0   Never
```

This example shows how to display a summary of all active DTLS connections:

```
Switch# show wireless dtls connections
AP Name         Local Port   Peer IP       Peer Port  Ciphersuite
--------------- ------------ ------------- ---------- --------------------
3602a           Capwap_Ctrl  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
3602a           Capwap_Data  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
```



CHAPTER 10

Configuring Retransmission Interval and Retry Count

- Finding Feature Information, page 119
- Prerequisites for Configuring the Access Point Retransmission Interval and Retry Count, page 119
- Information About Retransmission Interval and Retry Count, page 120
- How to Configure Access Point Retransmission Interval and Retry Count, page 120
- Viewing CAPWAP Maximum Transmission Unit Information (CLI), page 121
- Configuration Examples for Configuring Access Point Retransmission Interval and Retry Count, page 122

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 the Access Point Retransmission Interval and Retry Count

- You can configure the retransmission intervals and retry count both at a global and a specific access point level. A global configuration applies these configuration parameters to all the access points. Alternatively, when you configure the retransmission level and retry count at a specific access point level, the values are applied to that particular access point. The access point specific configuration has a higher precedence than the global configuration.

Information About Retransmission Interval and Retry Count

The switch and the access points exchange packets using the Control and Provisioning of Wireless Access Points (CAPWAP) reliable transport protocol. For each request, a response is defined. This response is used to acknowledge the receipt of the request message. Response messages are not explicitly acknowledged; therefore, if a response message is not received, the original request message is retransmitted after the retransmit interval. If the request is not acknowledged after a maximum number of retransmissions, the session is closed and the access points reassociate with another switch.

How to Configure Access Point Retransmission Interval and Retry Count

Configuring the Access Point Retransmission Interval and Retry Count (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap capwap retransmit interval** *interval_time*
4. **ap capwap retransmit count** *count_value*
5. **end**
6. **ap name** *Cisco_AP* **capwap retransmit interval** *interval_time*
7. **ap name** *Cisco_AP* **capwap retransmit count** *count_value*
8. **show ap capwap retransmit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap capwap retransmit interval** *interval_time* **Example:** `Switch(config)# ap capwap retransmit interval 2`	Configures the control packet retransmit interval for all access points globally. **Note** The range for the interval parameter is from 2 to 5.

	Command or Action	Purpose
Step 4	**ap capwap retransmit count** *count_value* **Example:** `Switch(config)# ap capwap retransmit count 3`	Configures the control packet retry count for all access points globally. **Note** The range for the count is from 3 to 8.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 6	**ap name** *Cisco_AP* **capwap retransmit interval** *interval_time* **Example:** `Switch# ap name AP02 capwap retransmit interval 2`	Configures the control packet retransmit interval for the individual access point that you specify. **Note** The range for the interval is from 2 to 5. **Note** You must be in privileged EXEC mode to use the **ap name** commands.
Step 7	**ap name** *Cisco_AP* **capwap retransmit count** *count_value* **Example:** `Switch# ap name AP02 capwap retransmit count 3`	Configures the control packet retry count for the individual access point that you specify. **Note** The range for the retry count is from 3 to 8.
Step 8	**show ap capwap retransmit** **Example:** `Switch# show ap capwap retransmit`	Displays the CAPWAP retransmit details.

Viewing CAPWAP Maximum Transmission Unit Information (CLI)

SUMMARY STEPS

1. **enable**
2. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name Maria-1250 config general | include MTU`	Displays the maximum transmission unit (MTU) for the CAPWAP path on the switch. The MTU specifies the maximum size of any packet (in bytes) in a transmission.

Related Topics

Viewing the CAPWAP Retransmission Details: Example, on page 122

Viewing Maximum Transmission Unit Information: Example, on page 122

Configuration Examples for Configuring Access Point Retransmission Interval and Retry Count

Viewing the CAPWAP Retransmission Details: Example

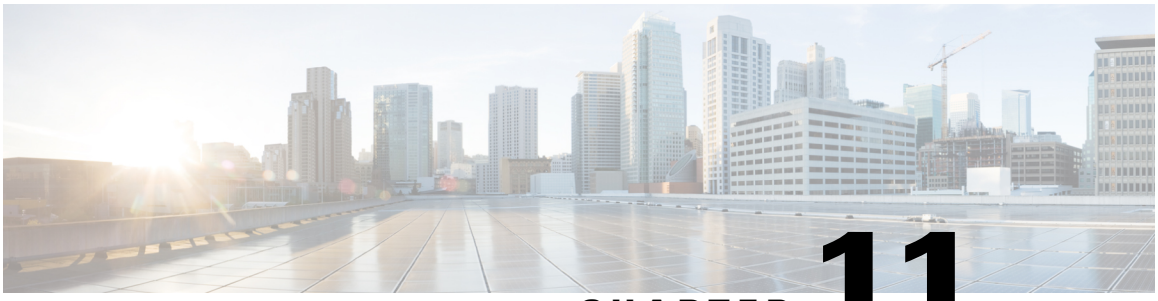
Enter the following command:

```
Switch# show ap capwap retransmit
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval             Retransmit Count

-------------------------------- --------------------------------
--------------------------------
3602a                            5                               3
```

Viewing Maximum Transmission Unit Information: Example

This example shows how to view the maximum transmission unit (MTU) for the CAPWAP path on the switch. The MTU specifies the maximum size of any packet (in bytes) in a transmission:

```
Switch# show ap name cisco-ap-name config general | include MTU
CAPWAP Path MTU.................................. 1500
```



CHAPTER 11

Configuring Adaptive Wireless Intrusion Prevention System

- Finding Feature Information, page 123
- Prerequisites for Configuring wIPS, page 123
- How to Configure wIPS on Access Points, page 124
- Monitoring wIPS Information, page 125
- Configuration Examples for Configuring wIPS on Access Points, page 126

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 wIPS

- The regular local mode access point has been extended with a subset of Wireless Intrusion Prevention System (wIPS) capabilities. This feature enables you to deploy your access points to provide protection without needing a separate overlay network.

How to Configure wIPS on Access Points

Configuring wIPS on an Access Point (CLI)

SUMMARY STEPS

1. **ap name** *Cisco_AP* **mode local**
2. **ap name** *Cisco_AP* **dot11 5ghz shutdown**
3. **ap name** *Cisco_AP* **dot11 24ghz shutdown**
4. **ap name** *Cisco_AP* **mode monitor submode wips**
5. **ap name** *Cisco_AP* **monitor-mode wips-optimized**
6. **show ap dot11 24ghz monitor**
7. **ap name** *Cisco_AP* **no dot11 5ghz shutdown**
8. **ap name** *Cisco_AP* **no dot11 24ghz shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode local** **Example:** `Switch# ap name AP01 mode local`	Configures an access point for monitor mode. A message appears that indicates that changing the AP's mode causes the access point to reboot. This message also displays a prompt that enables you to specify whether or not you want to continue with changing the AP mode. Enter **y** at the prompt to continue.
Step 2	**ap name** *Cisco_AP* **dot11 5ghz shutdown** **Example:** `Switch# ap name AP01 dot11 5ghz shutdown`	Disables the 802.11a radio on the access point.
Step 3	**ap name** *Cisco_AP* **dot11 24ghz shutdown** **Example:** `Switch# ap name AP02 dot11 24ghz shutdown`	Disables the 802.11b radio on the access point.
Step 4	**ap name** *Cisco_AP* **mode monitor submode wips** **Example:** `Switch# ap name AP01 mode monitor submode wips`	Configures the wIPS submode on the access point. **Note** To disable wIPS on the access point, enter the **ap name** *Cisco_AP* **modemonitor submode none** command.
Step 5	**ap name** *Cisco_AP* **monitor-mode wips-optimized**	Enables wIPS optimized channel scanning for the access point. The access point scans each channel for 250 milliseconds. It derives the list of channels to be scanned from the monitor configuration. You can choose the following options:

	Command or Action	Purpose
	Example: `Switch# ap name AP01 monitor-mode wips-optimized`	• **All—**All channels supported by the access point's radio. • **Country—**Only the channels supported by the access point's country of operation. • **DCA—**Only the channel set used by the dynamic channel assignment (DCA) algorithm, which by default includes all of the nonoverlapping channels allowed in the access point's country of operation.
Step 6	**show ap dot11 24ghz monitor** **Example:** `Switch# show ap dot11 24ghz monitor`	Displays the monitor configuration channel set. **Note** The 802.11b Monitor Channels value in the output of the command indicates the monitor configuration channel set.
Step 7	**ap name** *Cisco_AP* **no dot11 5ghz shutdown** **Example:** `Switch# ap name AP01 no dot11 5ghz shutdown`	Enables the 802.11a radio on the access point.
Step 8	**ap name** *Cisco_AP* **no dot11 24ghz shutdown** **Example:** `Switch# ap name AP01 no dot11 24ghz shutdown`	Enables the 802.11b radio on the access point.

Monitoring wIPS Information

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **show ap name** *Cisco_AP* **config general**
2. **show ap monitor-mode summary**
3. **show wireless wps wips summary**
4. **show wireless wps wips statistics**
5. **clear wireless wips statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP01 config general`	Displays information on the wIPS submode on the access point.
Step 2	**show ap monitor-mode summary** **Example:** `Switch# show ap monitor-mode summary`	Displays the wIPS optimized channel scanning configuration on the access point.
Step 3	**show wireless wps wips summary** **Example:** `Switch# show wireless wps wips summary`	Displays the wIPS configuration forwarded by NCS or Prime to the switch.
Step 4	**show wireless wps wips statistics** **Example:** `Switch# show wireless wps wips statistics`	Displays the current state of wIPS operation on the switch.
Step 5	**clear wireless wips statistics** **Example:** `Switch# clear wireless wips statistics`	Clears the wIPS statistics on the switch.

Related Topics

Displaying the Monitor Configuration Channel Set: Example, on page 126

Displaying wIPS Information: Examples, on page 127

Configuration Examples for Configuring wIPS on Access Points

Displaying the Monitor Configuration Channel Set: Example

This example shows how to display the monitor configuration channel set:

```
Switch# show ap dot11 24ghz monitor
Default 802.11b AP monitoring
802.11b Monitor Mode.......................... enable
802.11b Monitor Channels...................... Country channels
802.11b AP Coverage Interval.................. 180 seconds
802.11b AP Load Interval...................... 60 seconds
802.11b AP Noise Interval..................... 180 seconds
802.11b AP Signal Strength Interval............ 60 seconds
```

Displaying wIPS Information: Examples

This example shows how to display information on the wIPS submode on the access point:

```
Switch# show ap name AP01 config general
Cisco AP Identifier.............. 3
Cisco AP Name.................... AP1131:46f2.98ac
...
AP Mode ......................... Monitor
Public Safety ................... Disabled Disabled
AP SubMode ...................... WIPS
```

This example shows how to display the wIPS optimized channel scanning configuration on the access point:

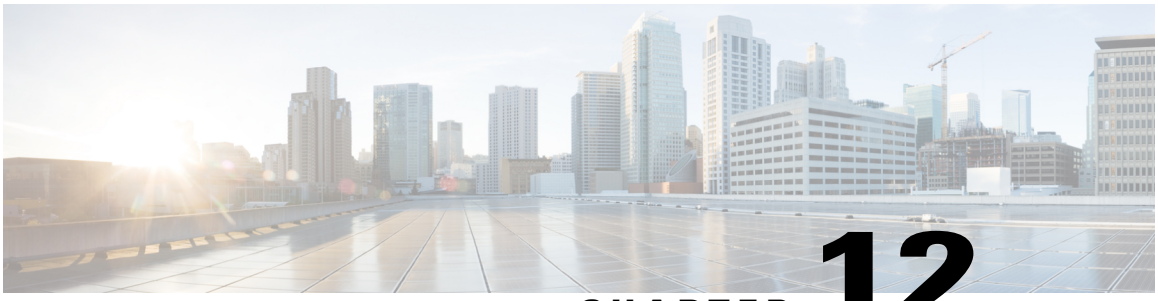
```
Switch# show ap monitor-mode summary
AP Name       Ethernet MAC   Status   Scanning
                                      Channel
                                      List
------------- -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a WIPS     1,6,NA,NA
```

This example shows how to display the wIPS configuration forwarded by WCS to the switch:

```
Switch# show wireless wps wips summary
Policy Name.............. Default
Policy Version........... 3
```

This example shows how to display the current state of wIPS operation on the switch:

```
Switch# show wireless wps wips statistics
Policy Assignment Requests............ 1
Policy Assignment Responses........... 1
Policy Update Requests................ 0
Policy Update Responses............... 0
Policy Delete Requests................ 0
Policy Delete Responses............... 0
Alarm Updates......................... 13572
Device Updates........................ 8376
Device Update Requests................ 0
Device Update Responses............... 0
Forensic Updates...................... 1001
Invalid WIPS Payloads................. 0
Invalid Messages Received............. 0
CAPWAP Enqueue Failed................. 0
NMSP Enqueue Failed................... 0
NMSP Transmitted Packets.............. 22950
NMSP Transmit Packets Dropped......... 0
NMSP Largest Packet................... 1377
```



CHAPTER 12

Configuring Authentication for Access Points

- Finding Feature Information, page 129
- Prerequisites for Configuring Authentication for Access Points, page 129
- Restrictions for Configuring Authentication for Access Points, page 130
- Information about Configuring Authentication for Access Points, page 130
- How to Configure Authentication for Access Points, page 131
- Configuration Examples for Configuring Authentication for Access Points, page 137

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 Authentication for Access Points

- You can set a global username, password, and enable password for all access points that are currently joined to the switch and any that join in the future inherit as they join the switch. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.
- After an access point joins the switch, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point's console port. When you log in, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.
- The global credentials that you configure on the switch are retained across switch and access point reboots. They are overwritten only if the access point joins a new switch that is configured with a global

username and password. If the new switch is not configured with global credentials, the access point retains the global username and password configured for the first switch.

- You must track the credentials used by the access points. Otherwise, you might not be able to log into an access point's console port. If you need to return the access points to the default *Cisco/Cisco* username and password, you must clear the switch's configuration and the access point's configuration to return them to factory-default settings. To reset the default access point configuration, enter the **ap name** *Cisco_AP* **mgmtuser username** *Cisco* **password** *Cisco* command. Entering the command does not clear the static IP address of the access point. Once the access point rejoins a switch, it adopts the default *Cisco/Cisco* username and password.
- You can configure global authentication settings for all access points that are currently joined to the switch and any that join in the future. If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.
- This feature is supported on the following hardware:
  - All Cisco switches that support authentication.
  - Cisco Aironet 1140, 1260, 1310, 1520, 1600, 2600, 3500, and 3600 access points

Restrictions for Configuring Authentication for Access Points

- The switch name in the AP configuration is case sensitive. Therefore, make sure to configure the exact system name on the AP configuration. Failure to do this results in the AP fallback not working.

Information about Configuring Authentication for Access Points

Cisco IOS access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the nonprivileged mode and enter the **show** and **debug** commands that pose a security threat to your network. You must change the default enable password to prevent unauthorized access and to enable users to enter configuration commands from the access point's console port.

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The access point acts as an 802.1X supplicant and is authenticated by the switch where it uses EAP-FAST with anonymous PAC provisioning.

How to Configure Authentication for Access Points

Configuring Global Credentials for Access Points (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value*
4. **end**
5. **ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret*
6. **show ap summary**
7. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value* **Example:** `Switch(config)# ap mgmtuser apusr1 password appass 0 secret 0 appass1`	Configures the global username and password and enables the password for all access points that are currently joined to the switch and any access points that join the switch in the future. In the command, the parameter 0 specifies that an unencrypted password will follow and 8 specifies that an AES encrypted password will follow.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret* **Example:** `Switch(config)# ap name TSIM_AP-2 mgmtuser apusr1 password appass secret secret`	Overrides the global credentials for a specific access point and assigns a unique username and password and enables password to this access point. The credentials that you enter in this command are retained across switch and access point reboots and if the access point joins a new switch. **Note** If you want to force this access point to use the switch's global credentials, enter the **ap name** *Cisco_AP* **no mgmtuser** command. The following message appears after you execute this command: "AP reverted to global username configuration."

	Command or Action	Purpose
Step 6	**show ap summary** **Example:** `Switch# show ap summary`	Displays a summary of all connected Cisco APs.
Step 7	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP02 config general`	Displays the global credentials configuration for a specific access point. **Note** If this access point is configured for global credentials, the AP User Mode text boxes shows "Automatic." If the global credentials have been overwritten for this access point, the AP User Mode text box shows "Customized."

Configuring Global Credentials for Access Points (GUI)

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **Global AP Configuration**.
The **Global Configuration** page is displayed.

Step 2 In the **Login Credentials** area, enter the following parameters:

- **User Name**
- **Password**
- **Confirm Password**
- **Secret Password**
- **Confirm Secret Password**

The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters. No character in the password can be repeated more than three times consecutively. The password should not contain the management username or the reverse of the username. The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 3 Click **Apply**.
The global username and password are applied to all the access points that are associated with the switches

Step 4 Click **Save Configuration**.

Step 5 (Optional) You can override the global credentials for a specific access point and assign a unique username and password by following these steps:

a) Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.
The **All APs** page is displayed.

b) Click the name of an access point.
The **AP > Edit** page is displayed.

c) Click the **Credentials** tab.
d) In the **Login Credentials** area, select the **Over-ride Global Credentials** check box.
e) Enter the values for the following parameters:

- **Username**
- **Password**
- **Enable Password**

f) Click **Apply**.
g) Click **Save Configuration**.

Configuring Authentication for Access Points (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap dot1x username** *user_name_value* **password 0** *password_value*
4. **end**
5. **ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value*
6. **configure terminal**
7. **no ap dot1x username** *user_name_value* **password 0** *password_value*
8. **end**
9. **show ap summary**
10. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap dot1x username** *user_name_value* **password 0** *password_value*	Configures the global authentication username and password for all access points that are currently joined to the switch and any access points that join the switch in the future. This command contains the following keywords and arguments:

	Command or Action	Purpose
	Example: `Switch(config)# ap dot1x username AP3 password 0 password`	• **username—**Specifies an 802.1X username for all access points. • *user-id*—Username. • **password—**Specifies an 802.1X password for all access points. • **0—**Specifies an unencrypted password. • **8—**Specifies an AES encrypted password. • *passwd*—Password. **Note** You must enter a strong password for the password parameter. Strong passwords are at least eight characters long, contain a combination of uppercase and lowercase letters, numbers, and symbols, and are not a word in any language.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value* **Example:** `Switch# ap name AP03 dot1x-user username apuser1 password appass`	Overrides the global authentication settings and assigns a unique username and password to a specific access point. This command contains the following keywords and arguments: • **username—**Specifies to add a username. • *user-id*—Username. • **password—**Specifies to add a password. • **0—**Specifies an unencrypted password. • **8—**Specifies an AES encrypted password. • *passwd*—Password. **Note** You must enter a strong password for the password parameter. See the note in Step 2 for the characteristics of strong passwords. The authentication settings that you enter in this command are retained across switch and access point reboots and whenever the access point joins a new switch.
Step 6	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 7	**no ap dot1x username** *user_name_value* **password 0** *password_value* **Example:** `Switch(config)# no ap dot1x username dot1xusr password 0 dot1xpass`	Disables 802.1X authentication for all access points or for a specific access point. The following message appears after you execute this command: "AP reverted to global username configuration."

	Command or Action	Purpose
		Note You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.
Step 8	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show ap summary** **Example:** `Switch# show ap summary`	Displays the authentication settings for all access points that join the switch. **Note** If global authentication settings are not configured, the Global AP Dot1x User Name text box shows "Not Configured."
Step 10	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP02 config general`	Displays the authentication settings for a specific access point. **Note** If this access point is configured for global authentication, the AP Dot1x User Mode text boxes shows "Automatic." If the global authentication settings have been overwritten for this access point, the AP Dot1x User Mode text box shows "Customized."

Related Topics

Displaying the Authentication Settings for Access Points: Examples, on page 137

Configuring the Switch for Authentication (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x system-auth-control**
4. **aaa new-model**
5. **aaa authentication dot1x default group radius**
6. **radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key*
7. **interface TenGigabitEthernet1/0/1**
8. **switch mode access**
9. **dot1x pae authenticator**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**dot1x system-auth-control** **Example:** `Switch(config)# dot1x system-auth-control`	Enables system authentication control.
Step 4	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables new access control commands and functions.
Step 5	**aaa authentication dot1x default group radius** **Example:** `Switch(config)# aaa authentication dot1x default group radius`	Sets the default authentications lists for IEEE 802.1X by using all the radius hosts in a server group.
Step 6	**radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key* **Example:** `Switch(config)# radius-server host 10.1.1.1 acct-port 1813 auth-port 6225 key 0 encryptkey`	Sets a clear text encryption key for the RADIUS authentication server.
Step 7	**interface TenGigabitEthernet1/0/1** **Example:** `Switch(config)# interface TenGigabitEthernet1/0/1`	Sets the 10-Gigbit Ethernet interface. The command prompt changes from Controller(config)# to Controller(config-if)#.
Step 8	**switch mode access** **Example:** `Switch(config-if)# switch mode access`	Sets the unconditional truncking mode access to the interface.
Step 9	**dot1x pae authenticator** **Example:** `Switch(config-if)# dot1x pae authenticator`	Sets the 802.1X interface PAE type as the authenticator.

	Command or Action	Purpose
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Displaying the Authentication Settings for Access Points: Examples, on page 137

Configuration Examples for Configuring Authentication for Access Points

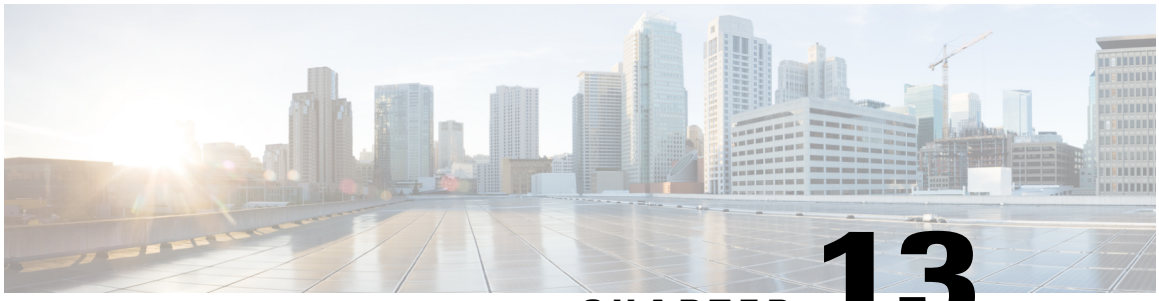
Displaying the Authentication Settings for Access Points: Examples

This example shows how to display the authentication settings for all access points that join the switch:

```
Switch# show ap summary
Number of APs.................................. 1
Global AP User Name............................ globalap
Global AP Dot1x User Name...................... globalDot1x
```

This example shows how to display the authentication settings for a specific access point:

```
Switch# show ap name AP02 config dot11 24ghz general
Cisco AP Identifier............................ 0
Cisco AP Name.................................. TSIM_AP2
...
AP Dot1x User Mode............................. AUTOMATIC
AP Dot1x User Name............................. globalDot1x
```



CHAPTER 13

Converting Autonomous Access Points to Lightweight Mode

- Finding Feature Information, page 139
- Prerequisites for Converting Autonomous Access Points to Lightweight Mode, page 139
- Information About Autonomous Access Points Converted to Lightweight Mode, page 140
- How to Convert a Lightweight Access Point Back to an Autonomous Access Point, page 142
- Authorizing Access Points (CLI), page 143
- Disabling the Reset Button on Converted Access Points (CLI), page 144
- Monitoring the AP Crash Log Information, page 145
- How to Configure a Static IP Address on an Access Point, page 146
- Recovering the Access Point Using the TFTP Recovery Procedure, page 148
- Configuration Examples for Converting Autonomous Access Points to Lightweight Mode, page 148

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 Converting Autonomous Access Points to Lightweight Mode

- Access points that are converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN switchs and cannot communicate with WDS devices. However, the switch provides functionality that is equivalent to WDS when the access point associates to it.

- All Cisco lightweight access points support 16 Basic Service Set Identifiers (BSSIDs) per radio and a total of 16 wireless LANs per access point. When a converted access point associates to a switch, only wireless LANs with IDs 1 through 16 are pushed to the access point unless the access point is a member of an access point group.
- Access points that are converted to lightweight mode must get an IP address and discover the switch using DHCP, DNS, or IP subnet broadcast.

Information About Autonomous Access Points Converted to Lightweight Mode

You can convert autonomous Cisco Aironet access points to lightweight mode. When you upgrade the access points to lightweight mode, the access point communicates with the switch and receives a configuration and software image from the switch.

See the *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document for instructions to upgrade an autonomous access point to lightweight mode:

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

Reverting from Lightweight Mode to Autonomous Mode

After you convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS Release 12.3(7)JA or earlier releases). If the access point is associated with a switch, you can use the switch to load the Cisco IOS release. If the access point is not associated to a switch, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

Using DHCP Option 43 and DHCP Option 60

Cisco Aironet access points use the type-length-value (TLV) format for DHCP option 43. You must program the DHCP servers to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP option 60).

For more information about DHCP VCI strings of access points, see http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00808714fe.shtml.

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. The *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document contains example steps for configuring option 43 on a DHCP server.

If the access point is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that access point will be different than those strings listed in the previous table. The VCI string has the following suffix: ServiceProvider. For example, a 1260 with this option returns this VCI string: Cisco AP c1260-ServiceProvider.

Note The switch IP address that you obtain from the DHCP server should be a unicast IP address. Do not configure the switch IP address as a multicast address when configuring DHCP option 43.

How Converted Access Points Send Crash Information to the Switch

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the switch. If the unit rebooted because of a crash, the switch pulls up the crash file using existing CAPWAP messages and stores it in the switch flash memory. The crash information copy is removed from the access point flash memory when the switch pulls it from the access point.

Uploading Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the switch. This section provides instructions to upload access point core dumps using the switch GUI or CLI.

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary page, the controller lists the Ethernet MAC addresses of converted access points.
- On the AP Detail page, the controller lists the BSS MAC addresses and Ethernet MAC addresses of converted access points.
- On the Radio Summary page, the switch lists converted access points by the radio MAC address.

Configuring a Static IP Address for a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of users.

An access point cannot discover the switch using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs. You can configure these parameters using either the switch CLI or the GUI.

Note If you configure an access point to use a static IP address that is not on the same subnet on which the access point's previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the **show ap config general** *Cisco_AP* CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.

How to Convert a Lightweight Access Point Back to an Autonomous Access Point

Converting a Lightweight Access Point Back to an Autonomous Access Point (CLI)

SUMMARY STEPS

1. **enable**
2. **ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename* **Example:** `Switch# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname`	Converts the lightweight access point back to autonomous mode. **Note** After entering this command, you must wait until the access point reboots and then reconfigure the access point using the CLI or GUI.

Converting a Lightweight Access Point Back to an Autonomous Access Point (Using the Mode Button and a TFTP Server)

Step 1 Configure the PC on which your TFTP server software runs with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *c1140-k9w7-tar.123-7.JA.tar* for a 1140 series access point) in the TFTP server folder and that the TFTP server is activated.

Step 3 Rename the access point image file in the TFTP server folder to **c1140-k9w7-tar.default** for a 1140 series access point.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Note The **MODE** button on the access point must be enabled.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, reconfigure the access point using the GUI or the CLI.

Authorizing Access Points (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap auth-list ap-policy authorize-ap**
4. **username** *user_name* **mac aaa attribute list** *list_name*
5. **aaa new-model**
6. **aaa authorization credential-download** *auth_list* **local**
7. **aaa attribute list** *list*
8. **aaa session-id common**
9. **aaa local authentication default authorization default**
10. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap auth-list ap-policy authorize-ap** **Example:** `Switch(config)# ap auth-list ap-policy authorize-ap`	Configures an access point authorization policy.
Step 4	**username** *user_name* **mac aaa attribute list** *list_name* **Example:** `Switch(config)# username aaa.bbb.ccc mac aaa attribute list attrlist`	Configures the MAC address of an access point locally.

	Command or Action	Purpose
Step 5	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables new access control commands and functions.
Step 6	**aaa authorization credential-download** *auth_list* **local** **Example:** `Switch(config)# aaa authorization credential-download auth_download local`	Downloads EAP credentials from the local server.
Step 7	**aaa attribute list** *list* **Example:** `Switch(config)# aaa attribute list alist`	Configures AAA attribute list definitions.
Step 8	**aaa session-id common** **Example:** `Switch(config)# aaa session-id common`	Configures the AAA common session ID.
Step 9	**aaa local authentication default authorization default** **Example:** `Switch(config)# aaa local authentication default authorization default`	Configures the local authentication method list.
Step 10	**show ap name** *Cisco_AP* **config general** **Example:** `Switch(config)# show ap name AP01 config general`	Displays the configuration information that corresponds to a specific access point.

Disabling the Reset Button on Converted Access Points (CLI)

You can enable or disable the Reset button on access points that are converted to lightweight mode. The Reset button is labeled MODE on the outside of the access point.

Note The procedure to perform this task using the controller GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ap reset-button**
4. **end**
5. **ap name** *Cisco_AP* **reset-button**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**no ap reset-button** **Example:** `Switch(config)# no ap reset-button`	Disables the Reset buttons on all converted access points that are associated to the switch. **Note** To enable the Reset buttons on all converted access points that are associated to the switch, enter the **ap reset-button** command.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **reset-button** **Example:** `Switch# ap name AP02 reset-button`	Enables the Reset button on the converted access point that you specify.

Monitoring the AP Crash Log Information

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **show ap crash-file**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show ap crash-file** **Example:** `Switch# show ap crash-file`	Verifies whether the crash file is downloaded to the switch.

How to Configure a Static IP Address on an Access Point

Configuring a Static IP Address on an Access Point (CLI)

SUMMARY STEPS

1. **enable**
2. **ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway*
3. **enable**
4. **configure terminal**
5. **ap static-ip name-server** *nameserver_ip_address*
6. **ap static-ip domain** *static_ip_domain*
7. **end**
8. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway*	Configures a static IP address on the access point. This command contains the following keywords and arguments: • **ip-address—** Specifies the Cisco access point static IP address.

	Command or Action	Purpose
	Example: `Switch# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	• *ip-address*— Cisco access point static IP address. • **netmask**—Specifies the Cisco access point static IP netmask. • *netmask*— Cisco access point static IP netmask. • **gateway**—Specifies the Cisco access point gateway. • *gateway*— IP address of the Cisco access point gateway. The access point reboots and rejoins the switch, and the static IP address that you specify is pushed to the access point. After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name. You must perform Steps 3 and 4 after the access points reboot.
Step 3	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 4	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 5	**ap static-ip name-server** *nameserver_ip_address* **Example:** `Switch(config)# ap static-ip name-server 10.10.10.205`	Configures a DNS server so that a specific access point or all access points can discover the switch using DNS resolution. **Note** To undo the DNS server configuration, enter the **no ap static-ip name-server** *nameserver_ip_address* command.
Step 6	**ap static-ip domain** *static_ip_domain* **Example:** `Switch(config)# ap static-ip domain domain1`	Configures the domain to which a specific access point or all access points belong. **Note** To undo the domain name configuration, enter the **no ap static-ip domain** *static_ip_domain* command.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP03 config general`	Displays the IP address configuration for the access point.

Recovering the Access Point Using the TFTP Recovery Procedure

Step 1 Download the required recovery image from Cisco.com (ap3g2-k9w8-tar.152-2.JA.tar) and install it in the root directory of your TFTP server.

Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the switch to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you can remove the TFTP server.

Configuration Examples for Converting Autonomous Access Points to Lightweight Mode

Displaying the IP Address Configuration for Access Points: Example

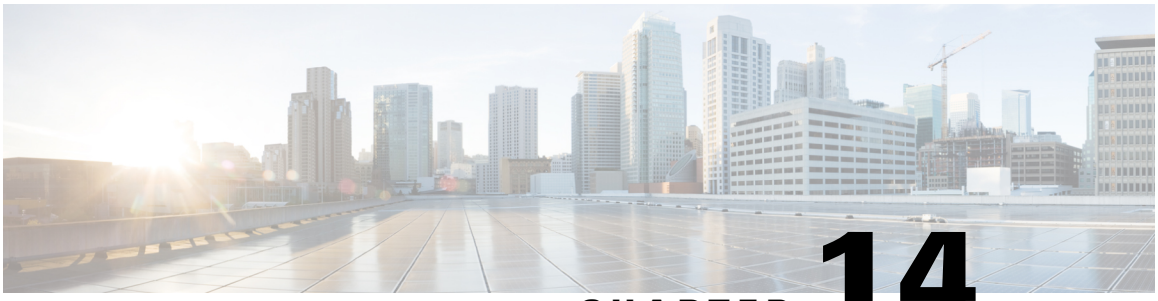
This example shows how to display the IP address configuration for the access point:

```
Switch# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier.............. 4
Cisco AP Name.................................... AP6
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.10.10.118
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.10.10.1
Domain........................................... Domain1
Name Server...................................... 10.10.10.205
...
```

Displaying Access Point Crash File Information: Example

This example shows how to display access point crash file information. Using this command, you can verify whether the file is downloaded to the switch:

```
Switch# show ap crash-file
Local Core Files:
lrad_AP1130.rdump0 (156)

The number in parentheses indicates the size of the file. The size should
be greater than zero if a core dump file is available.
```



CHAPTER 14

Using Cisco Workgroup Bridges

- Finding Feature Information, page 149
- Information About Cisco Workgroup Bridges and non-Cisco Workgroup bridges, page 149
- Monitoring the Status of Workgroup Bridges, page 150
- Debugging WGB Issues (CLI), page 150
- Configuration Examples for Configuring Workgroup Bridges, page 152

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 Cisco Workgroup Bridges and non-Cisco Workgroup bridges

A WGB is a mode that can be configured on an autonomous Cisco IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The WGB provides wireless access connectivity to wired clients by establishing a single wireless connection to the lightweight access point.

When a Cisco WGB is used, the WGB informs the access points of all the clients that it is associated with. The switch is aware of the clients that are associated with the access point. When non-Cisco WGBs are used, the switch has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the switch drops the following types of messages:

- ARP REQ from the distribution system for the WGB client.
- ARP RPLY from the WGB client.
- DHCP REQ from the WGB client.

• DHCP RPLY for the WGB client.

Monitoring the Status of Workgroup Bridges

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **show wireless wgb summary**
3. **show wireless wgb mac-address** *wgb_mac_address* **detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show wireless wgb summary** **Example:** `Switch# show wireless wgb summary`	Displays the WGBs on your network.
Step 3	**show wireless wgb mac-address** *wgb_mac_address* **detail** **Example:** `Switch# show wireless wgb mac-address 00:0d:ed:dd:25:82 detail`	Displays the details of any wired clients that are connected to a particular WGB.

Debugging WGB Issues (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **debug iapp all**
3. **debug iapp error**
4. **debug iapp packet**
5. **debug mobility handoff** [**switch** *switch_number*]
6. **debug dhcp**
7. **debug dot11 mobile**
8. **debug dot11 state**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**debug iapp all** **Example:** `Switch# debug iapp all`	Enables debugging for IAPP messages.
Step 3	**debug iapp error** **Example:** `Switch# debug iapp error`	Enables debugging for IAPP error events.
Step 4	**debug iapp packet** **Example:** `Switch# debug iapp packet`	Enables debugging for IAPP packets.
Step 5	**debug mobility handoff** [**switch** *switch_number*] **Example:** `Switch# debug mobility handoff`	Enables debugging for any roaming issues.
Step 6	**debug dhcp** **Example:** `Switch# debug dhcp`	Debug an IP assignment issue when DHCP is used.
Step 7	**debug dot11 mobile** **Example:** `Switch# debug dot11 mobile`	Enables dot11/mobile debugging. Debug an IP assignment issue when static IP is used.

	Command or Action	Purpose
Step 8	**debug dot11 state** **Example:** `Switch# debug dot11 state`	Enables dot11/state debugging. Debug an IP assignment issue when static IP is used.

Configuration Examples for Configuring Workgroup Bridges

WGB Configuration: Example

This example shows how to configure a WGB access point using static WEP with a 40-bit WEP key:

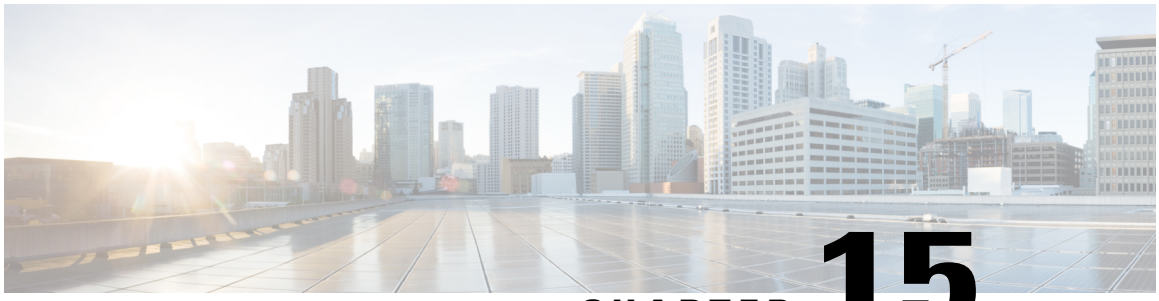
```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# dot11 ssid WGB_with_static_WEP
Switch(config-ssid)# authentication open
Switch(config-ssid)# guest-mode
Switch(config-ssid)# exit
Switch(config)# interface  dot11Radio 0
Switch(config)# station-role workgroup-bridge
Switch(config-if)# encry mode wep 40
Switch(config-if)# encry key 1 size 40 0 1234567890
Switch(config-if)# ssid WGB_with_static_WEP
Switch(config-if)# end
```

Verify that the WGB is associated to an access point by entering this command on the WGB:

show dot11 association

Information similar to the following appears:

```
Switch# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```



CHAPTER 15

Configuring Backup Switches and Failover Priority for Access Points

- Finding Feature Information, page 153
- Prerequisites for Configuring Backup Switchs and Failover Priority for Access Points, page 153
- Restrictions for Configuring Backup Switchs and Failover Priority for Access Points, page 154
- Information About Configuring Backup Switchs, page 154
- How to Configure Backup Switches for Access Points, page 156
- How to Configure Failover Priority for Access Points, page 158
- Retrieving Unique Device Identifier on Switches (CLI), page 159
- Monitoring Failover Priority Settings (CLI), page 160
- Configuration Examples for Configuring Backup Switchs and Failover Priority for Access Points, page 160

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 Backup Switchs and Failover Priority for Access Points

- You can configure primary and secondary backup switches (which are used if primary, secondary, or tertiary switchs are not specified or are not responsive) for all access points that are connected to the switch as well as various timers, including heartbeat timers and discovery request timers. To reduce the switch failure detection time, you can configure the fast heartbeat interval (between the switch and the

access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the switch within the last interval. If no packets have been received, the access point sends a fast echo request to the switch.

- The access point maintains a list of backup switchs and periodically sends primary discovery requests to each entry on the list. When the access point receives a new discovery response from a switch, the backup switch list is updated. Any switch that fails to respond to two consecutive primary discovery requests is removed from the list. If the access point's local switch fails, it chooses an available switch from the backup switch list in this order: primary, secondary, tertiary, primary backup, and secondary backup. The access point waits for a discovery response from the first available switch in the backup list and joins the switch if it receives a response within the time configured for the primary discovery request timer. If the time limit is reached, the access point assumes that the switch cannot be joined and waits for a discovery response from the next available switch in the list.
- When an access point's primary switch comes back online, the access point disassociates from the backup switch and reconnects to its primary switch. The access point falls back only to its primary switch and not to any available secondary switch for which it is configured. For example, if an access point is configured with primary, secondary, and tertiary switchs, it fails over to the tertiary switch when the primary and secondary switchs become unresponsive. If the secondary switch comes back online while the primary switch is down, the access point does not fall back to the secondary switch and stays connected to the tertiary switch. The access point waits until the primary switch comes back online to fall back from the tertiary switch to the primary switch. If the tertiary switch fails and the primary switch is still down, the access point then falls back to the available secondary switch.
- You can configure your wireless network so that the backup switch recognizes a join request from a higher-priority access point and if necessary disassociates a lower-priority access point as a means to provide an available port.
- You must enable failover priority on your network and assign priorities to the individual access points before you can configure this feature.

Restrictions for Configuring Backup Switchs and Failover Priority for Access Points

- You can configure the fast heartbeat timer only for access points in local mode.
- Failover priority is not in effect during the regular operation of your wireless network. It takes effect only if there are more association requests after a switch failure than there are available backup switch ports.
- By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you must assign a priority level only to those access points that warrant a higher priority.

Information About Configuring Backup Switchs

A single switch at a centralized location can act as a backup for access points when they lose connectivity with the primary switch in the local region. Centralized and regional switchs do not need to be in the same mobility group. You can specify a primary, secondary, and tertiary switch for specific access points in your network. Using the switch CLI, you can specify the IP addresses of the backup switchs, which allows the access points to fail over to switchs outside of the mobility group.

Configuring Failover Priority for Access Points

Each controller has a defined number of communication ports for access points. When multiple controllers with unused access point ports are deployed on the same network and one controller fails, the dropped access points automatically poll for unused controller ports and associate with them.

Optimizing RFID Tracking on Access Points

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

Retrieving the Unique Device Identifier on Switchs and Access Points

The Unique Device Identifier (UDI) standard uniquely identifies products across all Cisco hardware product families, enabling customers to identify and track Cisco products throughout their business and network operations and to automate their asset management systems. The standard is consistent across all electronic, physical, and standard business communications. The UDI consists of five data elements:

- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

The UDI is burned into the EEPROM of controllers and lightweight access points at the factory. It can be retrieved through either the GUI or the CLI.

How to Configure Backup Switches for Access Points

Configuring Backup Switches for Access Points (CLI)

SUMMARY STEPS

1. **enable**
2. **ap name** *Cisco_AP* **controller primary** *primary_controller_name* [*primary_controller_ip_address*]
3. **ap name** *Cisco_AP* **controller secondary** *secondary_controller_name* [*secondary_controller_ip_address*]
4. **ap name** *Cisco_AP* **controller tertiary** *tertiary_controller_name* [*tertiary_controller_ip_adress*]
5. **configure terminal**
6. **ap capwap backup primary** *primary_backup_controller_name primary_backup_controller_ip_address*
7. **ap capwap backup secondary** *secondary_backup_controller_name secondary_backup_controller_ip_address*
8. **ap capwap timers fast-heartbeat-timeout** {**local** *timeout_interval*}
9. **ap capwap timers heartbeat-timeout** [*interval*].
10. **ap capwap timers primary-discovery-timeout** [*interval*].
11. **ap capwap timers discovery-timeout** [*interval*].
12. **end**
13. **show ap name** *Cisco_AP* **config general**
14. **show wireless client timers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **controller primary** *primary_controller_name* [*primary_controller_ip_address*] **Example:** `Switch# ap name AP02 controller primary pricon 10.0.0.1`	Configures a primary switch for a specific access point. **Note** The *controller_ip_address* argument in Step 2 and Step 4 is optional. If the backup switch is outside the mobility group to which the access point is connected (the primary switch), you must provide the IP address of the primary, secondary, or tertiary switch, respectively. In each command, the *controller_name* and *controller_ip_address* must belong to the same primary, secondary, or tertiary switch. Otherwise, the access point cannot join the backup switch.
Step 3	**ap name** *Cisco_AP* **controller secondary** *secondary_controller_name* [*secondary_controller_ip_address*]	Configures a secondary switch for a specific access point.

	Command or Action	Purpose
	Example: `Switch# ap name AP02 controller secondary seccon 10.0.0.2`	
Step 4	**ap name** *Cisco_AP* **controller tertiary** *tertiary_controller_name* [*tertiary_controller_ip_adress*] **Example:** `Switch# ap name AP02 controller tertiary tercon 10.0.0.3`	Configures a tertiary switch for a specific access point.
Step 5	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 6	**ap capwap backup primary** *primary_backup_controller_name primary_backup_controller_ip_address* **Example:** `Switch(config)# ap capwap backup primary advbackuppricon 10.0.0.3`	Configures a primary backup switch for all access points. **Note** To delete the primary backup switch, enter the **no ap capwap backup primary** *primary_backup_controller_name primary_backup_controller_ip_address* command.
Step 7	**ap capwap backup secondary** *secondary_backup_controller_name secondary_backup_controller_ip_address* **Example:** `Switch(config)# ap capwap backup secondary advbackupseccon 10.0.0.4`	Configures a secondary backup switch for all access points. **Note** To delete a secondary backup switch, enter the **no ap capwap backup secondary** *secondary_backup_controller_name secondary_backup_controller_ip_address* command.
Step 8	**ap capwap timers fast-heartbeat-timeout** {**local** *timeout_interval*} **Example:** `Switch(config)# ap capwap timers fast-heartbeat-timeout local 5`	Enables the fast heartbeat timer for local access points. **Note** The *timeout_Interval* is from 1 to 10 seconds (inclusive). Specifying a small heartbeat interval reduces the amount of time that it takes to detect a switch failure. The default value is disabled. **Note** To disable the fast heartbeat timer for local access points, enter the **no ap capwap timers fast-heartbeat-timeout** {**local** *timeout_interval*} command.
Step 9	**ap capwap timers heartbeat-timeout** [*interval*]. **Example:** `Switch(config)# ap capwap timers heartbeat-timeout 15`	Configures the access point heartbeat timer. **Note** The timeout *interval* is from 1 to 30 seconds (inclusive). This value should be at least three times larger than the fast heartbeat timer. The default value is 30 seconds. **Note** To disable the access point heartbeat timer, enter the **no ap capwap timers heartbeat-timeout** [*interval*] command. **Caution** Do not enable the fast heartbeat timer with the high latency link. If you have to enable the fast heartbeat timer, the timer value must be greater than the latency.

	Command or Action	Purpose
Step 10	**ap capwap timers primary-discovery-timeout** [*interval*]. **Example:** `Switch(config)# ap capwap timers primary-discovery-timeout 90`	Configures the access point primary discovery request timer. **Note** The timeout *interval* is from 30 to 3600 seconds. The default is 120 seconds. **Note** To disable the access point primary discovery request timer, enter the **no ap capwap timers primary-discovery-timeout** [*interval*] command.
Step 11	**ap capwap timers discovery-timeout** [*interval*]. **Example:** `Switch(config)# ap capwap timers discovery-timeout 9`	Configures the access point discovery timer. **Note** The timeout *interval* is from 1 to 10 seconds (inclusive). The default is 10 seconds. **Note** To disable the access point discovery timer, enter the **no ap capwap timers discovery-timeout** [*interval*] command.
Step 12	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 13	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP02 config general`	Displays access point configuration information.
Step 14	**show wireless client timers** **Example:** `Switch# show wireless client timers`	Displays the wireless client timer information.

How to Configure Failover Priority for Access Points

Configuring Failover Priority for Access Points (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap capwap priority**
4. **end**
5. **ap name** *Cisco_AP* {**priority** *priority_value*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap capwap priority** **Example:** `Switch(config)# ap capwap priority`	Enables the access point failover priority. **Note** To disable access point failover priority, enter the **no ap capwap priority** command.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* {**priority** *priority_value*} **Example:** `Switch# ap name AP02 priority 140`	Specifies the priority of an access point. **Note** You can enter a value from 1 to 4 for the priority value parameter.

Retrieving Unique Device Identifier on Switches (CLI)

SUMMARY STEPS

1. **enable**
2. **show inventory**
3. **show inventory oid**
4. **show inventory raw**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show inventory**	Shows the Unique Device Identifier (UDI) string of the switch.

	Command or Action	Purpose
Step 3	**show inventory oid**	Shows vendor-specific hardware registration identifier.
Step 4	**show inventory raw**	Shows every entity in the container hierarchy.

Monitoring Failover Priority Settings (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **show ap capwap summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show ap capwap summary** **Example:** `Switch# show ap capwap summary`	Displays access point capwap summary. Using this command, you can confirm whether the access point failover priority is enabled on your network.

Configuration Examples for Configuring Backup Switchs and Failover Priority for Access Points

Displaying Access Point Configuration Information: Examples

This example shows how to display access point configuration information:

```
Switch# show ap name AP01 config general

Cisco AP Identifier : 0
Cisco AP Name : AP01
Country Code : US - United States
Regulatory Domain Allowed by Country : 802.11bg:-A
```

```
802.11a:-A
AP Country Code : US - United States
AP Regulatory Domain : Unconfigured
Switch Port Number : Te1/0/1
MAC Address : 0000.2000.03f0
IP Address Configuration : Static IP assigned
IP Address : 9.9.9.16
...... ........
...... ........
Primary Cisco Switch Name : 1-4404
Primary Cisco Switch IP Address : 2.2.2.2
Secondary Cisco Switch Name : 1-4404
Secondary Cisco Switch IP Address : 2.2.2.2
Tertiary Cisco Switch Name : 2-4404
Tertiary Cisco Switch IP Address : 1.1.1.4
```

Displaying Wireless Client Timer Information

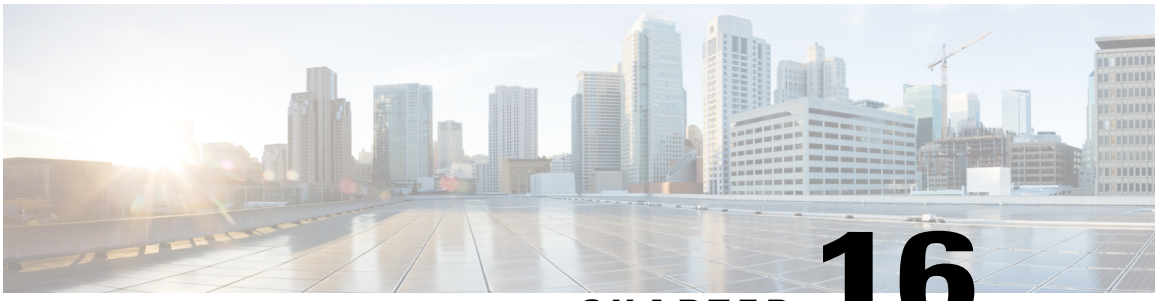
This example shows how to display wireless client timer information:

```
Switch# show wireless client timers

Authentication Response Timeout (seconds) : 10
Rogue Entry Timeout (seconds) : 1300
AP Heart Beat Timeout (seconds) : 30
AP Discovery Timeout (seconds) : 10
AP Local mode Fast Heartbeat (seconds) : 10 (enable)
AP flexconnect mode Fast Heartbeat (seconds) : disable
AP Primary Discovery Timeout (seconds) : 120
```

Displaying Access Point CAPWAP Summary: Example

This example shows how to display access point CAPWAP summary. Using this command, you can confirm whether or not the access point failover priority is enabled on your network.

```
Switch# show ap capwap summary

AP Fallback : Enabled
AP Join Priority : Disabled
AP Master : Disabled
Primary backup Controller Name :
Primary backup Controller IP : 0.0.0.0
Secondary backup Controller Name :
Secondary backup Controller IP : 0.0.0.0
```



CHAPTER 16

Configuring Probe Request Forwarding

- Finding Feature Information, page 163
- Information About Configuring Probe Request Forwarding, page 163
- How to Configure Probe Request Forwarding (CLI), page 163

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 Probe Request Forwarding

Probe requests are 802.11 management frames that are sent by clients to request information about the capabilities of Service Set Identifiers (SSIDs). By default, access points forward acknowledged probe requests to the switch for processing. Acknowledged probe requests are probe requests for SSIDs that are supported by the access point. If desired, you can configure access points to forward both acknowledged and unacknowledged probe requests to the switch. The switch can use the information from unacknowledged probe requests to improve the location accuracy.

How to Configure Probe Request Forwarding (CLI)

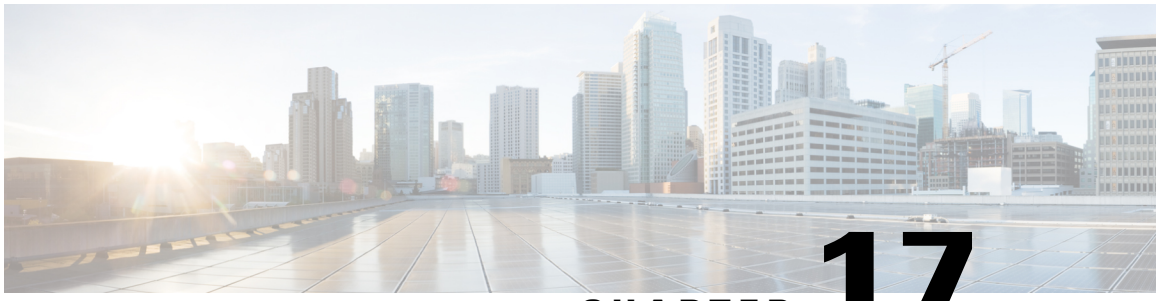
Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **configure terminal**
2. **wireless probe filter**
3. **wireless probe filter** *num_probes interval*
4. **end**
5. **show wireless probe**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless probe filter** **Example:** `Switch(config)# wireless probe filter`	Enables or disables the filtering of probe requests forwarded from an access point to the switch. **Note** If you enable probe filtering, the default filter setting, the access point forwards only acknowledged probe requests to the switch. If you disable probe filtering, the access point forwards both acknowledged and unacknowledged probe requests to the switch.
Step 3	**wireless probe filter** *num_probes interval* **Example:** `Switch(config)# wireless probe filter 5 5`	Limits the number of probe requests sent to the switch per client per access point radio in a given interval. You must specify the following arguments with this command: • *num_probes*—Number of probe requests forwarded to the switch per client per access point radio in a given interval. The range is from 1 to 100. • *interval*—Probe limit interval in milliseconds. The range is from 100 to 10000.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**show wireless probe** **Example:** `Switch# show wireless probe`	Displays the advanced probe request configuration.



CHAPTER 17

Optimizing RFID Tracking

- Finding Feature Information, page 165
- Optimizing RFID Tracking on Access Points, page 165
- How to Optimize RFID Tracking on Access Points, page 166
- Configuration Examples for Optimizing RFID Tracking, page 167

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.

Optimizing RFID Tracking on Access Points

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

How to Optimize RFID Tracking on Access Points

Optimizing RFID Tracking on Access Points (CLI)

SUMMARY STEPS

1. **ap name** *Cisco_AP* **mode monitor submode none**
2. **ap name** *Cisco_AP* **dot11 24ghz shutdown**
3. **ap name** *Cisco_AP* **monitor-mode tracking-opt**
4. **ap name** *Cisco_AP* **monitor-mode dot11b** {**fast-channel** [*first_channel second_channel third_channel fourth_channel*]}
5. **ap name** *Cisco_AP* **no dot11 24ghz shutdown**
6. **show ap monitor-mode summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode monitor submode none** **Example:** `Switch# ap name 3602a mode monitor submode none`	Specifies the monitor submode for the access point as none. **Note** A warning message indicates that changing the access point's mode will cause the access point to reboot and prompts you to specify whether you want to continue by entering **Y**. After you enter **Y**, the access point reboots.
Step 2	**ap name** *Cisco_AP* **dot11 24ghz shutdown** **Example:** `Switch# ap name AP01 dot11 24ghz shutdown`	Disables the access point radio.
Step 3	**ap name** *Cisco_AP* **monitor-mode tracking-opt** **Example:** `Switch# ap name TSIM_AP1 monitor-mode tracking-opt`	Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation. **Note** To disable tracking optimization for an access point, enter the **ap name** *Cisco_AP* **monitor-mode tracking-opt no-optimization** command.
Step 4	**ap name** *Cisco_AP* **monitor-mode dot11b** {**fast-channel** [*first_channel second_channel third_channel fourth_channel*]} **Example:** `Switch# ap name AP01 monitor-mode dot11b fast-channel 1 2 3 4`	Chooses up to four specific 802.11b channels to be scanned by the access point. **Note** In the United States, you can assign any value from 1 to 11 (inclusive) to the channel variable. Other countries support additional channels. You must assign at least one channel.

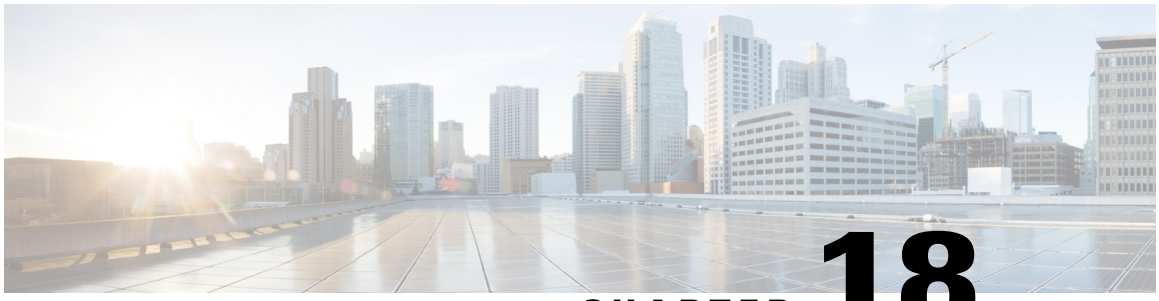
	Command or Action	Purpose
Step 5	**ap name** *Cisco_AP* **no dot11 24ghz shutdown** **Example:** `Switch# ap name AP01 no dot11 24ghz shutdown`	Enables the access point radio.
Step 6	**show ap monitor-mode summary** **Example:** `Switch# show ap monitor-mode summary`	Displays all the access points in monitor mode.

Configuration Examples for Optimizing RFID Tracking

Displaying all the Access Points in Monitor Mode: Example

This example shows how to display all the access points in monitor mode:

```
Switch# show ap monitor-mode summary

AP Name       Ethernet MAC   Status   Scanning
                                      Channel
                                      List
------------- -------------- -------- ---------
AP1131:4f2.9a 00:16:4:f2:9:a Tracking 1,6,NA,NA
```



CHAPTER 18

Configuring Country Codes

- Finding Feature Information, page 169
- Prerequisites for Configuring Country Codes, page 169
- Information About Configuring Country Codes, page 170
- How to Configure Country Codes (CLI), page 170
- Configuration Examples for Configuring Country Codes, page 173

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 Country Codes

- Generally, you configure one country code per switch; you configure one code that matches the physical location of the switch and its access points. You can configure up to 20 country codes per switch. This multiple-country support enables you to manage access points in various countries from a single switch.
- When the multiple-country feature is used, all switchs that are going to join the same RF group must be configured with the same set of countries, configured in the same order.
- Access points are capable of using all the available legal frequencies. However, access points are assigned to the frequencies that are supported in their relevant domains.
- The country list configured on the RF group leader determines which channels the members would operate on. This list is independent of which countries have been configured on the RF group members.
- For switchs in the Japan regulatory domain, you must have had one or more Japan country codes (JP, J2, or J3) configured on your switch at the time you last booted your switch.

- For switchs in the Japan regulatory domain, you must have at least one access point with a -J regulatory domain joined to your switch.

Information About Configuring Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Information About Japanese Country Codes

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- JP—Allows only -J radios to join the controller
- J2—Allows only -P radios to join the controller
- J3—Uses the -U frequencies but allows -U, -P and -Q (other than 1550/1600/2600/3600) radios to join the controller
- J4—Allows 2.4G JPQU and 5G PQU to join the controller.

Note The 1550, 1600, 2600, and 3600 APs require J4.

See the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the list of channels and power levels supported by access points in the Japanese regulatory domains.

How to Configure Country Codes (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **show wireless country supported**
3. **configure terminal**
4. **ap dot11 24ghz shutdown**
5. **ap dot11 5ghz shutdown**
6. **ap country** *country_code*
7. **end**
8. **show wireless country channels**
9. **configure terminal**
10. **no ap dot11 5ghz shutdown**
11. **no ap dot11 24ghz shutdown**
12. **end**
13. **ap name** *Cisco_AP* **shutdown**
14. **configure terminal**
15. **ap country** *country_code*
16. **end**
17. **ap name** *Cisco_AP* **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show wireless country supported** **Example:** `Switch# show wireless country supported`	Displays a list of all available country codes.
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 4	**ap dot11 24ghz shutdown** **Example:** `Switch(config)# ap dot11 5ghz shutdown`	Disables the 802.11a network.
Step 5	**ap dot11 5ghz shutdown** **Example:** `Switch(config)# ap dot11 24ghz shutdown`	Disables the 802.11b/g network.

	Command or Action	Purpose
Step 6	**ap country** *country_code* **Example:** `Switch(config)# ap country IN`	Assigns access points to a specific country. **Note** Make sure that the country code you choose is compatible with the regulatory domain of at least one of the access point's radios.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show wireless country channels** **Example:** `Switch# show wireless country channels`	Displays the list of available channels for the country codes configured on your switch. **Note** Perform Steps 9 through 17 only if you have configured multiple country codes in Step 6.
Step 9	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 10	**no ap dot11 5ghz shutdown** **Example:** `Switch(config)# no ap dot11 5ghz shutdown`	Enables the 802.11a network.
Step 11	**no ap dot11 24ghz shutdown** **Example:** `Switch(config)# no ap dot11 24ghz shutdown`	Enables the 802.11b/g network.
Step 12	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 13	**ap name** *Cisco_AP* **shutdown** **Example:** `Switch# ap name AP02 shutdown`	Disables the access point. **Note** Ensure that you disable only the access point for which you are configuring country codes.
Step 14	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 15	**ap country** *country_code* **Example:** `Switch# ap country IN`	Assigns an access point to a specific country. **Note** Ensure that the country code that you choose is compatible with the regulatory domain of at least one of the access point's radios. **Note** If you enabled the networks and disabled some access points and then enter the **ap country** *country_code* command, the specified country code is configured on only the disabled access points. All other access points are ignored.
Step 16	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 17	**ap name** *Cisco_AP* **no shutdown** **Example:** `Switch# ap name AP02 no shutdown`	Enables the access point.

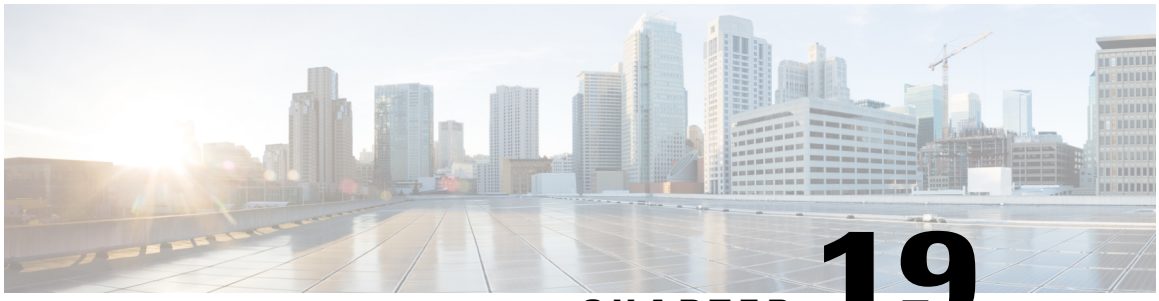
Configuration Examples for Configuring Country Codes

Displaying Channel List for Country Codes: Example

This example shows how to display the list of available channels for the country codes configured on your switch:

```
Switch# show wireless country channels

Configured Country.......................: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
A = Channel is the Auto-RF default in this country.
. = Channel is not legal in this country.
C = Channel has been configured for use by Auto-RF.
x = Channel is available to be configured for use by Auto-RF.
(-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11bg :
Channels : 1 1 1 1 1
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US : A * * * * A * * * * A . . .
Auto-RF : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11a : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
: 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US : . A . A . A . A A A A A * * * * * . . . * * * A A A A
*
Auto-RF : . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
4.9GHz 802.11a :
```

```
Channels : 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
US (-A ,-AB ): * * * * * * * * * * * * * * * * * * * A * * * * * A
Auto-RF : . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```



CHAPTER 19

Configuring Link Latency

- Finding Feature Information, page 175
- Prerequisites for Configuring Link Latency, page 175
- Restrictions for Configuring Link Latency, page 176
- Information About Configuring Link Latency, page 176
- How to Configure Link Latency, page 177
- How to Configure TCP MSS, page 179
- Performing a Link Test (CLI), page 179
- Configuration Examples for Configuring Link Latency, page 180

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 Link Latency

- The switch displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the switch is up or can be cleared and allowed to restart.
- You can configure link latency for a specific access point using the switch GUI or CLI or for all access points joined to the switch using the CLI.

Restrictions for Configuring Link Latency

- Link latency calculates the Control and Provisioning of Wireless Access Points (CAPWAP) response time between the access point and the switch. It does not measure network latency or ping responses.

Information About Configuring Link Latency

You can configure link latency on the switch to measure the link between an access point and the switch. You can use this feature with all access points that are joined to the switch where the link can be a slow or unreliable WAN connection.

TCP MSS

If the client's maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem, you can specify the MSS for all access points that are joined to the switch or for a specific access point.

When you enable this feature, the access point selects the MSS for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

Link Tests

A link test is used to determine the quality of the radio link between two devices. Two types of link-test packets are transmitted during a link test: request and response. Any radio receiving a link-test request packet fills in the appropriate text boxes and echoes the packet back to the sender with the response type set.

The radio link quality in the client-to-access point direction can differ from that in the access point-to-client direction due to the asymmetrical distribution of the transmit power and receive sensitivity on both sides. Two types of link tests can be performed: a ping test and a CCX link test.

With the *ping link test*, the controller can test link quality only in the client-to-access point direction. The RF parameters of the ping reply packets received by the access point are polled by the controller to determine the client-to-access point link quality.

With the *CCX link test*, the switch can also test the link quality in the access point-to-client direction. The switch issues link-test requests to the client, and the client records the RF parameters (received signal strength indicator [RSSI], signal-to-noise ratio [SNR], and so on) of the received request packet in the response packet. Both the link-test requestor and responder roles are implemented on the access point and switch. Not only can the access point or switch initiate a link test to a CCX v4 or v5 client, but a CCX v4 or v5 client can initiate a link test to the access point or switch.

The switch shows the link-quality metrics for CCX link tests in both directions (out— the access point to the client; in— the client to the access point):

- Signal strength in the form of RSSI (minimum, maximum, and average)
- Signal quality in the form of SNR (minimum, maximum, and average)
- Total number of packets that are retried

- Maximum retry count for a single packet
- Number of lost packets
- Data rate of a successfully transmitted packet

The controller shows this metric regardless of direction:

- Link test request/reply round-trip time (minimum, maximum, and average)

The controller software supports CCX versions 1 through 5. 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 limit the features for this client. If a client does not support CCXv4 or v5, the controller performs a ping link test on the client. If a client supports CCXv4 or v5, the controller performs a CCX link test on the client. If a client times out during a CCX link test, the controller switches to the ping link test automatically.

How to Configure Link Latency

Configuring Link Latency (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap link-latency**
4. **ap tcp-adjust-mss size** *size*
5. **show ap name** *Cisco_AP* **config general**
6. **ap name** *Cisco_AP* **link-latency** [**reset**]
7. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap link-latency** **Example:** `Switch(config)# ap link-latency`	Enables link latency for all access points that are currently associated with the switch. **Note** To disable link latency for all the access points that are associated with the switch, use the **no ap link-latency** command.

	Command or Action	Purpose
		Note These commands enable or disable link latency only for access points that are currently joined to the switch. You have to enable or disable link latency for the access points that join in the future. **Note** To enable or disable link latency for specific access points that are associated with the switch, enter the following commands in Priveleged EXEC mode: • **ap name** *Cisco_AP* **link-latency—**Enables link latency. • **ap name** *Cisco_AP* **no link-latency—**Disables link latency.
Step 4	**ap tcp-adjust-mss size** *size* **Example:** `Switch(config)# ap tcp-adjust-mss size 537`	Configures TCP MSS adjust size for all access points. The range is from 536 to 1363.
Step 5	**show ap name** *Cisco_AP* **config general** **Example:** `Switch(config)# show ap name AP02 config general`	Displays the general configuration details of the access point. These configuration details contain the link latency results that correspond to the access point that you specify in the command. The output of this command contains the following link latency results: • Current Delay—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back. • Maximum Delay—Since the time that link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back. • Minimum Delay—Since the time that link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the switch and back.
Step 6	**ap name** *Cisco_AP* **link-latency** [**reset**] **Example:** `Switch(config)# ap name AP02 link-latency reset`	Clears the current, minimum, and maximum link latency statistics on the switch for a specific access point.
Step 7	**show ap name** *Cisco_AP* **config general** **Example:** `Switch(config)# show ap name AP02 config general`	Displays the general configuration details of the access point. Use this command to see the result of the reset operation.

How to Configure TCP MSS

Configuring TCP MSS (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap tcp-adjust-mss size** *size_value*
3. **reload**
4. **show ap tcp-adjust-mss**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap tcp-adjust-mss size** *size_value* **Example:** `Switch(config)# ap tcp-adjust-mss size 537`	Enables the TCP MSS on the particular access point that you specify. **Note** To enable TCP MSS on all the access points that are associated with the switch, enter the **ap tcp-adjust-mss size** *size_value* command, where the size parameter is from 536 to 1363 bytes. The default value varies for different clients.
Step 3	**reload** **Example:** `Switch# reload`	Reboots the switch in order for your change to take effect.
Step 4	**show ap tcp-adjust-mss** **Example:** `Switch# show ap tcp-adjust-mss`	Displays the current TCP MSS setting for all the access points that are associated with the switch. **Note** To display the TCP MSS settings that correspond to a specific access point, enter the **show ap name** *Cisco_AP* **tcp-adjust-mss** command.

Performing a Link Test (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **test wireless linktest** *mac_address*
2. **configure terminal**
3. **wireless linktest frame-size** *frame_size*
4. **wireless linktest number-of-frames** *number_of_frames*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**test wireless linktest** *mac_address* **Example:** `Switch# test wireless linktest 00:0d:88:c5:8a:d1`	Runs a link test.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**wireless linktest frame-size** *frame_size* **Example:** `Switch(config)# wireless linktest frame-size 41`	Configures the link test frame size for each packet.
Step 4	**wireless linktest number-of-frames** *number_of_frames* **Example:** `Switch(config)# wireless linktest number-of-frames 50`	Configures the number of frames to send for the link test.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuration Examples for Configuring Link Latency

Running a Link Test: Example

This example shows how to run a link test:

```
Switch# test wireless linktest 00:0d:88:c5:8a:d1

When CCX v4 or later releases is enabled on both the controller and the client being tested,
 information similar to the following appears:
```

```
CCX Link Test to 00:0d:88:c5:8a:d1.
Link Test Packets Sent..................................... 20
Link Test Packets Received................................. 10
Link Test Packets Lost (Total/AP to Client/Client to AP).... 10/5/5
Link Test Packets round trip time (min/max/average)........ 5ms/20ms/15ms
RSSI at AP (min/max/average)............................... -60dBm/-50dBm/-55dBm
RSSI at Client (min/max/average)........................... -50dBm/-40dBm/-45dBm
SNR at AP (min/max/average)................................ 40dB/30dB/35dB
SNR at Client (min/max/average)............................ 40dB/30dB/35dB
Transmit Retries at AP (Total/Maximum)..................... 5/3
Transmit Retries at Client (Total/Maximum).................. 4/2
Transmit rate: 1M 2M 5.5M 6M 9M 11M 12M 18M 24M 36M 48M 54M 108M
Packet Count: 0 0 0 0 0 0 0 0 0 2 0 18 0
Transmit rate: 1M 2M 5.5M 6M 9M 11M 12M 18M 24M 36M 48M 54M 108M
Packet Count: 0 0 0 0 0 0 0 0 0 2 0 8 0

When CCX v4 or later releases is not enabled on either the controller or the client being
tested, fewer details appear:
Ping Link Test to 00:0d:88:c5:8a:d1.
Link Test Packets Sent..................... 20
Link Test Packets Received................. 20
Local Signal Strength...................... -49dBm
Local Signal to Noise Ratio................ 39dB
```

Displaying Link Latency Information: Example

This example shows how to display general configuration details of the access point. These configuration details contain the link latency results that correspond to the access point that you specify in the command.

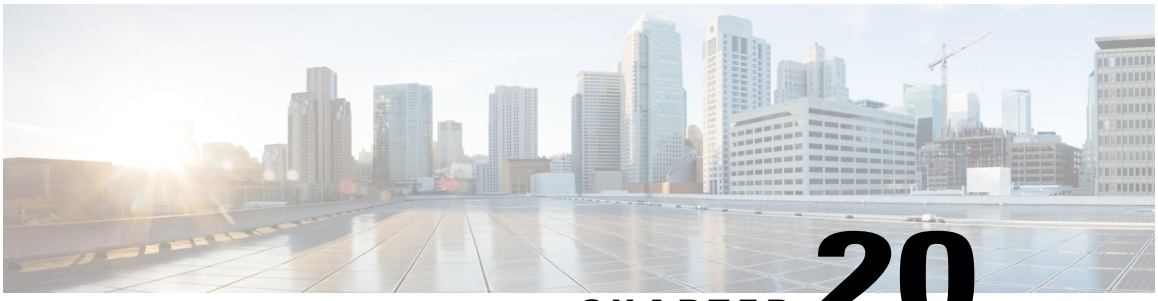
```
Switch# show ap name AP01 config general

Cisco AP Name                                   : AP01
Cisco AP Identifier                             : 55
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : Unconfigured
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.03f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 9.9.9.16
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 9.9.9.2
Fallback IP Address Being Used                  : 9.9.9.16
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : default-location
Cisco AP Group Name                             : default-group
Primary Cisco Controller Name                   : CAPWAP Controller
Primary Cisco Controller IP Address             : 9.9.9.2
Secondary Cisco Controller Name                 :
Secondary Cisco Controller IP Address           : Not Configured
Tertiary Cisco Controller Name                  :
Tertiary Cisco Controller IP Address            : Not Configured
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
```

```
Number of Slots                                 : 2
AP Model                                        : 3502E
AP Image                                        : C3500-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K002
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : Not Configured
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 16 days 3 hours 14 minutes 1 s
econd
AP CAPWAP Up Time                               : 33 minutes 15 seconds
Join Date and Time                              : 01/02/2013 22:41:47
Join Taken Time                                 : 16 days 2 hours 40 minutes 45
seconds
Join Priority                                   : 1
Ethernet Port Duplex                            : Auto
Ethernet Port Speed                             : Auto
AP Link Latency                                 : Enabled
Current Delay                                   : 0
Maximum Delay                                   : 0
Minimum Delay                                   : 0
Last Updated (based on AP up time)              : 0 seconds
Rogue Detection                                 : Disabled
AP TCP MSS Adjust                               : Disabled
AP TCP MSS Size                                 : 536
```

Displaying TCP MSS Settings: Example

This example shows how to display the current TCP MSS setting for all the access points that are associated with the switch:

```
Switch# show ap tcp-adjust-mss

AP Name                     TCP State        MSS Size
------------------------------------------------------
AP01                        Disabled         6146
AP02                        Disabled         536
AP03                        Disabled         6146
AP04                        Disabled         6146
AP05                        Disabled         6146
```



CHAPTER 20

Configuring Power over Ethernet

- Finding Feature Information, page 183
- Information About Configuring Power over Ethernet, page 183
- How to Configure Power over Ethernet, page 184
- Configuration Examples for Configuring Power over Ethernet, page 185

Finding Feature Information

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

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

Information About Configuring Power over Ethernet

When an access point that has been converted to lightweight mode (such as an AP1262) access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch, you must configure Power over Ethernet (PoE), which is also known as *inline power*.

How to Configure Power over Ethernet

Configuring Power over Ethernet (CLI)

SUMMARY STEPS

1. **ap name** *Cisco_AP* **power injector installed**
2. **ap name** *Cisco_AP* **power injector override**
3. **ap name** *Cisco_AP* **power injector switch-mac-address** *switch_mac_address*
4. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **power injector installed** **Example:** `Switch# ap name AP02 power injector installed`	Enables the PoE power injector state. The access point remembers that a power injector is connected to this particular switch port. If you relocate the access point, you must reenter this command after the presence of a new power injector is verified. **Note** Enter this command if your network contains any older Cisco 6-W switches that could be accidentally overloaded if connected directly to a 12-W access point. Make sure that the Cisco Discovery Protocol (CDP) is enabled before entering this command. Otherwise, this command will fail.
Step 2	**ap name** *Cisco_AP* **power injector override** **Example:** `Switch# ap name AP02 power injector override`	Removes the safety checks and allows the access point to be connected to any switch port. You can use this command if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The access point assumes that a power injector is always connected. If you relocate the access point, it continues to assume that a power injector is present.
Step 3	**ap name** *Cisco_AP* **power injector switch-mac-address** *switch_mac_address* **Example:** `Switch# ap name AP02 power injector switch-mac-address 10a.2d.5c.3d`	Sets the MAC address of the switch port that has a power injector. **Note** Enter this command if you know the MAC address of the connected switch port and do not want to automatically detect it using the installed option.
Step 4	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP02 config general`	Displays common information that includes the PoE settings for a specific access point. **Note** The Power Type/Mode text box shows “degraded mode” if the access point is not operating at full power.

Configuration Examples for Configuring Power over Ethernet

Displaying Power over Ethernet Information: Example

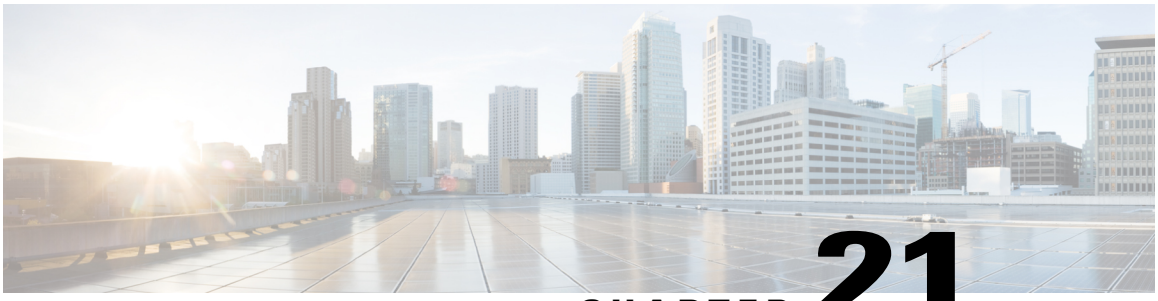
This example shows how to display common information that includes the PoE settings for a specific access point:

```
Switch# show ap name AP01 config general

Cisco AP Identifier.............. 1
Cisco AP Name..................... AP1
...
PoE Pre-Standard Switch........... Enabled
PoE Power Injector MAC Addr....... Disabled
Power Type/Mode................... PoE/Low Power (degraded mode)
...
```

PART V

CleanAir

- Configuring Cisco CleanAir, page 189



CHAPTER 21

Configuring Cisco CleanAir

- Finding Feature Information, page 189
- Prerequisites for CleanAir, page 189
- Restrictions for CleanAir, page 190
- Information About CleanAir, page 191
- How to Configure CleanAir, page 196
- Configuring Cisco CleanAir using the Controller GUI, page 205
- Configuring Cisco Spectrum Expert, page 205
- Monitoring CleanAir Parameters, page 206
- Configuration Examples for Configuring CleanAir, page 209
- CleanAir FAQs, page 210
- Additional References, page 212

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 CleanAir

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Only Cisco CleanAir-enabled access points using the following access point modes can perform Cisco CleanAir spectrum monitoring:

- Local—In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only.

- Monitor—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

  The following options are available:

  - All— All channels
  - DCA—Channel selection governed by the DCA list
  - Country—All channel legal within a regulatory domain

  Note The access point does not participate in AQ HeatMap in Prime Infrastructure.

- SE-Connect—This mode enables a user to connect a Spectrum Expert application running on an external Microsoft Windows XP or Vista PC to a Cisco CleanAir-enabled access point in order to display and analyze detailed spectrum data. The Spectrum Expert application connects directly to the access point, bypassing the switch. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the switch. All CleanAir system functionality is suspended while the AP is in this mode, and no clients are served. This mode is intended for remote troubleshooting only. Up to three active Spectrum Expert connections are possible.

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 196

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 197

Configuring Interference Reporting for 2.4-GHz Devices, on page 198

Enabling CleanAir for 5-GHz Band, on page 200

Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 201

Configuring Interference Reporting for 5-GHz devices, on page 202

Restrictions for CleanAir

- Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor access point list. IDR clustering depends on the switch's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- Cisco recommends a ratio of 1 monitor mode access point for every 5 local mode access points, this may also vary based on the network design and expert guidance for best coverage.
- Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 196

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 197

Configuring Interference Reporting for 2.4-GHz Devices, on page 198

Enabling CleanAir for 5-GHz Band, on page 200
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 201
Configuring Interference Reporting for 5-GHz devices, on page 202

Information About CleanAir

Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. All of the users of the shared spectrum can be seen (both native devices and foreign interferers). It also enables the network to act upon this information. For example, the interfering device can be manually removed or the system can automatically change the channel away from the interference.

A Cisco CleanAir system consists of CleanAir-enabled access points, wireless controller modules, mobility controllers, mobility anchors and next generation switches. The access points join the mobility controller directly or through the mobility anchor. They collect information about all devices that operate in the industrial, scientific, and medical (ISM) bands, identify and evaluate the information as a potential interference source, and forward it to the switch. The switch controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure (PI) or a Cisco Mobility Services Engine (MSE) upon request.

Any networking configurations can be performed only on the mobility controller, configurations cannot be performed in the MA mode. However, any radio level CleanAir configurations can be done using mobility anchor.

For every device operating in the unlicensed band, Cisco CleanAir tells what it is, where it is, how it is impacting the wireless network, and what actions should be taken. It simplifies RF.

Wireless LAN systems operate in unlicensed 2.4-GHz and 5-GHz ISM bands. Many devices like microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect the Wi-Fi operations.

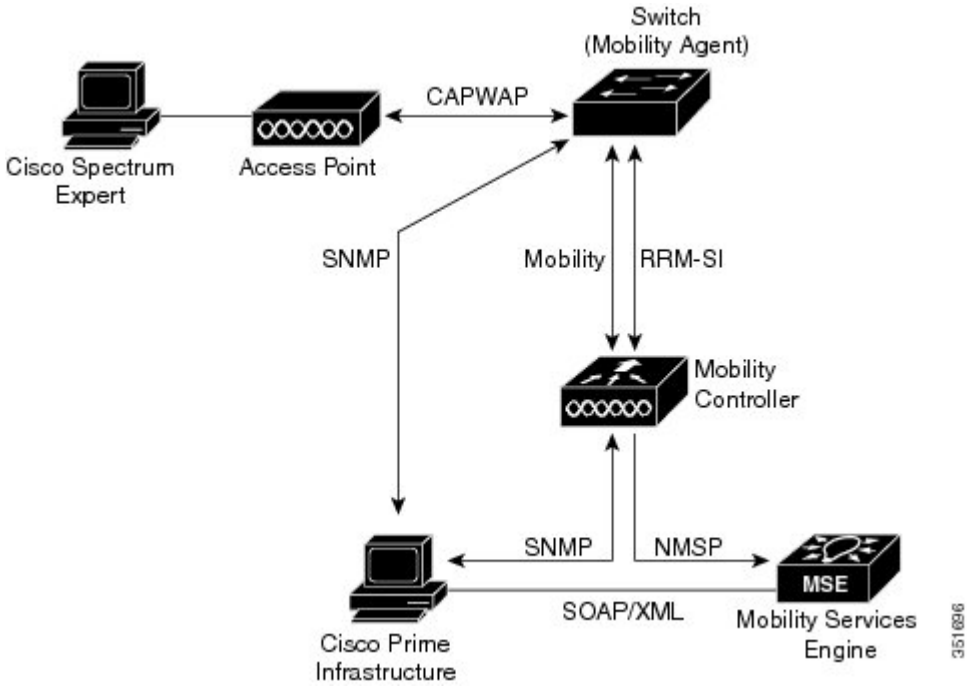
Some of the most advanced WLAN services, such as voice over wireless and IEEE 802.11n radio communications, could be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality addresses this problem of radio frequency (RF) interference.

Cisco CleanAir Components

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and switch. Cisco Prime Infrastructure (PI), Mobility Services Engine (MSE) and Cisco Spectrum Expert are optional system

components. Cisco PI and MSE provide user interfaces for advanced spectrum capabilities such as historic charts, tracking interference devices, location services and impact analysis.

Figure 3: Cisco CleanAir Solution



An access point equipped with Cisco CleanAir technology collects information about non-Wi-Fi interference sources, processes it, and forwards it to the MA. The access point sends AQR and IDR reports to the controller.

The mobility controller (MC) controls and configures CleanAir-capable access points, collects and processes spectrum data, and provides it to the PI and/or the MSE. The MC provides local user interfaces (GUI and CLI) to configure basic CleanAir features and services and display current spectrum information. The MC also does detection, merging and mitigation of interference devices using RRM TPC and DCM. For details on Interference Device Merging, see Interference Device Merging, on page 195.

Cisco PI provides advanced user interfaces for CleanAir that include feature enabling and configuration, consolidated display information, historic AQ records and reporting engines. PI also shows charts of interference devices, AQ trends, and alerts.

Cisco MSE is required for location and historic tracking of interference devices, and provides coordination and consolidation of interference reports across multiple controllers. MSE also provides adaptive Wireless Intrusion Prevention System (WIPS) service that provides comprehensive over-the-air threat detection, location and mitigation. MSE also merges all the interference data.

To obtain detailed spectrum data that can be used to generate RF analysis plots similar to those provided by a spectrum analyzer, you can configure a Cisco CleanAir-enabled access point to connect directly to a Microsoft Windows XP or Vista PC running the Cisco Spectrum Expert application.

The switch performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (CLI, and SNMP) for configuring Cisco CleanAir features and retrieving data.

- Displays spectrum data.
- Collects and processes AQRs from the access point and stores them in the air quality database. AQRs contains information about the total interference from all identified sources represented by Air Quality Index (AQI) and summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per interference type reports which enable you to take action in cases where the interference due to unclassified interfering devices is frequent.
- Collects and processes Interference Device Reports (IDRs) from the access point and stores them in the interference device database.
- Forwards spectrum data to Prime Infrastructure and the MSE.

Terms Used in Cisco CleanAir

Table 8: CleanAir-related Terms

Term	Decription
AQI	Air Quality Index. The AQI is an indicator of air quality, based on the air pollutants. An AQI of 0 is bad and an AQI > 85 is good.
AQR	Air Quality Report. AQRs contain information about the total interference from all identified sources represented by AQI and summary of the most severe interference categories. AQRs are sent every 15 minutes to the Mobility Controller and every 30 seconds in the Rapid mode.
DC	Duty Cycle. Percentage of time that the channel is utilized by a device.
EDRRM	EDRRM Event Driven RRM. EDRRM allows an access point in distress to bypass normal RRM intervals and immediately change channels.
IDR	Interference Device Reports that the access point sends to the controller.
ISI	Interference Severity Index. The ISI is an indicator of the severity of the interference.
MA	Mobility Agent. An MA is either an access switch that has a wireless module running on it or an MC with an internal MA running on it. An MA is the wireless component that maintains client mobility state machine for a mobile client that is connected to an access point to the device that the MA is running on.
MC	Mobility Controller. An MC provides mobility management services for inter-peer group roaming events. The MC provides a central point of contact for management and sends the configuration to all the mobility agents under its sub-domain of their mobility configuration, peer group membership and list of members.
RSSI	Received Signal Strength Indicator. RSSI is a measurement of the power present in a received radio signal. It is the power at which an access point sees the interferer device.

Interference Types that Cisco CleanAir can Detect

Cisco CleanAir can detect interference, report on the location and severity of the interference, and recommend different mitigation strategies. Two such mitigation strategies are persistent device avoidance and spectrum event-driven RRM. New

Wi-Fi chip-based RF management systems share these characteristics:

- Any RF energy that cannot be identified as a Wi-Fi signal is reported as noise.
- Noise measurements that are used to assign a channel plan tend to be averaged over a period of time to avoid instability or rapid changes that can be disruptive to certain client devices.
- Averaging measurements reduces the resolution of the measurement. As such, a signal that disrupts clients might not look like it needs to be mitigated after averaging.
- All RF management systems available today are reactive in nature.

Cisco CleanAir is different and can positively identify not only the source of the noise but also its location and potential impact to a WLAN. Having this information allows you to consider the noise within the context of the network and make intelligent and, where possible, proactive decisions. For CleanAir, two types of interference events are common:

- Persistent interference
- Spontaneous interference

Persistent interference events are created by devices that are stationary in nature and have intermittent but largely repeatable patterns of interference. For example, consider the case of a microwave oven located in a break room. Such a device might be active for only 1 or 2 minutes at a time. When operating, however, it can be disruptive to the performance of the wireless network and associated clients. Using Cisco CleanAir, you can positively identify the device as a microwave oven rather than indiscriminate noise. You can also determine exactly which part of the band is affected by the device, and because you can locate it, you can understand which access points are most severely affected. You can then use this information to direct RRM in selecting a channel plan that avoids this source of interference for the access points within its range. Because this interference is not active for a large portion of the day, existing RF management applications might attempt to again change the channels of the affected access points. Persistent device avoidance is unique, however, in that it remains in effect as long as the source of interference is periodically detected to refresh the persistent status. The Cisco CleanAir system knows that the microwave oven exists and includes it in all future planning. If you move either the microwave oven or the surrounding access points, the algorithm updates RRM automatically.

Note Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interference only if the devices are actively transmitting. Bluetooth devices have extensive power save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

Interference Device Merging

The Interference Devices (ID) messages are processed on a Mobility Controller (MC). The Mobility Anchor (MA) forwards the ID messages from APs and hence they are processed on the MC. The MC has visibility of the neighbor information across APs connected to different MAs.

ID merging logic requires AP neighbor information. Neighbor information is obtained from the RRM module. This api only gives neighbor information to the APs directly connected to MC.

Currently the AP neighbor list on MA is synced to MC once every 3 minutes; hence the AP neighbor list obtained by this api could be at most 3 mins old. This delay results in delay in merging of Devices as they are discovered. The subsequent periodic merge will pick up the updated neighbor information and merge is performed

Persistent Devices

Some interference devices such as outdoor bridges and Microwave Ovens only transmit when needed. These devices can cause significant interference to the local WLAN due to short duration and periodic operation remain largely undetected by normal RF management metrics. With CleanAir the RRM DCA algorithm can detect, measure, register and remember the impact and adjust the DCA algorithm. This minimizes the use of channels affected by the persistent devices in the channel plan local to the interference source. Cisco CleanAir detects and stores the persistent device information in the switch and this information is used to mitigate interfering channels.

Persistent Devices Detection

CleanAir-capable Monitor Mode access point collects information about persistent devices on all configured channels and store the information in controller. Local/Bridge mode AP detects interference devices on the serving channels only.

Persistent Device Avoidance

When a Persistent Device (PD) is detected in the CleanAir module, it is reported to the RRM module on the MA. This information is used in the channel selection by the subsequent EDRRM Event Driven RRM (ED-RRM) signal sent to the RRM module.

EDRRM and AQR Update Mode

EDRRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AQ and reports the AQ every 15 minutes. AQ only reports classified interference devices. The key benefit of EDRRM is very fast action time. If an interfering device is operating on an active channel and causes enough AQ degradation to trigger an EDRRM, then no clients will be able to use that channel or the access point. You must remove the access point from the channel. EDRRM is not enabled by default, you must first enable CleanAir and then enable EDRRM.

AQRs are only available on the MC. The mode configuration and timers are held in Radio Control Block (RCB) on MA (for APs connected to MA). There is no change to the current API available for EMS/NMS. No change is required for directly connected APs as RCB (spectrum config and timers) is available locally. For remote APs (APs connected to MA), three new control messages are added. These three messages are for enable, restart timer and disable rapid update mode for a given AP MAC address and slot.

Related Topics

Configuring EDRRM for CleanAir-Events, on page 203

CleanAir High Availability

CleanAir configuration (network and radio) is stateful during the switchover. On the MC, Embedded Instrumentation Core (EICORE) provides the sync on network configurations across active and standby nodes. The radio configurations are synced using the HA Infrastructre. The CleanAir configurations on MA are pulled from the MC upon joining. The network configuration is not stored in the EICORE on MA, hence it is synced using HA Infrastructure.

CleanAir Data (AQ and IDR) reports are not stateful, that is, the standby and active nodes are not synced. On switchover, the APs send the reports to the current active slot. The RRM Client (HA Infra Client) is used for CleanAir HA sync.

How to Configure CleanAir

Enabling CleanAir for 2.4-GHz Band

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz cleanair**
3. **end**

DETAILED STEPS

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

Step 2	**ap dot11 24ghz cleanair**
	
	Example:
	`Switch(config)#ap dot11 24ghz cleanair`
	`Switch(config)#no ap dot11 24ghz cleanair`
		Enables the CleanAir feature on 802.11b network. Add **no** in the command to disable CleanAir on the 802.11b network.

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

Related Topics

Prerequisites for CleanAir, on page 189
Restrictions for CleanAir, on page 190
CleanAir FAQs, on page 210

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value*
3. **ap dot11 24ghz cleanair alarm device** {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** }
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value* **Example:** `Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50`	Configures the alarm for the threshold value for air-quality for all the 2.4-GHz devices. Add the **no** form of this command to disable the alarm.
Step 3	**ap dot11 24ghz cleanair alarm device** {**bt-discovery**	**bt-link**	**canopy**	**cont-tx**	**dect-like**	**fh**	**inv**	**jammer**	**mw-oven**	**nonstd**	**report**	**superag**	**tdd-tx**	**video**	**wimax-fixed**	**wimax-mobile**	**xbox**	**zigbee** } **Example:** `Switch(config)#ap dot11 24ghz cleanair alarm device canopy`	Configures the alarm for the 2.4-GHz devices. Add the **no** form command to disable the alarm. • **bt-discovery—**Bluetooth Discovery. • **bt-link—**Bluetooth Link. • **canopy—**Canopy devices. • **cont-tx—**Continuous Transmitter. • **dect-like—**Digital Enhanced Cordless Communication (DECT)-like phone. • **fh—**802.11 frequency hopping devices. • **inv—**Devices using spectrally inverted WiFi signals. • **jammer—**Jammer.

	Command or Action	Purpose
		• **mw-oven—**Microwave oven. • **nonstd—**Devices using non standard Wi-Fi channels. • **report—**Interference device reporting. • **superag—**802.11 SuperAG devices. • **tdd-tx—**TDD Transmitter. • **video—**Video cameras. • **wimax-fixed—**WiMax Fixed. • **wimax-mobile—**WiMax Mobile. • **xbox—**Xbox. • **zigbee—**802.15.4 devices.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 189
Restrictions for CleanAir, on page 190
CleanAir FAQs, on page 210

Configuring Interference Reporting for 2.4-GHz Devices

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz cleanair device**{**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** }
3. **end**

DETAILED STEPS

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

Step 2	**ap dot11 24ghz cleanair device** {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee** }
	
	Example:
	`Switch(config)# ap dot11 24ghz cleanair device bt-discovery`
	`Switch(config)# ap dot11 24ghz cleanair device bt-link`
	`Switch(config)# ap dot11 24ghz cleanair device canopy`
	`Switch(config)# ap dot11 24ghz cleanair device cont-tx`
	`Switch(config)# ap dot11 24ghz cleanair device dect-like`
	`Switch(config)# ap dot11 24ghz cleanair device fh`
	`Switch(config)# ap dot11 24ghz cleanair device inv`
	`Switch(config)# ap dot11 24ghz cleanair device jammer`
	`Switch(config)# ap dot11 24ghz cleanair device mw-oven`
	`Switch(config)# ap dot11 24ghz cleanair device nonstd`
	`Switch(config)# ap dot11 24ghz cleanair device report`
	`Switch(config)# ap dot11 24ghz cleanair device superag`
	`Switch(config)# ap dot11 24ghz cleanair device tdd-tx`
	`Switch(config)# ap dot11 24ghz cleanair device video`
	`Switch(config)# ap dot11 24ghz cleanair device wimax-fixed`
	`Switch(config)# ap dot11 24ghz cleanair device wimax-mobile`
	`Switch(config)# ap dot11 24ghz cleanair device xbox`
	`Switch(config)# ap dot11 24ghz cleanair device zigbee`
		Configures the 2.4 GHz interference devices to report to the switch. Use the **no** form of this command to disable the configuration.
		• **bt-discovery—**Bluetooth Discovery
		• **bt-link—**Bluetooth Link
		• **canopy—**Canopy devices
		• **cont-tx**- Continuous Transmitter
		• **dect-like**- Digital Enhanced Cordless Communication (DECT) like phone
		• **fh**- 802.11 frequency hopping devices
		• **inv**- Devices using spectrally inverted WiFi signals
		• **jammer**- Jammer
		• **mw-oven**- Microwave Oven
		• **nonstd**- Devices using non-standard WiFi channels
		• **report**- no description
		• **superag**- 802.11 SuperAG devices
		• **tdd-tx**- TDD Transmitter
		• **video**- Video cameras
		• **wimax-fixed**- WiMax Fixed
		• **wimax-mobile**- WiMax Mobile
		• **xbox**- Xbox
		• **zigbee**- 802.15.4 devices

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

Related Topics

Prerequisites for CleanAir, on page 189
Restrictions for CleanAir, on page 190
CleanAir FAQs, on page 210

Enabling CleanAir for 5-GHz Band

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 5ghz cleanair**
3. **end**

DETAILED STEPS

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

Step 2	**ap dot11 5ghz cleanair**
	
	Example:
	`Switch(config)#ap dot11 5ghz cleanair`
	
	`Switch(config)#no ap dot11 5ghz cleanair`
		Enables the CleanAir feature on 802.11a network. Add **no** in the command to disable CleanAir on the 802.11a network.

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

Related Topics

Prerequisites for CleanAir, on page 189
Restrictions for CleanAir, on page 190
CleanAir FAQs, on page 210

Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value*
3. **ap dot11 5ghz cleanair alarm device**{**canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile**}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value* **Example:** `Switch(config)#ap dot11 5ghz cleanair alarm air-quality threshold 50`	Configures the alarm for the threshold value for air-quality for all the 5-GHz devices. Add the **No** form of the command to disable the alarm.
Step 3	**ap dot11 5ghz cleanair alarm device**{**canopy	cont-tx	dect-like	inv	jammer	nonstd	radar	report	superag	tdd-tx	video	wimax-fixed	wimax-mobile**} **Example:** `Switch(config)#ap dot11 5ghz cleanair alarm device`	Configures the alarm for the 5-GHz devices. Add the **no** form of the command to disable the alarm. • **canopy—**Canopy devices. • **cont-tx—**Continuous Transmitter. • **dect-like—**Digital Enhanced Cordless Communication (DECT) like phone. • **fh—**802.11 frequency hopping devices. • **inv—**Devices using spectrally inverted WiFi signals. • **jammer—**Jammer. • **nonstd—**Devices using non-standard WiFi channels. • **radar—**Radars. • **report—**Interference device reporting. • **superag—**802.11 SuperAG devices. • **tdd-tx—**TDD Transmitter. • **video—**Video cameras. • **wimax-fixed—**WiMax Fixed.

	Command or Action	Purpose
		• **wimax-mobile**—WiMax Mobile.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 189
Restrictions for CleanAir, on page 190
CleanAir FAQs, on page 210

Configuring Interference Reporting for 5-GHz devices

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 5ghz cleanair device**{**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz cleanair device**{**canopy**	**cont-tx**	**dect-like**	**inv**	**jammer**	**nonstd**	**radar**	**report**	**superag**	**tdd-tx**	**video**	**wimax-fixed**	**wimax-mobile**} **Example:** `Switch(config)#ap dot11 5ghz cleanair device canopy` `Switch(config)#ap dot11 5ghz cleanair device cont-tx` `Switch(config)#ap dot11 5ghz cleanair device dect-like` `Switch(config)#ap dot11 5ghz cleanair device inv`	Configures the 5-GHz interference devices to report to the switch. Add the **no** form of the command to disable interference device reporting. • **canopy**—Canopy devices • **cont-tx**—Continuous Transmitter • **dect-like**—Digital Enhanced Cordless Communication (DECT) like phone • **fh**—802.11 frequency hopping devices • **inv**—Devices using spectrally inverted WiFi signals • **jammer**—Jammer

	Command or Action	Purpose

	`Switch(config)#ap dot11 5ghz cleanair device jammer`
	`Switch(config)#ap dot11 5ghz cleanair device nonstd`
	`Switch(config)#ap dot11 5ghz cleanair device radar`
	`Switch(config)#ap dot11 5ghz cleanair device report`
	`Switch(config)#ap dot11 5ghz cleanair device superag`
	`Switch(config)#ap dot11 5ghz cleanair device tdd-tx`
	`Switch(config)#ap dot11 5ghz cleanair device video`
	`Switch(config)#ap dot11 5ghz cleanair device wimax-fixed`
	`Switch(config)#ap dot11 5ghz cleanair device wimax-mobile`
		• **nonstd—**Devices using non-standard WiFi channels
		• **radar—**Radars
		• **report—**Interference device reporting
		• **superag—**802.11 SuperAG devices
		• **tdd-tx—**TDD Transmitter
		• **video—**Video cameras
		• **wimax-fixed—**WiMax Fixed
		• **wimax-mobile—**WiMax Mobile

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

Related Topics

Prerequisites for CleanAir, on page 189
Restrictions for CleanAir, on page 190
CleanAir FAQs, on page 210

Configuring EDRRM for CleanAir-Events

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event**
3. **ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high** | **low** | **medium**}]
4. **end**

DETAILED STEPS

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

	Command or Action	Purpose

Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event**
	
	Example:
	`Switch(config)#ap dot11 24ghz rrm channel cleanair-event`
	`Switch(config)#no ap dot11 24ghz rrm channel cleanair-event`
		Enables EDRRM cleanair-event. Add the **no** form of the command to disable EDRRM.

Step 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high** | **low** | **medium**}] **Example:** `Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures the EDRRM sensitivity of cleanair-event. • **High—**Specifies the most sensitivity to non Wi–Fi interference as indicated by the air quality (AQ) value. • **Low—**Specifies the least sensitivity to non Wi–Fi interference as indicated by the AQ value. • **Medium—**Specifies medium sensitivity to non Wi–Fi interference as indicated by the AQ value.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

EDRRM and AQR Update Mode, on page 195

Configuring Persistent Device Avoidance

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11** {**24ghz** | **5ghz**} **rrm channel device**
3. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** **Example:** `Switch(config)#ap dot11 24ghz rrm channel device`	Enables the persistent non Wi–Fi device avoidance in the 802.11 channel assignment. Add the **no** form of the command to disable the persistent device avoidance.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Cisco CleanAir using the Controller GUI

Configuring Cisco Spectrum Expert

Configuring Spectrum Expert (CLI)

Before You Begin

- Spectrum Expert (Windows XP laptop client) and access point should be pingable, otherwise; it will not work.
- Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.
- The access point must be a TCP server listening on ports 37540 for 2.4-GHz and 37550 for 5-GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.
- You can view the NSI key from the switch CLI by using the **show ap name** *ap_name* **config dot11** {**24ghz** | **5ghz**} command.

Step 1 To configure the access point for SE-Connect mode, enter this command:
ap name *ap_name* **mode se-connect**

Example:
```
Switch#ap name Cisco_AP3500 mode se-connect
```

Step 2 When prompted to reboot the access point, enter **Y**.

Step 3 To view the NSI key for the access point, enter this command:
show ap name *ap_name* **config dot11** {**24ghz** | **5ghz**}

Example:

```
Switch#show ap name Cisco_AP3500 config dot11 24ghz

<snippet>
CleanAir Management Information
    CleanAir Capable                          : Yes
    CleanAir Management Admin State           : Enabled
    CleanAir Management Operation State       : Up
    CleanAir NSI Key                          : 274F1F9B1A5206683FAF57D87BFFBC9B
    CleanAir Sensor State                     : Configured

<snippet>
```

What to Do Next

On the Windows PC, download Cisco Spectrum Expert:

- Access the Cisco Software Center from this URL: http://www.cisco.com/cisco/software/navigator.html
- Click **Product > Wireless > Cisco Spectrum Intelligence** > **Cisco Spectrum Expert** > **Cisco Spectrum Expert Wi-Fi**, and then download the Spectrum Expert 4.1.11 executable (*.exe) file.
- Run the Spectrum Expert application on the PC.
- When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

  When an access point in SE-Connect mode joins a switch, it sends a Spectrum Capabilities notification message, and the switch responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the switch for use in NSI authentication. The switch generates one key per access point, which the access point stores until it is rebooted.

  Note You can establish up to three Spectrum Expert console connections per access point radio.

- Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.
- Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Monitoring CleanAir Parameters

You can monitor CleanAir parameters using the following commands:

Table 9: Commands for Monitoring CleanAir

Commands	Description
show ap dot11 24ghz cleanair air-quality summary	Displays CleanAir Air Quality (AQ) data for 2.4-GHz band
show ap dot11 24ghz cleanair air-quality worst	Displays CleanAir Air Quality (AQ) worst data for 2.4-GHz band
show ap dot11 24ghz cleanair config	Displays CleanAir Configuration for 2.4-GHz band
show ap dot11 24ghz cleanair device type all	Displays all CleanAir Interferers for 2.4-GHz band
show ap dot11 24ghz cleanair device type bt-discovery	Displays CleanAir Interferers of type BT Discovery for 2.4-GHz band
show ap dot11 24ghz cleanair device type bt-link	Displays CleanAir Interferers of type BT Link for 2.4-GHz band
show ap dot11 24ghz cleanair device type canopy	Displays CleanAir Interferers of type Canopy for 2.4-GHz band
show ap dot11 24ghz cleanair device type cont-tx	Displays CleanAir Interferers of type Continuous transmitter for 2.4-GHz band
show ap dot11 24ghz cleanair device type dect-like	Displays CleanAir Interferers of type DECT Like for 2.4-GHz band
show ap dot11 24ghz cleanair device type fh	Displays CleanAir Interferers of type 802.11FH for 2.4-GHz band
show ap dot11 24ghz cleanair device type inv	Displays CleanAir Interferers of type WiFi Inverted for 2.4-GHz band
show ap dot11 24ghz cleanair device type jammer	Displays CleanAir Interferers of type Jammer for 2.4-GHz band
show ap dot11 24ghz cleanair device type mw-oven	Displays CleanAir Interferers of type MW Oven for 2.4-GHz band
show ap dot11 24ghz cleanair device type nonstd	Displays CleanAir Interferers of type WiFi Inv. Ch for 2.4-GHz band
show ap dot11 24ghz cleanair device type persistent	Displays CleanAir Interferers of type Persistent for 2.4-GHz band
show ap dot11 24ghz cleanair device type superag	Displays CleanAir Interferers of type SuperAG for 2.4-GHz band

Commands	Description
show ap dot11 24ghz cleanair device type tdd-tx	Displays CleanAir Interferers of type TDD Transmit for 2.4-GHz band
show ap dot11 24ghz cleanair device type video	Displays CleanAir Interferers of type Video Camera for 2.4-GHz band
show ap dot11 24ghz cleanair device type wimax-fixed	Displays CleanAir Interferers of type WiMax Fixed for 2.4-GHz band
show ap dot11 24ghz cleanair device type wimax-mobile	Displays CleanAir Interferers of type WiMax Mobile for 2.4-GHz band
show ap dot11 24ghz cleanair device type xbox	Displays CleanAir Interferers of type Xbox for 2.4-GHz band
show ap dot11 24ghz cleanair device type zigbee	Displays CleanAir Interferers of type zigbee for 2.4-GHz band
show ap dot11 5ghz cleanair air-quality summary	Displays CleanAir Air Quality (AQ) data for 5-GHz band
show ap dot11 5ghz cleanair air-quality worst	Displays CleanAir Air Quality (AQ) worst data for 5-GHz band
show ap dot11 5ghz cleanair config	Displays CleanAir Configuration for 5-GHz band
show ap dot11 5ghz cleanair device type all	Displays all CleanAir Interferers for 5-GHz band
show ap dot11 5ghz cleanair device type canopy	Displays CleanAir Interferers of type Canopy for 5-GHz band
show ap dot11 5ghz cleanair device type cont-tx	Displays CleanAir Interferers of type Continuous TX for 5-GHz band
show ap dot11 5ghz cleanair device type dect-like	Displays CleanAir Interferers of type DECT Like for 5-GHz band
show ap dot11 5ghz cleanair device type inv	Displays CleanAir Interferers of type WiFi Inverted for 5-GHz band
show ap dot11 5ghz cleanair device type jammer	Displays CleanAir Interferers of type Jammer for 5-GHz band
show ap dot11 5ghz cleanair device type nonstd	Displays CleanAir Interferers of type WiFi Inv. Ch for 5-GHz band
show ap dot11 5ghz cleanair device type persistent	Displays CleanAir Interferers of type Persistent for 5-GHz band

Commands	Description
show ap dot11 5ghz cleanair device type superag	Displays CleanAir Interferers of type SuperAG for 5-GHz band
show ap dot11 5ghz cleanair device type tdd-tx	Displays CleanAir Interferers of type TDD Transmit for 5-GHz band
show ap dot11 5ghz cleanair device type video	Displays CleanAir Interferers of type Video Camera for 5-GHz band
show ap dot11 5ghz cleanair device type wimax-fixed	Displays CleanAir Interferers of type WiMax Fixed for 5-GHz band
show ap dot11 5ghz cleanair device type wimax-mobile	Displays CleanAir Interferers of type WiMax Mobile for 5-GHz band

Monitoring the Interference Devices

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed which results in the spectrum sensor to temporarily stop detecting the device. This device is then correctly marked as down. A down device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific devices are reported, the cluster ID is kept alive for an extended period of time to prevent possible device detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device detection history is preserved.

For example, some bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Configuration Examples for Configuring CleanAir

Enabling CleanAir on 2.4-GHz Band and an Access Point: Example

This example shows how to enable CleanAir on the 2.4-GHz band and an access point operating in the channel:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair
Switch(config)#exit
Switch#ap name TAP1 dot11 24ghz cleanair
Switch#end
```

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices: Example

This example shows how to configure a CleanAir Alarm for 2.4-GHz Air-Quality threshold of 50 dBm and an Xbox device:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50
Switch(config)#ap dot11 24ghz cleanair alarm device xbox
Switch(config)#end
```

Configuring Interference Reporting for 5-GHz Devices: Example

This example shows how to configure interference reporting for 5-GHz devices:

```
Switch#configure terminal
Switch(config)#ap dot11 5ghz cleanair alarm device xbox
Switch(config)#end
```

Configuring EDRRM for CleanAir-Events: Example

This example shows how to enable an EDRRM cleanair-event in the 2.4-GHz band and configure high sensitivity to non Wi–Fi interference:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel cleanair-event
Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Switch(config)#end
```

Configuring Persistent Device Avoidance: Example

This example shows how to enable persistent non Wi–Fi device avoidance in the 2.4-GHz band:

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel device
Switch(config)#end
```

Configuring an Access Point for SE-Connect Mode: Example

This example shows how to configure an access point in the SE-Connect mode:

```
Switch#ap name Cisco_AP3500 mode se-connect
```

CleanAir FAQs

Q. How do I check if my MC is up?

A. To check if the MC is up, use the command: **show wireless mobility summary**.

This example shows how to display the mobility summary:

```
Switch#show wireless mobility summary

Mobility Controller Summary:
Mobility Role                                 : Mobility Controller
Mobility Protocol Port                        : 16666
Mobility Group Name                           : MG-AK
Mobility Oracle                               : Disabled
Mobility Oracle IP Address                    : 0.0.0.0
DTLS Mode                                     : Enabled
Mobility Domain ID for 802.11r                : 0x39b2
Mobility Keepalive Interval                   : 10
Mobility Keepalive Count                      : 3
Mobility Control Message DSCP Value           : 48
Mobility Domain Member Count                  : 2
```

```
Link Status is Control Link Status : Data Link Status
Controllers configured in the Mobility Domain:
IP              Public IP       Group Name       Multicast IP     Link Status
------------------------------------------------------------------------------
9.6.136.10      -               MG-AK            0.0.0.0          UP   : UP
```

Q. Multiple access points detect the same interference device, however, the switch shows them as separate clusters or different suspected devices clustered together. Why does this happen?

A. Access points must be RF neighbors for the switch to consider the merging of devices that are detected by these access points. The access point takes time to establish neighbor relationships. A few minutes after the switch reboots or a change in the RF group and similar events, clustering will not be very accurate.

Q. Can I merge two monitor mode access points using a switch?

A. No, you cannot merge two monitor mode access points using a switch. You can merge the monitor mode access points only using MSE.

Q. How do I view neighbor access points?

A. To view neighbor access points, use the command: **show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**}

This example shows how to display the neighbor access points:

```
Switch#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                        :  -12 dBm on   1 (10.10.0.5)
  AP 0C85.25AB.CCA0 slot 0                        :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25C7.B7A0 slot 0                        :  -26 dBm on  11 (10.10.0.5)
  AP 0C85.25DE.2C10 slot 0                        :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25DE.C8E0 slot 0                        :  -14 dBm on  11 (10.10.0.5)
  AP 0C85.25DF.3280 slot 0                        :  -31 dBm on   6 (10.10.0.5)
  AP 0CD9.96BA.5600 slot 0                        :  -44 dBm on   6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0                        :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. What are the debug commands available for CleanAir?

A. The debug commands for CleanAir are:

debug cleanair {**all** | **error** | **event** | **internal-event** | **nmsp** | **packet**}

debug rrm {**all** | **channel** | **detail** | **error** | **group** | **ha** | **manager** | **message** | **packet** | **power** | **prealarm** | **profile** | **radar** | **rf-change** | **scale** | **spectrum**}

Q. Why are CleanAir Alarms not generated for interferer devices?

A. Verify that the access points are CleanAir-capable and CleanAir is enabled both on the access point and the switch.

Q. Can the Cisco Catalyst 3850 Series Switches function as a Mobility Agent (MA)?

A. Yes, the Cisco Catalyst 3850 Series Switches can function as an MA.

Q. Are CleanAir configurations available on the MA?

A. From Release 3.3 SE, CleanAir configurations are available on the MA. You can use the following two CleanAir commands on the MA:

- **show ap dot11 5ghz cleanair config**
- **show ap dot11 24ghz cleanair config**

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 196
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 197
Configuring Interference Reporting for 2.4-GHz Devices, on page 198
Enabling CleanAir for 5-GHz Band, on page 200
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 201
Configuring Interference Reporting for 5-GHz devices, on page 202

Additional References

Related Documents

Related Topic	Document Title
CleanAir commands and their details	*CleanAir Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
High Availability configurations	*High Availability Configuration Guide, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*
High Availability commands and their details	*High Availability Command Reference, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

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

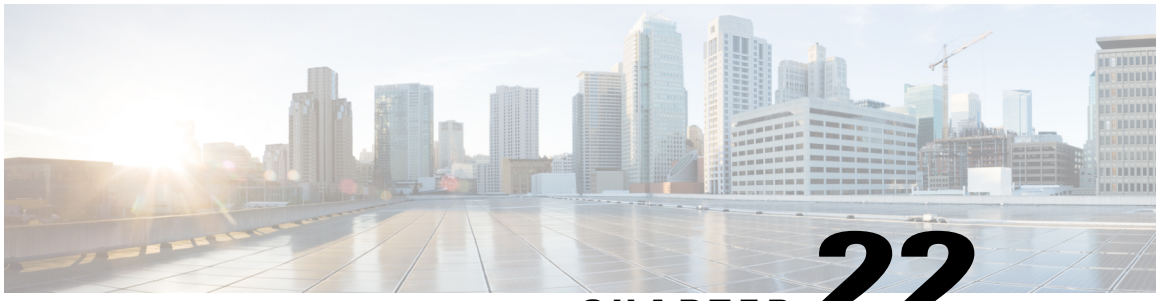
Technical Assistance

Description	Link
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.	http://www.cisco.com/support

PART VI

Mobility

- Information About Mobility, page 217
- Mobility Network Elements, page 223
- Mobility Control Protocols, page 227
- Intra Sub Domain Mobility, page 235
- Inter Sub Domain Mobility, page 239
- Mobility Controller and Mobility Tunnel Endpoint Redundancy, page 243
- Configuring Mobility, page 245



CHAPTER 22

Information About Mobility

- Overview, page 217
- Wired and Wireless Mobility, page 218
- Features of Mobility, page 218
- Sticky Anchoring for Low Latency Roaming, page 220
- Bridge Domain ID and L2/L3 Roaming, page 220
- Link Down Behavior, page 220
- Platform Specific Scale Requirement for the Mobility Controller, page 220

Overview

The switch delivers more services at access layer other than merely providing increased speeds and feeds. Wireless services is now integrated with the switch, which ensures that the access layer switch terminates the wireless users data plane, thereby delivering on the promise of Cisco's unified architecture. Unification implies that mobility services are provided to both wireless and wired stations.

The switch provides seamless roaming, which requires transparency of the network configuration and deployment options to the client.

From the end user's perspective, any mobility event must not change its IP address, its default router or DHCP server. This means that as stations roam, they must be able to

- Send an ARP to their default router, or
- Transmit a DHCP request to the server that had previously assigned their address.

From the infrastructure's perspective, as mobility events occur, the station's traffic must follow its current point of attachment, which can either be a mobility agent (MA) or mobility controller (MC). This must be true regardless of whether the station has moved to a network that is configured for a different subnet. The period from which the station is not receiving traffic following its mobility event must be as short as possible, even below 40 ms whenever possible, which includes any authentication procedures that are required.

From the infrastructure's perspective, the mobility management solution must have four main components, and all of these functions must be performed within the constraints of roaming:

- Initial Association—This function is used to identify the user's new point of attachment in the network.
- Context Transfer—This function is used to transfer state information associated with the station. This ensures that the station's static and real-time policies, including security and application ACLs, and services, remain the same across handoffs.
- Handoff—This function is used to signal that the station's point of attachment has changed, and control of the station should be relinquished by the previous access switch.
- Data Plane—This function is typically tied to the handoff process, and ensures that the station's traffic continues to be delivered and received from the station without any noticeable performance degradation.

Wired and Wireless Mobility

One of the key features of the Converged access solution (applicable to both the Cisco Catalyst 3850 Switch and Cisco WLC 5700 Series Controller) is its ability to provide a device with an IP address and maintain its session persistence, across mobility events from ethernet connections to wireless and vice-versa. This feature allows users to remain on an ethernet network when possible, and make use of the freedom of mobility associated with wireless when necessary.

This feature leverages support from both the client and the infrastructure and uses the two factor authentication-device and user. The device authentication credentials is cached in the mobility controller (MC). When a device transitions across link layers, the device credentials is validated, and if a match is found, the MC ensures that the same IP address is assigned to the new interface.

Features of Mobility

- Mobility Controller (MC)—The controller provides mobility management services for inter-peer group roaming events. The MC provides a central point of contact for management and policy based control protocols, such as RADIUS. This eliminates the need for the infrastructure servers to maintain a user's location as it transitions throughout the network. The MC sends the configuration to all the mobility agents under its sub-domain of their mobility configuration, peer group membership and list of members. A sub-domain is synonymous to the MC that forms it. Each sub-domain consists of an MC and zero or more access switches that have AP's associated to them.
- Mobility Agents (MA)— A mobility agent is either an access switch that has a wireless module running on it or an MC with an internal MA running on it. A mobility agent is the wireless component that maintains client mobility state machine for a mobile client that is connected via an AP to the device that the MA is running on.
- Mobility Sub Domain— It is an autonomous portion of the mobility domain network. A mobility sub-domain comprises of a single mobility controller and its associated mobility agents (MAs).

  Note Even when more than one mobility controller is present, only one MC can be active at any given time.

  A mobility sub-domain is the set of devices managed by the active mobility controller. A mobility sub-domain comprises of a set of mobility agents and associated access points.

- Mobility Group— A collection of mobility controllers (MCs) across which fast roaming is supported. The concept of mobility group is the same as a collection of buildings in a campus across which frequent roaming is expected.
- Mobility Domain— A collection of mobility sub-domains across which mobility is supported. The term mobility domain may be the same as a campus network.
- Mobility Oracle (MO)—The mobility oracle acts as the point of contact for mobility events that occur across mobility sub-domains. It also maintains a local database of each station in the entire mobility domain, their home and current sub-domain. A mobility domain includes one or more mobility oracle, though only one would be active at any given time.
- Mobility Tunnel Endpoint (MTE)— The mobility tunnel endpoint (MTE) provides data plane services for mobile devices through the use of tunneling. This minimizes the impact of roaming events on the network by keeping the user's point of presence on the network a constant.
- Point of Attachment— A station's point of attachment is where its data path is initially processed upon entry in the network. This could either be the access switch that is currently providing it service, or the wireless LAN controller.
- Point of Presence— A station's point of presence is the place in the network where the station is being advertised. For instance, if an access switch is advertising reachability to the station via a routing protocol, the interface on which the route is being advertised is considered the station's point of presence.
- Switch Peer Group (SPG)— A peer group is a statically created list of neighboring access switches between which fast mobility services is provided. A peer group limits the scope of interactions between switches during handoffs to only those that are geographically proximate.
- Station—A user's device that connects to and requests service from the network. The device may have a wired, wireless or both interfaces.
- Switch in the same SPG—A peer switch that is part of the peer group of the local switch.
- Switch outside the SPG—A peer access switch that is not part of the local switch's peer group.
- Foreign Mobility Controller— The mobility controller providing mobility management service for the station in a foreign mobility sub-domain. The foreign mobility controller acts as a liaison between access switches in the foreign sub-domain and the mobility controller in the home domain.
- Foreign Mobility Sub-Domain— The mobility sub-domain, controlled by a mobility controller, supporting a station which is anchored in another mobility sub-domain
- Foreign Switch— The access switch in the foreign mobility sub-domain currently providing service to the station.
- Anchor Mobility Controller— The mobility controller providing a single point of control and mobility management service for stations in their home mobility sub-domain.
- Anchor Mobility Sub-Domain— The mobility sub-domain, controlled by a mobility controller, for a station where its IP address was assigned.
- Anchor Switch— The switch in the home mobility sub-domain that last provided service to a station.

Sticky Anchoring for Low Latency Roaming

Sticky Anchoring ensures low roaming latency from the client's point of presence is maintained at the switch where the client initially joins the network. It is expensive to apply client policies at a switch for a roaming client. There can be considerable delay as it involves contacting the AAA server for downloadable ACLs which is not acceptable for restoring time sensitive client traffic.

To manage this delay, when the client roams between APs connected to different switches , irrespective of whether it is an intra sub-domain roam or inter sub-domain roam, the client traffic is always tunneled to the switch where the client first associates. The client is anchored at its first point of attachment for its lifetime in the network.

This behavior is enabled by default. You can also disable this behavior to allow the client anchoring only for inter-subnet roams. This configuration is per WLAN config and is available under the WLAN config mode. The customer can configure different SSIDs for time sensitive and non time sensitive applications.

Bridge Domain ID and L2/L3 Roaming

Bridge domain ID provides the mobility nodes with information to decide on specific roam type, either as L2 or L3 roam. It also allows the network administrators to reuse the VLAN IDs across network distribution. When the VLAN IDs do not have the associated subnet configurations, they may require additional parameter to use in conjunction with VLAN ID. The network administrator ensures that the given VLAN under the same bridge domain ID are associated with the unique subnet. The mobility nodes will first check for the bridge domain ID for the given node and the VLAN ID associated with the client to identify the roam type. The bridge domain ID and the VLAN ID must be same to treat a roam as L2 roam.

The bridge domain ID is configured for each SPG when creating a SPG and later on the MC. The bridge domain ID could be same for more than one SPG and all the MAs under the SPG will share the same bridge domain ID. This information is pushed to the MAs as part of the configuration download when MA comes up initially. If the bridge domain ID is modified when the system is up, it will be pushed to all the MAs in the modified SPG and will take immediate effect for the future roams.

Note The MC can also have a bridge domain ID for it self, as the MC can also be part of a SPG.

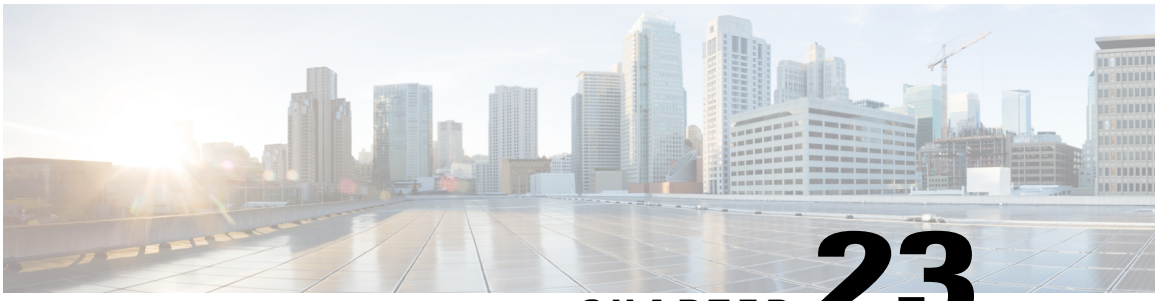
Link Down Behavior

This section provides information about data synchronization between MA-MC and MC-MO when MC or MO faces downtime in absence of redundancy manager. When Keepalive is configured between MA-MC or MC-MO the clients database is synchronized between the MO and the MCs and the MC and its MAs respectively.

Platform Specific Scale Requirement for the Mobility Controller

The Mobility Controller (MC) role is supported on a number of different platforms like, the Cisco WLC 5700 Series, CUWN and Catalyst 3850 Switches. The scale requirements on these three platforms are summarized in the table below:

Scalability	Catalyst 3850 as MC	Catalyst 3650 as MC	Cisco WLC 5700 as MC	CUWN 5508 as MC	WiSM2 as MC
Max number of MC in Mobility Domain	8	8	72	72	72
Max number of MC in Mobility Group	8	8	24	24	24
Max number of MAs in Sub-domain (per MC)	16	16	350	350	350
Max number of SPGs in Sub-domain (per MC)	8	8	24	24	24
Max number of MAs in a SPG	16	16	64	64	64



CHAPTER 23

Mobility Network Elements

- Mobility Agent, page 223
- Mobility Controller, page 224
- Mobility Oracle, page 225
- Guest Controller, page 225

Mobility Agent

A Mobility Controller resides on the switch. It is both, control path and data path entity and is responsible for:

- Handling the mobility events on the switch
- Configuring the datapath elements on the switch for mobility, and
- Communicating with the mobility controller

As MA, the switch performs the datapath functions by terminating the CAPWAP tunnels that encapsulate 802.11 traffic sourced by wireless stations.

This allows the switch to apply features to wired and wireless traffic in a uniform fashion. As far as switch is concerned, 802.11 is just another access medium.

The MA performs the following functions:

- Support the mobility protocol – The MA is responsible for responding in a timely manner, ensuring the switch is capable of achieving its roaming budget.
- Point of presence – If the wireless subnets are not available at the MC, the MA assumes the point of presence if the wireless client VLAN is not available at the new point of attachment and tunnel the client traffic accordingly.
- ARP Server – When the network is configured in a layer 2 mode, the MA is responsible for advertising reachability for the stations connected to it. If tunneling is employed, the ARP request is transmitted on behalf of the station through the tunnel, which the point of presence (anchor switch) would bridge onto its uplink interface.

- Proxy IGMP – The MA on the switch is responsible for subscribing to multicast groups on behalf of a station after a roaming event has occurred. This information is passed as part of the context to the new switch. This ensures the multicast flows follow the user as it roams.
- Routing – When the switch is connected to a layer 3 access network, the MA is responsible for injecting routes for the stations that are associated with it for which tunneling is not provided.
- 802.1X Authenticator – The authenticator function is included in the MA, and handles both wired and wireless stations.
- Secure PMK Sharing – When a station successfully authenticates to the network, the MA forwards the PMK to the MC. The MC is responsible for flooding the PMK to all the MAs under its sub-domain and to the peer MCs in the mobility group.

The MA also performs the following datapath functions:

- Mobility tunnel – If tunneling is used, the MA encapsulates and decapsulates packets from the mobility tunnel to the MC, and to other MA in the peer group, if the access switches are serving as points of presence. The MA supports the tunneling of client data traffic between the point of attachment and the point of attachment. The packet format used for other switches is CAPWAP with an 802.3 payload. The MA also supports reassembly and fragmentation for mobility tunnels.
- Encryption – The mobility control traffic between the mobility nodes is DTLS encrypted. The MA also encrypts the CAPWAP control and data (optional) at the point of attachment.
- CAPWAP – The switch supports the CAPWAP control and data planes. The switch forwarding logic is responsible for terminating the CAPWAP tunnels with 802.11 as well as 802.3 payloads. Since support for large frames (greater than 1500bytes) is not universally available, the switch supports CAPWAP fragmentation and reassembly.

Mobility Controller

The main function of mobility controller is to coordinate the client roaming beyond a switch peer group. The other features of the mobility controller are:

- Station Database—The Mobility Controller maintains a database of all the clients that are connected within the local mobility sub-domain.
- Mobility Protocol—The MC supports the mobility protocol which ensures the target roaming point responds in a timely manner and achieves the 150ms roaming budget
- Interface to Mobility Oracle—The Mobility Controller acts as a gateway between the switch and the Mobility Oracle. When the Mobility Controller does not find a match in its local database, it suggests a match for a wireless client entry (in its database) and forwards the request to the Mobility Oracle, which manages the Mobility Domain.

Note Mobility Oracle function can be enabled on an MC only if it is supported by the platform.

- ARP Server—When tunneling is employed for a station, its point of presence on the network is the Mobility Tunnel Endpoint (MTE). The Mobility Controller responds to any ARP requests received for the stations it is responsible for.

- Routing—When the Mobility Controller is connected to a layer three network, the Mobility Controller is responsible for injecting routes for the stations it supports into the network.
- Configures MTE—The Mobility Controller is the control point for the switch for all mobility management related requests. When a change in a station's point of attachment occurs, the Mobility Controller is responsible for configuring the forwarding policy on the MTE.
- NTP Server—The Mobility Controller acts as an NTP server to the switch and supports all the nodes to have their clocks synchronized with it.

Mobility Oracle

The Mobility Oracle coordinates the client roams beyond the subdomain on a need basis and consists of the following features:

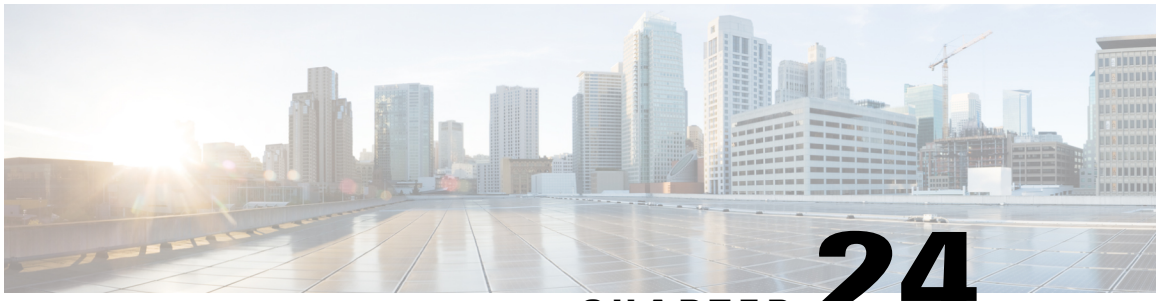
- Station Database—The Mobility Oracle maintains a database of all stations that are serviced within the mobility domain. This database is populated during the Mobility Oracle's interactions with all the Mobility Controllers, in all of the mobility sub-domains it supports.
- Interface to Mobility Controller—When the Mobility Oracle receives a request from a Mobility Controller, it performs a station lookup, and forwards, whenever needed, the request to the proper Mobility Controller.
- NTP Server—The Mobility Oracle acts as an NTP server to the Mobility Controllers and synchronizes all the **switch** clocks within the mobility domain.

Guest Controller

The guest access feature provides guest access to wireless clients. The guest tunnels use the same format as the mobility tunnels. Using the guest access feature, there is no need to configure guest VLANs on the access switch. Traffic from the wired and wireless clients terminates on Guest Controller. Since the guest VLAN is not present on the access switch, the traffic is tunneled to the MTE over the existing mobility tunnel, and then via a guest tunnel to the Guest Controller.

The advantage of this approach is that all guest traffic passes through the MTE before it is tunneled to the Guest Controller. The Guest Controller only needs to support tunnels between itself and all the MTEs.

The disadvantage is that the traffic from the guest client is tunneled twice - once to the MTE and then again to the Guest Controller.



CHAPTER 24

Mobility Control Protocols

- About Mobility Control Protocols, page 227
- Initial Association and Roaming, page 227
- Initial Association, page 228
- Intra Switch Handoff, page 229
- Intra Switch Peer Group Handoff, page 229
- Inter Switch Peer Group Handoff, page 230
- Inter Sub Domain Handoff, page 232
- Inter Mobility Group Handoff, page 233

About Mobility Control Protocols

The mobility control protocol is used regardless of whether tunneled or routed. The mobility control protocol is used for mobility events between the MO, MC and MA.

The mobility architecture uses both,

- Distributed approach, using the direct communication with the switches in their respective SPG, as well as
- Centralized approach, using the MC and MO.

The goal is to reduce the overhead on the centralized MC, while limiting the interactions between switches to help scale the overall system.

Initial Association and Roaming

The following scenarios are applicable to the mobility management protocol:

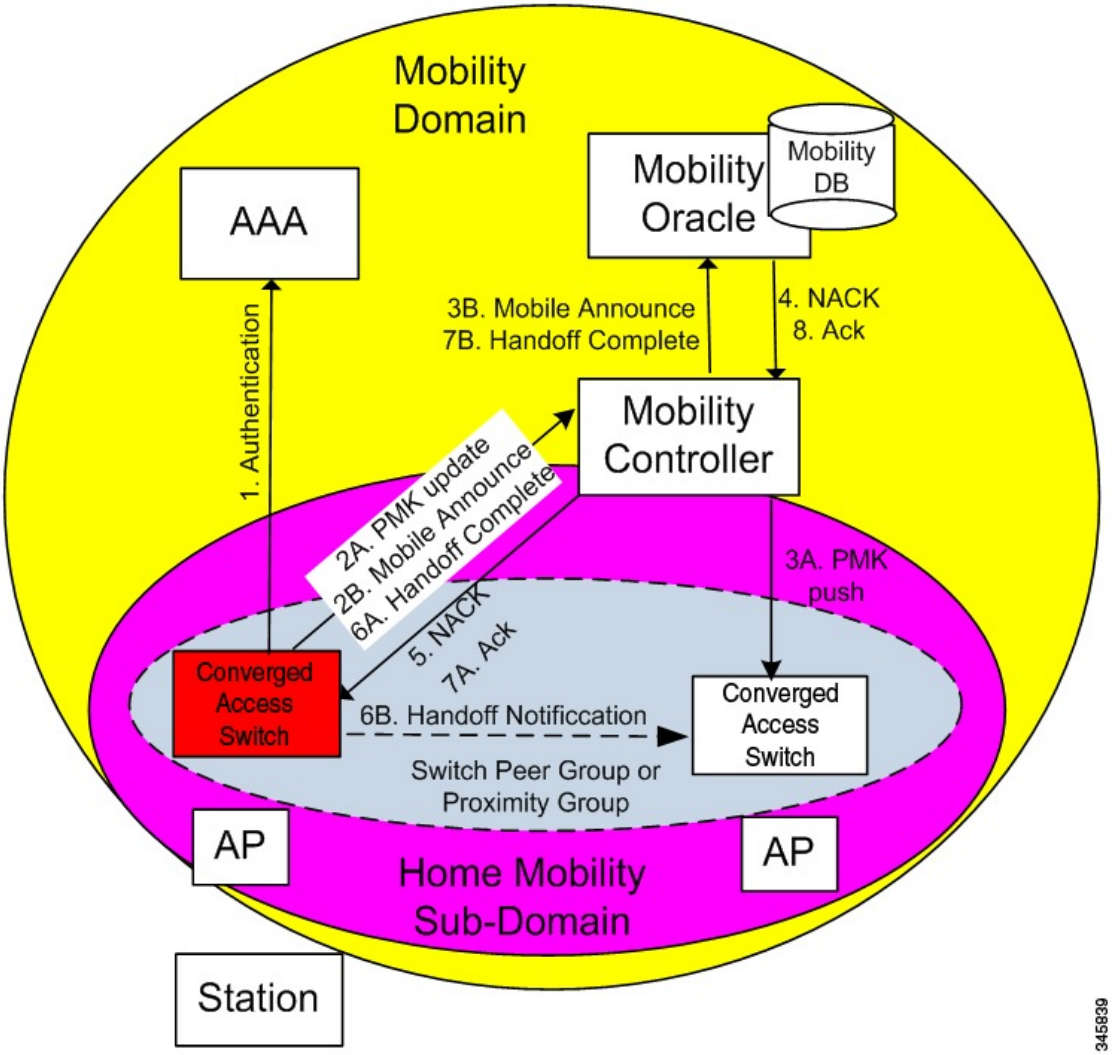
- Initial Association
- Intra Switch Roam
- Intra Switch Peer Group Roam

- Inter Switch Peer Group Roam
- Inter Sub-Domain Roam
- Inter Group Roam

Initial Association

The illustration below explains the initial association process followed by theswitch:

Figure 4: Initial Association



1 When a station initially associates with a mobility agent, the MA performs a lookup to determine whether keying information for key caching is locally available in the MA. If no keying information is available, which is the case when the station first appears in the network, the switch prompts the device to authenticate

itself to generate the Pairwise Master Key (PMK). The PMK is generated on the client and the RADIUS server side, and the RADIUS sever forwards the PMK to the authenticator, the MA.

2 The MA sends the PMK to the MC.

3 After receiving the PMK from the MA, the MC transmits the PMK to all the MAs in its sub-domain, and to all the other MCs in its mobility group.

4 The mobility group is a single key domain. This ensures that 802.11r compliant stations recognize the key domain, and attempts to utilize the fast transition procedures defined in 802.11r.

Note The 802.11r protocol defines a key domain, which is a collection of access points that share keying information.

5 (Refer to step 2B in the illustration). Since the station is new to the mobility sub-domain, as indicated by the fact that the PMK is not in the MA local key cache, the MA transmits a mobile announce message to the MC.

6 The MC checks if the client exists in its database. As the client cannot be found, the MC in turn forwards it to the MO, if available.

7 (Refer to step 5 in the illustration). As the station is new to the network, the MO returns a negative response (NACK), which is forwarded by the MC to the switch. If the Mobility Oracle is not available then the MC is responsible for not responding to the Mobile Announce.

8 The MA on the switch informs the MC about the station's new point of attachment via the Handoff Complete message.

9 The MA then informs the other MAs in its switch peer group (SPG) about the station's new point of attachment via the Handoff Notification message. It is necessary to transmit this notification to the MAs in its SPG to allow local handoff without interacting with the MC. The Handoff Notification message sent to MAs in SPG need not carry all the information in Handoff Complete message sent to the MC.

10 (Refer to step 7B in the illustration). The MC updates its database and forwards the Handoff Complete message to the Mobility Oracle. This ensures that the Mobility Oracle's database is updated to record the station's current home mobility sub-domain.

To eliminate race conditions that could occur with devices moving quickly across switch, regardless of whether they are within a mobility sub-domain or not, the messages between MA and MC/MO are time synchronized. This would allow the MC and MO to properly process requests, if they are received out of order.

The Handoff Notification sent to MAs in the SPG are not acknowledged.

Intra Switch Handoff

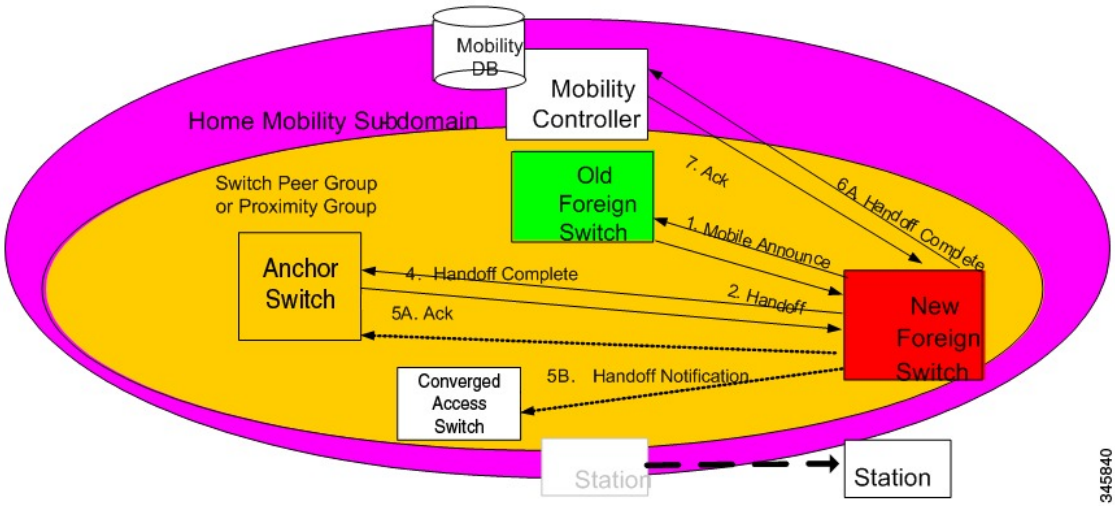
Mobility events within an MA are completely transparent to the SPG and the MC. When a station moves across APs on the same MA and attempts to perform a fast handoff, the PMK is present on the MA. The MA will complete the fast handoff without invoking any additional signal.

Intra Switch Peer Group Handoff

The switch peer group (SPG) is a group of MAs between which users may roam, and expect fast roaming services. Allowing the MA to handoff directly within a SPG reduces the overhead on the MC as it requires fewer messages to be exchanged.

After the initial association is complete the station moves to another MA belonging to its SPG. In an intra switch peer group roam, the initial association, the stations PMK was forwarded to all MAs in the mobility sub-domain.

Figure 5: Intra Switch Peer Group Handoff



The following process explains the intra switch peer group handoff:

1. In the initial association example, the Handoff Notification message is sent to all MAs in its SPG to know the station's current point of attachment.
2. The new MA sends a unicast Mobile Announce message to the previous MA to which the client is associated.
3. After the handoff completion, the new MA transmits a Handoff Complete message to the MC.
4. The new switch sends a Handoff Notification to all MA in its own SPG to inform them about the clients new point of presence.

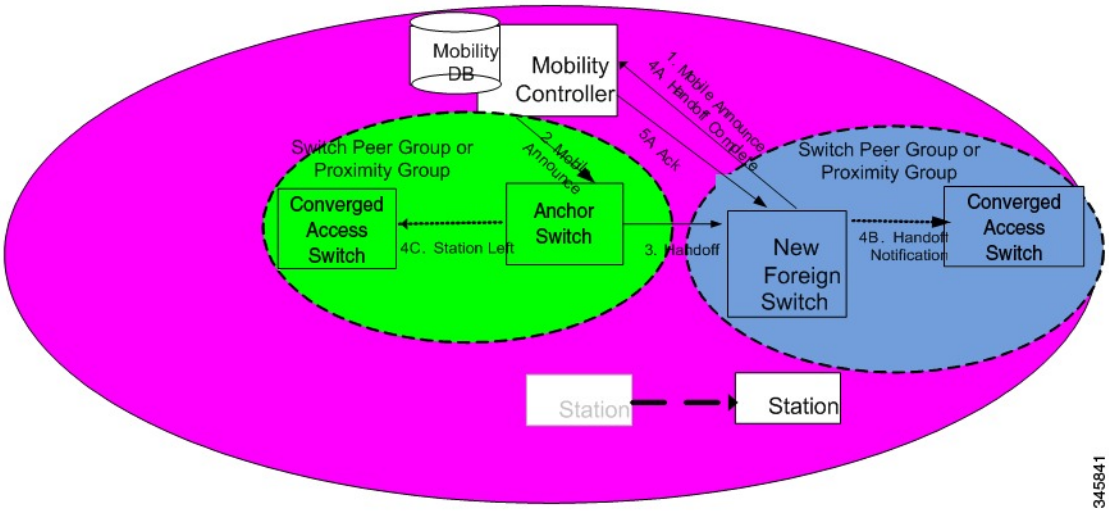
Inter Switch Peer Group Handoff

The Intra SPG roams do not cover all possible scenarios and there can be cases where it is possible for mobility events to occur between two MAs that are not in the same SPG.

When a MA does not have any information about a station's current point of attachment, because of the Handoff Notification message getting lost in the network, or because of the the station roaming to an MA that is not in the new SPG, the MA consults the MC. The MC provides information about the clients point of

presence within the mobility sub-domain. This eliminates the need to consult all other MCs within the mobility sub-domain.

Figure 6: Inter Switch Peer Group Handoff



The image above illustrates an example of a mobility event that occurs across MAs that are not in the same SPG, but within the same mobility sub-domain.

Note The MA color matches the circle representing its SPG.

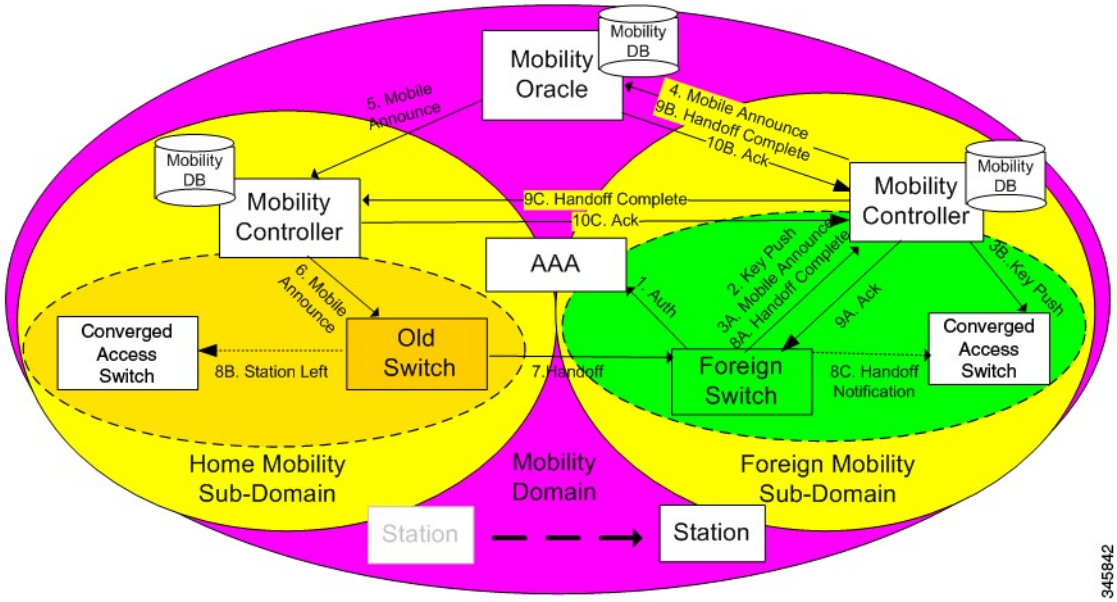
1. The new MA will have the PMK for the station, which was forwarded to each MA in the mobility sub-domain upon client initial authentication.
2. Since the MA had not been previously notified of the station's presence on a neighboring MA inside a different SPG transmits the mobile announce to the sub-domain's MC.
3. (Refer to step 2 in the illustration) On receiving the mobile announce message, the MC performs a lookup in its database, and forwards the request to the MA that was previously providing service to the station. This information is known to the MC through a previously received Handoff Complete message sent in a reliable fashion from the old MA.
4. (Refer to step 3 in the illustration) The old MA, shown in green above, transmits a Handoff message directly to the new MA.
5. The old MA needs to notify other MAs within its SPG of the fact that the station has left the group using a Station Left message. This ensures that if the station were to come back to one of the MA , they would be aware of the fact that the station is no longer being serviced by the old MA.
6. Once the handoff is complete, the new MA transmits the Handoff Complete message in a reliable fashion to the MC.
7. The new MA then transmits the Handoff Notification to the other MAs within its SPG.

Inter Sub Domain Handoff

A sub-domain is an ensemble formed by a mobility controller and the mobility agents it directly manages. An inter sub-domain mobility event implies communication between two mobility controllers. These 2 mobility controllers can be configured with the same mobility group value and recognize each other. They will appear in each other's mobility list, or they can be configured with different mobility group values, and still recognize each other.

When the roaming event occurs across sub-domains between MCs in the same mobility group, the 802.11r key domain advertised by the new APs are the same. Additionally, the client PMK is also transmitted to all MCs upon the client's initial authentication. The new MC does not need to force the client to reauthenticate, and the new MC also knows which previous MC was managing the wireless client mobility.

Figure 7: Inter Sub Domain Handoff



The following steps are involved in the inter sub domain handoff, when mobility controllers belong to the same mobility group:

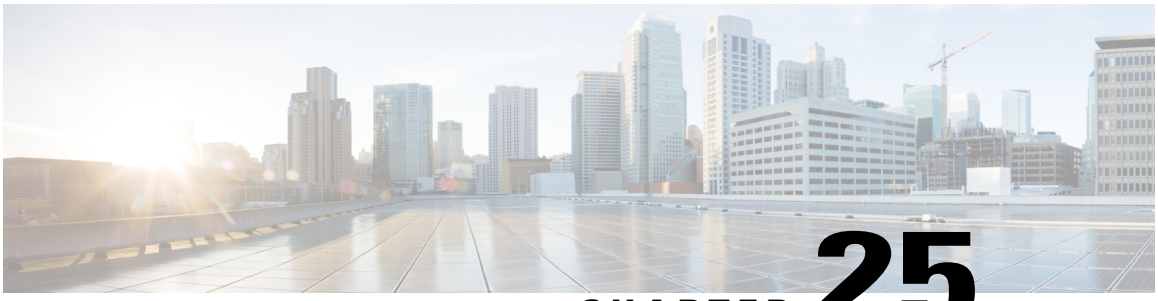
1. When a clients PMK was sent by the initial MA to all the MCs in the mobility group, the new MA already had already received the client PMK from its MC, and re-authentication is not required.
2. The new MA was not notified previously of the station's presence on a neighboring MA inside a different SPG it transmits the mobile announce to the sub-domain's MC.
3. On receiving the mobile announce message, the MC forwards the mobile announce to the MO, which performs a lookup in its database, and forwards the request to the MC that was previously providing service to the station.
4. The previous MC, in turn, forwards the request to the MA that was previously providing service to the station.
5. The old MA, shown in yellow color above, transmits a Handoff message directly to the new MA.

6. The old MA must notify the other MAs within its SPG of the fact that the station has left the SPG using a Station Left message. This ensures that if the station comes back to one of the MA , the MA is aware of the fact that the station is no longer serviced by the old MA.
7. Once the handoff is complete, the new MA transmits the Handoff Complete message in a reliable fashion to the new Mobility Controller.
8. The new MA then transmits the Handoff Notification to all other MAs.
9. The new MC then transmits the Handoff Complete to the old MC.

Inter Mobility Group Handoff

A mobility group is formed by MCs sharing the same mobility group name, and knowing each other.

Since the roaming event occurs across mobility groups, the 802.11r key domain advertised by the new APs differ. This forces the client to re-authenticate. They are propagated only within a mobility group, and roaming across mobility groups requires the stations to re-authenticate when they cross mobility group boundaries. When the authentication is complete, the PMK that is generated is pushed to the MAs and MCs within the same mobility group. The stations cache the PMK from the previous sub-domain because each PMK is associated to a given sub-domain (802.11y key domain). This ensures that you do not have to re-authenticate when the PMK roams back to the previous sub-domain within the pmk cache timeout interval. The remaining procedure follows the inter-sub-domain handoff steps, except that these steps relate to inter mobility group roaming.



CHAPTER 25

Intra Sub Domain Mobility

- Overview, page 235
- Layer 2 Roaming, page 235
- Layer 3 Roaming, page 236

Overview

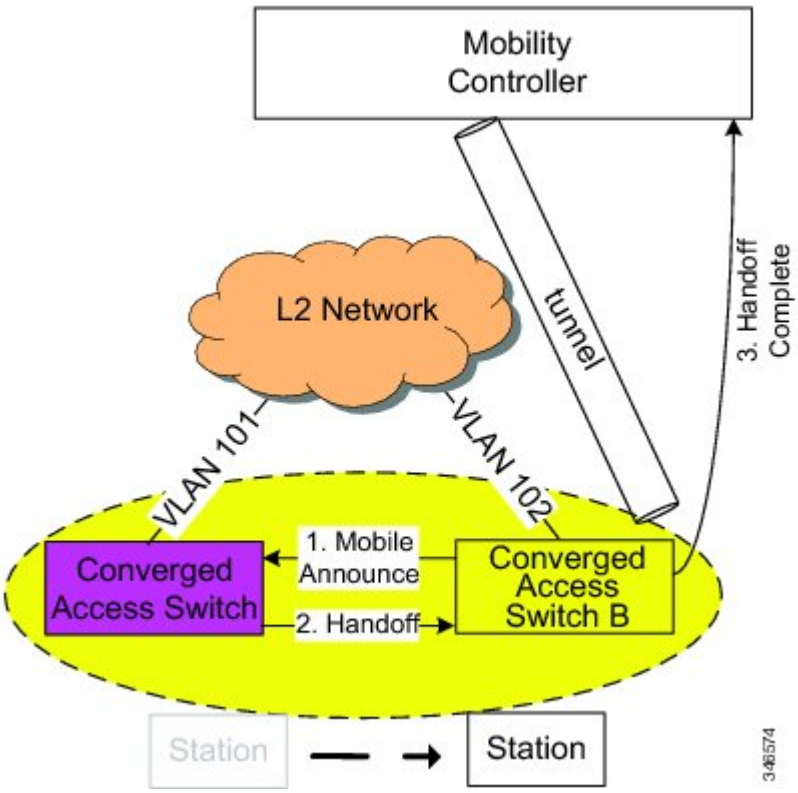
This section explains the mobility events that occur within a mobility sub-domain.

Layer 2 Roaming

This section explains the bridging concept where a station roams across the switch.

When a station roams across switches and if its SSID and VLAN mapping matches, it is called a layer 2 roam.

Figure 8: Layer 2 Roaming



In the illustration, when a station roams across switches the target switch has access to the station's VLAN or subnet. When the handoff is complete, the MC is informed through the Handoff Complete message. The new switchbecomes the new point of presence for the station, and is responsible for advertising serviceability for the station directly.

Layer 3 Roaming

Layer 3 roaming happens when a station roams to an switch where the same VLAN or subnet is not available.

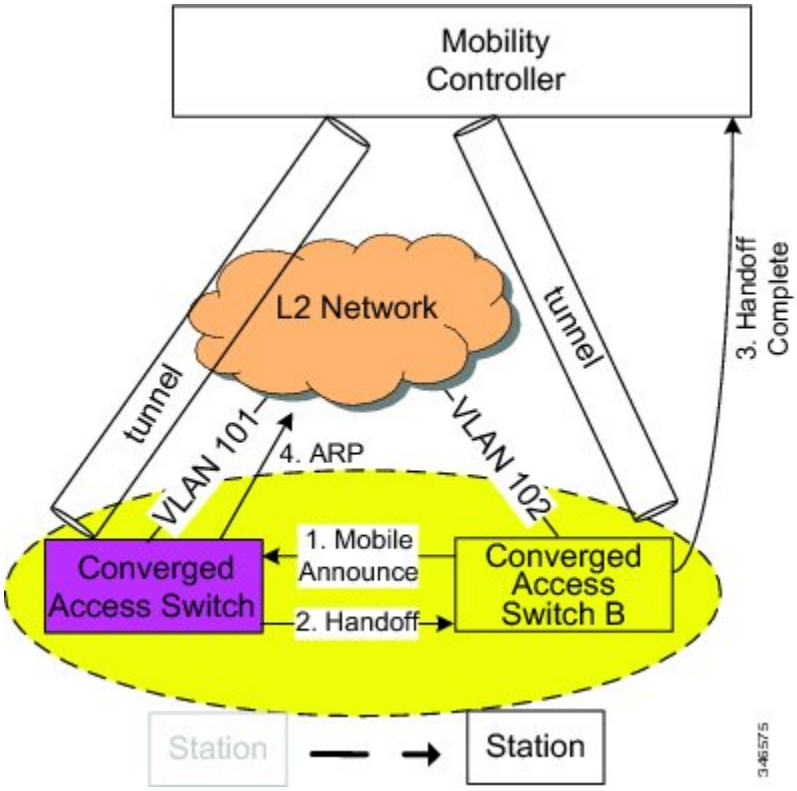
Point of Presence at Access Switch

The original switch becomes the anchor switch of the station. The new switch to which the station roams becomes the foreign switch of the station. In this scenario, the tunneling is direct between the foreign switch and the anchor switch.

In case of intra SPG, the tunneling is direct.

In case of inter SPG, the tunneling is directed through the MC.

Figure 9: Layer 3 Roaming



The illustration above explains the data path for for native stations and roamed stations.

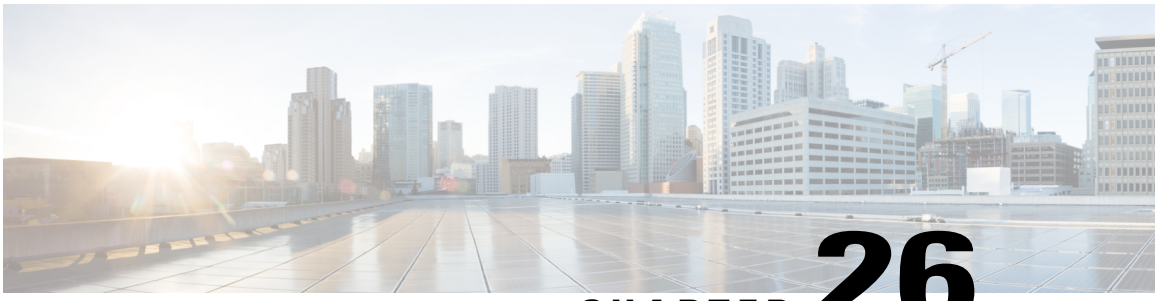
- For native stations, the point of presence and the point of attachment is the same, Switch A.
- For an L3 roamed clients, the point of presence remains at the last switch with which the station was associated and where the station's subnet was available, while point of attachment moves to the client to which it has has roamed.

The following events explains the Layer 3 roam with Anchor Switch as the point of presence:

1. A station joins the network by associating to the AP on Switch A and is provided with an IP address from a subnet available on it.
   Its traffic is natively bridged at the switch and no tunneling is required. Switch A is both the point of presence and point of attachment for the station.
2. When the station roams to Switch B where the same subnet is not available, the information is provided in the handoff process.
3. In inter SPG roaming within the same sub-domain, when the handoff is complete, the MC is informed via the Handoff Complete message, and includes an indicator that traffic arriving on a tunnel from Switch B needs to be transmitted on a tunnel to Switch A.
4. In intra SPG within the same sub-domain, when the handoff is complete, the tunneling does not have to go through MC. The tunneling is direct between Switch B and Switch A.

5 The anchor switch, Switch A, continues to be the station's point of presence and Switch B becomes the point of attachment.

When the roamed station sends traffic to a wired host, the traffic is tunneled to the MTE, and from there to the Switch A. In the same way, since the point of presence is at Switch A, the traffic from the wired host comes to Switch A, and is tunneled first to the MTE, and from there to the foreign Switch B.



CHAPTER 26

Inter Sub Domain Mobility

- Introduction, page 239
- Point of Presence at Anchor Switch, page 240

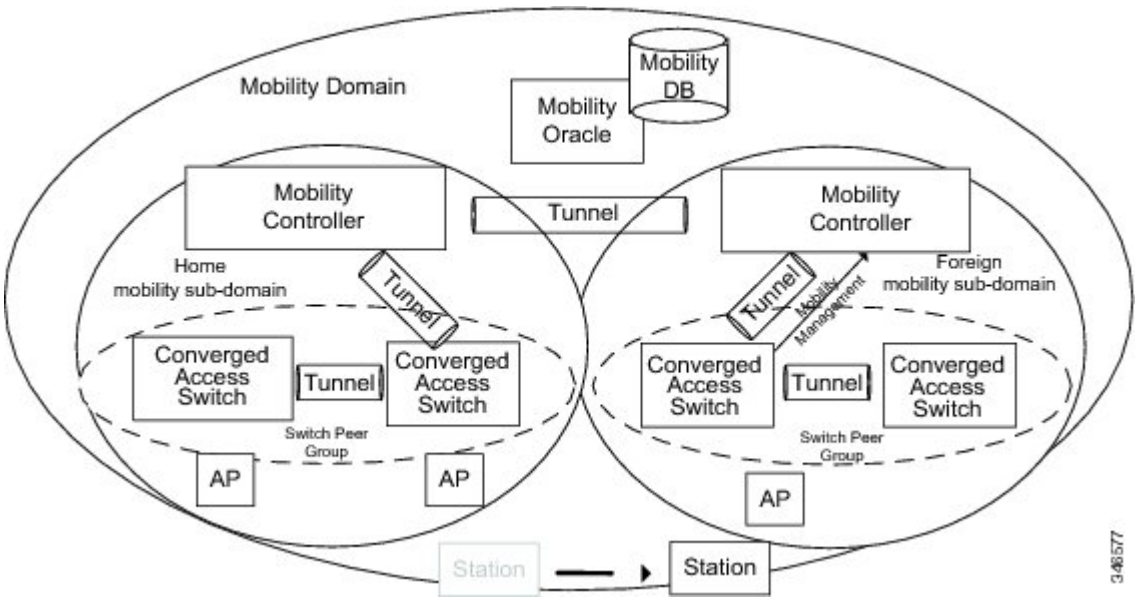
Introduction

This section focuses specifically on mobility events that occur across mobility sub-domains. An inter sub-domain mobility event occurs when a user moves from his home sub-domain to a foreign sub-domain. When the station initially roams to the foreign sub-domain, the foreign Mobility Controller signals the mobility event through the Mobility Oracle. This causes the station's traffic to be tunneled between the MCs in both sub-domains.

Point of Presence at Anchor Switch

When a station moves across sub-domains, the home and foreign MCs ensure that all of the station's traffic is tunneled.

Figure 10:



Tunneling across sub-domains when the client roams from Anchor Switch to Foreign Switch

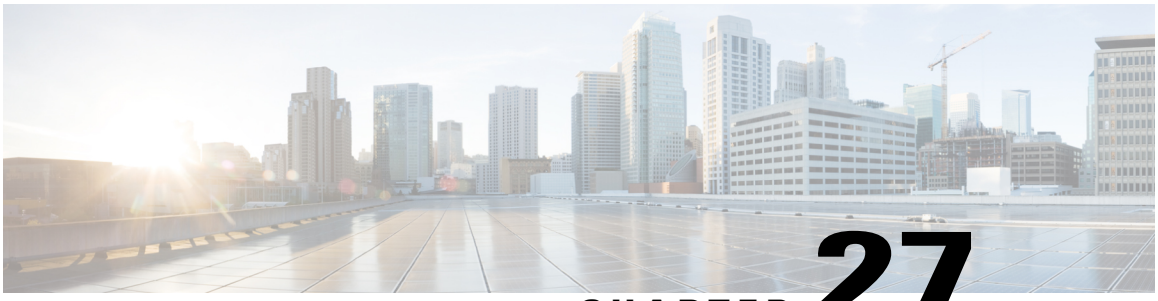
The following events happen when a station roams across sub-domains with the anchor switch in the home sub-domain as its point of presence:

- A station joins the network by associating to the AP on switch A and is provided with an IP address from a subnet available on it.
  Its traffic is natively bridged at the switch and no tunneling is required. switch A is both the point of presence and point of attachment for the station.
- When the station roams to switch B where the same subnet is not available, the information is provided in the handoff process.
- When the handoff is complete, the mobile announce message is sent from switch B to the MC in foreign sub-domain.
- The MC belonging to the foreign sub-domain will then tunnel the mobile announce message to the MO. This cause the stations traffic to be tunneled between the MCs in both the sub-domains.
- The MO will tunnel the mobile announce message to the MC in the home sub-domain.
- The MC in the home sub-domain will then tunnel the traffic to the anchor switch.

Tunneling across sub-domains with the Anchor Switch in the home sub-domain is the point of presence

The following events happen when a station roams across sub-domains with the anchor switch in the home sub-domain as its point of presence:

- A station joins the network by associating to the AP on switch A and is provided with an IP address from a subnet available on it.
  Its traffic is natively bridged at the switch and no tunneling is required. switch A is both the point of presence and point of attachment for the station.
- When the station roams to switch B where the same subnet is not available, the information is provided in the handoff process.
- When the handoff is complete, the anchor switch (Switch A) sends the handoff complete message to Switch B.
- The MC in the foreign sub-domain then forwards the handoff complete message to the MC in the home sub-domain.
- The MC belonging to the foreign sub-domain will then tunnel the traffic to the MO and finally reached the MC in the home sub-domain.
- The MC in the home sub-domain will then tunnel the traffic to the anchor switch.
- The anchor switch continues to be the point of presence for the station.
- The Switch B will contain the point of attachment.



CHAPTER 27

Mobility Controller and Mobility Tunnel Endpoint Redundancy

- About MC and MTE Redundancy , page 243

About MC and MTE Redundancy

The mobility controller maintains the station database, which includes information such as the current point of attachment, station's credentials, IP address, and the mobility protocol state associated with the station. These states are dynamically updated based on the authentication, address assignment, or mobility signaling events. Redundancy is required to handle the case when the MC fails or is taken down for service, thus eliminating the single point of failure phenomena. This level of reliability provides a switch-over mechanism (that is, backup MC taking over operation) that does not require the mobile station, Switch, or Mobility Oracle to be aware or take any additional action.

MC redundancy uses an active/passive approach and provides a scalable high availability with instantaneous fail over support. When the active MC fails, the backup MC takes over immediately to maintain the states for the stations. The MC sets up the tunneling operation on the MTE, which is responsible for the encapsulation and decapsulation of packets to/from the Switch or another MTE for the stations in the sub-domain.

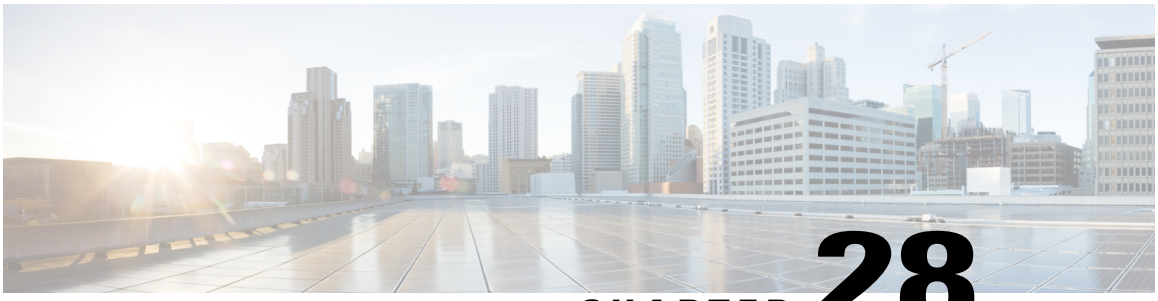
During normal operation, the active MTE does the encapsulation/decapsulation. Since all of the station states are completely replicated on the backup MC, the forwarding path on the backup MTE is already set up to handle packets for the station. This means there is minimal packet loss, which happens during the period between active MC going down and the backup MC detecting the condition and taking over. The number of stations on the MC does not affect the performance of switchover, which is based on the detection latency only. Normally, the active MTE advertises the station if the point of presence is at the MTE. When the backup MTE takes over, it will need to start advertising the station.

There are two components of MC redundancy:

- Unresponsiveness Detection – This is a mechanism to detect when a active MC is down
- State Synchronization – This mechanism is used transfer the stations' states between the MCs

State synchronization is accomplished by the transfer of the station states from the active MC to the backup MC. There are two types of operations: station update and bulk synchronization. When a station state is created, changed, or deleted, the station's states, or only the status code/delta, are transferred. This update messaging happens when both MCs are in operation. In the case when a backup MC initially comes up, bulk

synchronization happens. The backup MC sends a request to the active MC, and downloads the entire database from the active MC. The states of all the stations are reliably transferred using SCTP or application-based reliability mechanism.



CHAPTER 28

Configuring Mobility

- Configuring Mobility Controller, page 245
- Configuring Mobility Agent, page 251

Configuring Mobility Controller

Configuring Converged Access Controllers

Creating Peer Groups, Peer Group Member, and Bridge Domain ID (CLI)

Before You Begin

- On the mobility agent, you can only configure the IP address of the mobility controller.
- On the mobility controller, you can define the peer group and the IP address of each peer group member.

SUMMARY STEPS

1. **wireless mobility controller**
2. **wireless mobility controller peer-group** *SPG1*
3. **wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
4. **wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
5. **wireless mobility controller peer-group** *SPG2*
6. **wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr*
7. **wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility controller** **Example:** `Switch(config)# wireless mobility controller`	Enables the mobility controller functionality on the device. This command is applicable only to the switch. The controller is by default a mobility controller.
Step 2	**wireless mobility controller peer-group** *SPG1* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1`	Creates a peer group named SPG1.
Step 3	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip 10.10.20.2`	Adds a mobility agent to the peer group. **Note** The 10.10.20.2 is the mobility agent's direct IP address. When NAT is used, use the optional public IP address to enter the mobility agent's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility agent's direct IP address.
Step 4	**wireless mobility controller peer-group** *SPG1* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.10.20.6`	Adds another member to the peer group SPG1.
Step 5	**wireless mobility controller peer-group** *SPG2* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2`	Creates another peer group SPG2.
Step 6	**wireless mobility controller peer-group** *SPG2* **member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip 10.10.10.20`	Adds a member to peer group SPG2.
Step 7	**wireless mobility controller peer-group** *SPG1* **bridge-domain-id** *id* **Example:** `Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54`	(Optional) Adds a bridge domain to SPG1 used for defining the subnet-VLAN mapping with other SPGs.

This example shows how to create peer group and add members to it:

```
Switch(config)# wireless mobility controller
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.2 public-ip
 10.10.20.2
Switch(config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.10.20.6
Switch(config)# wireless mobility controller peer-group SPG2
Switch(config)# wireless mobility controller peer-group SPG2 member ip 10.10.10.20 public-ip
 10.10.10.20
Switch(config)# wireless mobility controller peer-group SPG1 bridge-domain-id 54
```

Configuring Local Mobility Group (CLI)

Configuration for wireless mobility groups and mobility group members where the mobility group is a group of MCs.

Before You Begin

MCs can belong only to one mobility group, and can know MCs in several mobility groups.

SUMMARY STEPS

1. **wireless mobility group name** *group-name*
2. **wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr*
3. **wireless mobility group keepalive interval** *time-in-seconds*
4. **wireless mobility group keepalive count** *count*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group-name* **Example:** `Switch(config)# wireless mobility group name Mygroup`	Creates a mobility group named Mygroup.
Step 2	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **Example:** `Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28`	Adds a mobility controller to the Mygroup mobility group. **Note** When NAT is used, use the optional public IP address to enter the NATed IP address of the mobility controller.
Step 3	**wireless mobility group keepalive interval** *time-in-seconds* **Example:** `Switch(config)# wireless mobility group keepalive interval 5`	Configures the interval between two keepalives sent to a mobility member.

	Command or Action	Purpose
Step 4	**wireless mobility group keepalive count** *count* **Example:** `Switch(config)# wireless mobility group keepalive count 3`	Configures the keep alive retries before a member status is termed DOWN.

```
Switch(config)# wireless mobility group name Mygroup
Switch(config)# wireless mobility group member ip 10.10.34.10 public-ip 10.10.34.28
Switch(config)# wireless mobility group keepalive interval 5
Switch(config)# wireless mobility group keepalive count 3
```

Adding a Peer Mobility Group (CLI)

Before You Begin

MCs belong to only one group, and can know MCs in several groups.

SUMMARY STEPS

1. **wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **public-ip** *public-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.24 public-ip 10.10.10.25 group Group2`	Adds the member as a peer MC in a different group than the Mygroup.

Configuring Optional Parameters for Roaming Behavior

Use this configuration to disable the sticky anchor. This command can also be used, if required, between all MA's and MC's where roaming is expected for the target SSID.

SUMMARY STEPS

1. **wlan** open21
2. **no mobility anchor sticky**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** open21 **Example:** `Switch(config)# wlan open20`	Configures a WLAN.
Step 2	**no mobility anchor sticky** **Example:** `Switch(config-wlan)# no mobility anchor sticky`	Disables the default sticky mobility anchor.

```
Switch(config)# wlan open20
Switch(config-wlan)# no mobility anchor sticky
```

Pointing the Mobility Controller to a Mobility Oracle (CLI)

Before You Begin

You can configure a mobility oracle on a known mobility controller.

SUMMARY STEPS

1. **wireless mobility group member ip** *member-ip-addr* **group** *group-name*
2. **wireless mobility oracle ip** *oracle-ip-addr*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility group member ip** *member-ip-addr* **group** *group-name* **Example:** `Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3`	Creates and adds a MC to a mobility group.
Step 2	**wireless mobility oracle ip** *oracle-ip-addr* **Example:** `Switch(config)# wireless mobility oracle ip 10.10.10.10`	Configures the mobility controller as mobility oracle.

```
Switch(config)# wireless mobility group member ip 10.10.10.10 group Group3
Switch(config)# wireless mobility oracle ip 10.10.10.10
```

Configuring Guest Controller

A guest controller is used when the client traffic is tunneled to a guest anchor controller in the demilitarized zone (DMZ). The guest client goes through a web authentication process. The web authentication process is optional, and the guest is allowed to pass traffic without authentication too.

Enable the WLAN on the mobility agent on which the guest client connects with the mobility anchor address of the guest controller.

On the guest controller WLAN, which can be Cisco 5500 Series WLC, Cisco WiSM2, or Cisco 5700 Series WLC, configure the IP address of the mobility anchor as its own IP address. This allows the traffic to be tunneled to the guest controller from the mobility agent.

SUMMARY STEPS

1. **wlan** *wlan-id*
2. **mobility anchor** *guest-anchor-ip-addr*
3. **client vlan** *vlan-name*
4. **security open**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** *wlan-id* **Example:** `Switch(config)# wlan Mywlan1`	Creates a WLAN for the client.
Step 2	**mobility anchor** *guest-anchor-ip-addr* **Example:** `Switch(config-wlan)# mobility anchor 10.10.10.2`	Enables the guest anchors (GA) IP address on the MA. **Note** To enable guest anchor on the mobility controller, you need not enter the IP address. Enter the **mobility anchor** command in the WLAN configuration mode to enable GA on the mobility controller.
Step 3	**client vlan** *vlan-name* **Example:** `Switch(config-wlan)# client vlan gc_ga_vlan1`	Assigns a VLAN to the client's WLAN.
Step 4	**security open** **Example:** `Switch(config-wlan)# security open`	Assigns a security type to the WLAN.

```
Switch(config)# wlan Mywlan1
Switch(config-wlan)# mobility anchor 10.10.10.2
Switch(config-wlan)# client vlan gc_ga_vlan1
Switch(config-wlan)# security open
```

Configuring Guest Anchor

SUMMARY STEPS

1. **wlan** Mywlan1
2. **mobility anchor** <guest-anchors-own-ip-address>
3. **client vlan**<vlan-name>
4. **security open**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wlan** Mywlan1 **Example:** `Switch(config)# wlan Mywlan1`	Creates a wlan for the client.
Step 2	**mobility anchor** <guest-anchors-own-ip-address> **Example:** `Switch(config-wlan)# mobility anchor 10.10.10.2`	Enables the guest anchors IP address on the guest anchor (GA). The GA assigns its own address on itself.
Step 3	**client vlan**<vlan-name> **Example:** `Switch(config-wlan)# client vlan gc_ga_vlan1`	Assigns a vlan to the clients wlan.
Step 4	**security open** **Example:** `Switch(config-wlan)# security open`	Assigns a security type to the wlan.

```
Switch(config)# wlan Mywlan1
Switch(config-wlan)# mobility anchor 10.10.10.2
Switch(config-wlan)# client vlan gc_ga_vlan1
Switch(config-wlan)# security open
```

Configuring Mobility Agent

Configuring Mobility Agent by Pointing to Mobility Controller (CLI)

Before You Begin

- By default, the switches are configured as mobility agents.
- Your network must have at least one mobility controller and the network connectivity with the mobility controller must be operational.

- You cannot configure mobility from the mobility agent. On the mobility agent, you can configure only the IP address of the mobility controller to download the SPG configuration.
- On the mobility agent, you can either configure the mobility controller address to point to an external mobility agent, or enable the mobility controller function.

SUMMARY STEPS

1. **configure terminal**
2. **wireless management interface** vlan 21

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless management interface** vlan 21 **Example:** `Switch (config)# wireless management interface vlan 21`	Enables the wireless functionality on the device and activates the mobility agent function. This ensures the APs have a place to terminate the CAPWAP tunnel.

This example shows how to add a mobility agent into the mobility group by pointing it to a mobility controller:

```
Switch(config)# wireless management interface vlan 21
```

Configuring the Mobility Controller for the Mobility Agent (CLI)

SUMMARY STEPS

1. **wireless mobility controller**
2. **wireless mobility controller ip** *ip-addr*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility controller** **Example:** `Switch (config)# wireless mobility controller`	Enables the mobility function on the switch. **Note** After you enter this command, save the configuration and reboot the switch for the mobility controller function to take effect.

	Command or Action	Purpose
	`Mobility role changed to Mobility Controller. Please save config and reboot the whole stack.`	
Step 2	**wireless mobility controller ip** *ip-addr* **Example:** `Switch (config)# wireless mobility controller ip 10.10.21.3`	Specifies the mobility controller to which the mobility agent relates. **Note** If a mobility agent is configured and the mobility controller exists on a different device, configure the SPG on the mobility controller to ensure the mobility agent functions properly.

What to Do Next

After you add a mobility controller role to the mobility agent, you can configure optional parameters on the mobility agent.

Configuring Optional Parameters on a Mobility Agent (CLI)

This section shows how to configure load-balancing on a switch.

- By default, the load-balancing is enabled and it cannot be disabled.
- The switch supports a maximum of 2000 clients and the default threshold value is fifty percent of client max load.
- When the switch reaches its threshold, it redistributes the new clients load to other mobility agents in the same SPG, if their client load is lower.

SUMMARY STEPS

1. **wireless mobility load-balance threshold** *threshold-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**wireless mobility load-balance threshold** *threshold-value* **Example:** `Switch(config)# wireless mobility load-balance threshold 150`	Configures the threshold that triggers load-balancing.

INDEX

802.1X authentication for access points 130
  described 130

A

Access Point Authentication 130
Access Point Communication Protocols 108
access point core dumps, uploading 141
  using the GUI 141
Access Point Retransmission Interval 120
Access Point Retry Count 120
access points 108, 109, 148
  priming 108
  supporting oversized images 148
  viewing join information 109
    using the GUI 109
acronyms 193
All APs page 100
AnchorTime parameter 91
AP Mode parameter 100
Autonomous Access Points Converted to Lightweight Mode 140

B

Backup Controllers 154

C

CCX 29, 176
  described 29
  link test 176
Channel Assignment Leader parameter 91
Channel Assignment Method parameter 90
Channel Scan Duration parameter 81
Cisco Workgroup Bridges 149
CleanAir 191
  components 191
Configuration Examples 209
Configure RF Group Mode 82
  Using GUI 82
Configuring a static IP address 141
Configuring Failover Priority for Access Points 155
Configuring Interference Reporting 198, 202
  2.4-GHz devices 198
  5-GHz devices 202
Control and Provisioning of Wireless Access Points protocol (CAPWAP) 108
  described 108
controllers 108
  discovery process 108
country codes 169
  described 169
Country Codes 170
Coverage Exception Level per AP parameter 94
coverage hole detection 93, 94
  configuring per controller 93, 94
    using the GUI 93, 94
coverage hole detection and correction 78

D

DCA Channel Sensitivity parameter 91
DCA Channels parameter 91
default enable password 130
default-group access point group 62
dhcp option 43 140
dhcp option 60 140
DHCP option 82 46, 47
  described 46
  example 47
DHCP servers 44
  internal 44
diagnostic channel 30
  described 30
domain name server (DNS) discovery 108
DTIM 28
DTLS data encryption. See data encryption 116
dynamic channel assignment (DCA) 77
  described 77

E

EDRRM 195
Enable Coverage Hole Detection parameter 94
Enabling CleanAir 196, 200
  2.4-GHz 196
  5-GHz 200

F

failover priority for access points 154
  described 154
FAQ 210
fast heartbeat timer 153
  described 153

G

General (controller) page 84
  configuring an RF group 84
Group Mode parameter 102

I

inline power 183
interference 78
Interference threshold parameter 80
Interval parameter 91
Invoke Channel Update Now button 90
Invoke Power Update Now button 87

J

Japanese country codes 170

L

lightweight mode, reverting to autonomous mode 140
Link Latency 176
link test 176
  types of packets 176
LWAPP-enabled access points 141, 143
  reverting to autonomous mode 143
  sending crash information to controller 141

M

MAC address of access point 141
  displayed on controller GUI 141
Min Failed Client Count per AP parameter 94
mobility groups 73
  difference from RF groups 73
monitor intervals, configuring using the GUI 81
Monitoring CleanAir 206, 209
  Using CLI 206
  Using GUI 209
Monitoring Interference Devices 209

N

Neighbor Packet Frequency parameter 81
Non-Cisco Workgroup Bridges 149

P

peer-to-peer blocking 29
  described 29
ping link test 176
Power Neighbor Count parameter 87
Power over Ethernet 183
Power Threshold parameter 87
probe request forwarding 163
probe requests, described 163
Protection Type parameter 100

R

radio resource management (RRM) 75, 78, 81, 87, 90, 91, 93
  configuring 81
    monitor intervals using the GUI 81
  coverage hole detection 78, 93
    configuring per controller using the GUI 93
    described 78
  specifying channels 90, 91
  update interval 75
  Wireless > 802.11a/n (or 802.11b/g/n) > RRM > TPC
  parameter 87
RF group leader 73, 74
  described 73, 74
RF group name 75
  described 75
RF groups 74, 75, 102
  cascading 74
  monitoring status 102
    using the GUI 102

RF groups *(continued)*
overview 75
pinning 74
viewing status 102
using the GUI 102
RF-Network Name parameter 84
RFID Tracking 155, 165
rogue access points 100
alarm 100

S

Set to Factory Default button 81
Spectrum Expert 205
configuring using CLI 205
SSID 27
described 27
Static IP address 141
described 141

T

tcp mss 176
troubleshooting join process 109

U

unique device identifier (UDI) 155
described 155

V

VCI strings 140
Voice RSSI parameter 94

W

WLAN broadcast ssid, Configure 35
WLAN call snoop, Configure 35
WLAN interface VLAN, Configure 35
WLAN media stream multicast, Configure 35
WLAN radio, Configure 35
WLAN, enable, disable 35
WLANs 29
session timeout 29
described 29