Cisco Wireless Controller Configuration Guide, Release 7.5

First Published: 2013-07-30

Last Modified: 2013-07-30

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

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

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

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

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

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

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

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

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

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

© 2002-2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xlix

Audience xlix

Conventions xlix

Related Documentation l

PART I

System Management 53

CHAPTER 1

Cisco Wireless Solution Overview 1

Core Components 2

Overview of Cisco Mobility Express 3

Single-Controller Deployments 3

Multiple-Controller Deployments 4

Operating System Software 5

Operating System Security 5

Layer 2 and Layer 3 Operation 6

Operational Requirements 6

Configuration Requirements 6

Cisco Wireless Controllers 7

Client Location 7

Cisco WLC Platforms 7

Client Location 8

Cisco WLC Platforms 8

Cisco Wireless Solution WLANs 8

File Transfers 9

Power over Ethernet 9

Cisco Wireless Controller Memory 9

Cisco Wireless Controller Failover Protection 9

CHAPTER 2 **Getting Started** 11

Configuring the Controller Using the Configuration Wizard 11

Connecting the Console Port of the Controller 11

Configuring the Controller (GUI) 12

Configuring the Controller—Using the CLI Configuration Wizard 23

Using the Controller GUI 25

Restrictions on using Controller GUI 26

Logging On to the GUI 26

Logging out of the GUI 27

Enabling Web and Secure Web Modes 27

Enabling Web and Secure Web Modes (GUI) 27

Enabling Web and Secure Web Modes (CLI) 28

Loading an Externally Generated SSL Certificate 29

Loading an Externally Generated SSL Certificate 29

Loading an SSL Certificate (GUI) 30

Loading an SSL Certificate (CLI) 30

Using the Controller CLI 31

Logging on to the Controller CLI 32

Using a Serial or USB Console Connection on Cisco WLC 32

Using a Local Serial Connection 32

Using a Remote Telnet or SSH Connection 33

Logging Out of the CLI 34

Navigating the CLI 34

Using the AutoInstall Feature for Controllers Without a Configuration 35

Information About the AutoInstall Feature 36

Restrictions on AutoInstall 36

Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server 36

Selecting a Configuration File 37

Example: AutoInstall Operation 38

Managing the Controller System Date and Time 39

Information About Controller System Date and Time 39

Restrictions on Configuring the Controller Date and Time 39
Configuring the NTP/SNTP Server to Obtain the Date and Time (CLI) 40
Configuring NTP/SNTP Authentication (GUI) 40
Configuring NTP/SNTP Authentication (CLI) 41
Configuring the Date and Time (GUI) 41
Configuring the Date and Time (CLI) 42
Telnet and Secure Shell Sessions 44
Telnet and Secure Shell Sessions 44
Restrictions on Telnet and SSH 44
Configuring Telnet and SSH Sessions (GUI) 45
Configuring Telnet and SSH Sessions (CLI) 46
Configuring Telnet Privileges for Selected Management Users (GUI) 47
Configuring Telnet Privileges for Selected Management Users (CLI) 48
Troubleshooting Access Points Using Telnet or SSH 48
Troubleshooting Access Points Using Telnet or SSH (GUI) 48
Troubleshooting Access Points Using Telnet or SSH (CLI) 48
Managing the Controller Wirelessly 49
Enabling Wireless Connections (GUI) 49
Enabling Wireless Connections (CLI) 50

CHAPTER 3 **Managing Licenses** 51
Installing and Configuring Licenses 51
Information About Installing and Configuring Licenses 51
Restrictions for Using Licenses 52
Obtaining an Upgrade or Capacity Adder License 52
Information About Obtaining an Upgrade or Capacity Adder License 52
Obtaining and Registering a PAK Certificate 53
Installing a License 54
Installing a License (GUI) 54
Installing a License (CLI) 54
Viewing Licenses 55
Viewing Licenses (GUI) 55
Viewing Licenses (CLI) 56
Configuring the Maximum Number of Access Points Supported 59

Configuring Maximum Number of Access Points to be Supported (GUI) 59
Configuring Maximum Number of Access Points to be Supported (CLI) 59
Troubleshooting Licensing Issues 59
Activating an AP-Count Evaluation License 60
Information About Activating an AP-Count Evaluation License 60
Activating an AP-Count Evaluation License (GUI) 60
Activating an AP-Count Evaluation License (CLI) 61
Configuring Right to Use Licensing 62
Right to Use Licensing 62
Configuring Right to Use Licensing (GUI) 63
Configuring Right to Use Licensing (CLI) 64
Rehosting Licenses 64
Information About Rehosting Licenses 64
Rehosting a License 65
Rehosting a License (GUI) 65
Rehosting a License (CLI) 66
Transferring Licenses to a Replacement Controller after an RMA 67
Information About Transferring Licenses to a Replacement Controller after an RMA 67
Transferring a License to a Replacement Controller after an RMA 68

CHAPTER 4 **Configuring 802.11 Bands** 69
Configuring 802.11 Bands 69
802.11 Bands 69
Configuring the 802.11 Bands (GUI) 69
Configuring the 802.11 Bands (CLI) 70
Configuring Band Selection 72
Band Selection 72
Restrictions for Band Selection 73
Configuring Band Selection 74
Configuring Band Selection (GUI) 74
Configuring Band Selection (CLI) 75

CHAPTER 5 **Configuring 802.11 Parameters** 77
Configuring the 802.11n Parameters 77

802.11n Parameters 77
Configuring the 802.11n Parameters (GUI) 77
Configuring the 802.11n Parameters (CLI) 79
Configuring 802.11h Parameters 80
802.11h Parameters 80
Configuring the 802.11h Parameters (GUI) 80
Configuring the 802.11h Parameters (CLI) 81
Configuring the 802.11ac Parameters 82
802.11ac Parameters 82
Restrictions for 802.11ac Support 83
Configuring the 802.11ac High-Throughput Parameters (GUI) 84
Configuring the 802.11ac High-Throughput Parameters (CLI) 84

CHAPTER 6 **Configuring DHCP Proxy** 85
DHCP Proxy 85
Restrictions on Using DHCP Proxy 85
Configuring DHCP Proxy (GUI) 86
Configuring DHCP Proxy (GUI) 86
Configuring DHCP Proxy (CLI) 86
Configuring DHCP Proxy (CLI) 87
Configuring a DHCP Timeout (GUI) 87
Configuring a DHCP Timeout (CLI) 87

CHAPTER 7 **Configuring SNMP** 89
Configuring SNMP (CLI) 89
SNMP Community Strings 91
Changing the SNMP Community String Default Values (GUI) 91
Changing the SNMP Community String Default Values (CLI) 92
Configuring Real Time Statistics (CLI) 93
SNMP Trap Enhancements 93
Configuring SNMP Trap Receiver (GUI) 94

CHAPTER 8 **Configuring Aggressive Load Balancing** 95
Aggressive Load Balancing 95

Configuring Aggressive Load Balancing (GUI) 96
Configuring Aggressive Load Balancing (CLI) 97

CHAPTER 9 **Configuring Fast SSID Changing** 99
Fast SSID Changing 99
Configuring Fast SSID Changing (GUI) 99
Configuring Fast SSID Changing (CLI) 99

CHAPTER 10 **Configuring 802.3 Bridging** 101
Configuring 802.3 Bridging 101
802.3 Bridging 101
Restrictions on 802.3 Bridging 101
Configuring 802.3 Bridging 101
Configuring 802.3 Bridging (GUI) 101
Configuring 802.3 Bridging (CLI) 102
Enabling 802.3X Flow Control 102

CHAPTER 11 **Configuring Multicast** 103
Configuring Multicast Mode 103
Multicast/Broadcast Mode 103
Restrictions on Configuring Multicast Mode 105
Enabling Multicast Mode (GUI) 107
Enabling Multicast Mode (CLI) 108
Viewing Multicast Groups (GUI) 109
Viewing Multicast Groups (CLI) 109
Viewing an Access Point's Multicast Client Table (CLI) 110
Configuring Multicast Domain Name System 110
Multicast Domain Name System 110
Restrictions for Configuring Multicast DNS 112
Configuring Multicast DNS (GUI) 113
Configuring Multicast DNS (CLI) 115
Bonjour Gateway Based on Access Policy 118
Restrictions on Bonjour Gateway Based on Access Policy 119
Creating Bonjour Access Policy through Prime Infrastructure 119

Configuring mDNS Service Groups (GUI) 119
Configuring mDNS Service Groups (CLI) 120
Multicast Configuration for Cisco vWLC, Flex 7510, 5520, 8510, and 8540 WLCs 120
Switching from Multicast-Unicast Mode to Multicast-Multicast Mode 120
Switching from Multicast-Multicast Mode to Multicast-Unicast Mode 120
Restrictions 121
Troubleshooting 121

CHAPTER 12 **Configuring Client Roaming** 123
Information About Client Roaming 123
Inter-Controller Roaming 123
Intra-Controller Roaming 123
Inter-Subnet Roaming 124
Voice-over-IP Telephone Roaming 124
CCX Layer 2 Client Roaming 124
Restrictions for Client Roaming 125
Configuring CCX Client Roaming Parameters (GUI) 125
Configuring CCX Client Roaming Parameters (CLI) 126
Obtaining CCX Client Roaming Information (CLI) 126
Debugging CCX Client Roaming Issues (CLI) 127

CHAPTER 13 **Configuring IP-MAC Address Binding** 129
IP-MAC Address Binding 129
Configuring IP-MAC Address Binding (CLI) 129

CHAPTER 14 **Configuring Quality of Service** 131
Configuring Quality of Service 131
Quality of Service 131
Configuring Quality of Service Profiles 132
Configuring QoS Profiles (GUI) 132
Configuring QoS Profiles (CLI) 133
Configuring Quality of Service Roles 135
Quality of Service Roles 135
Configuring QoS Roles 135

Configuring QoS Roles (GUI) 135
Configuring QoS Roles (CLI) 136

CHAPTER 15 Configuring Application Visibility and Control 139
Application Visibility and Control 139
Restrictions for Application Visibility and Control 140
Configuring Application Visibility and Control (GUI) 141
Configuring Application Visibility and Control (CLI) 142
Configuring NetFlow 143
NetFlow 143
Configuring NetFlow (GUI) 143
Configuring NetFlow (CLI) 144

CHAPTER 16 Configuring Media and EDCA Parameters 145
Configuring Voice and Video Parameters 145
Voice and Video Parameters 145
Call Admission Control 145
Expedited Bandwidth Requests 146
U-APSD 147
Traffic Stream Metrics 148
Configuring Voice Parameters 148
Configuring Voice Parameters (GUI) 148
Configuring Voice Parameters (CLI) 150
Configuring Video Parameters 151
Configuring Video Parameters (GUI) 151
Configuring Video Parameters (CLI) 152
Viewing Voice and Video Settings 153
Viewing Voice and Video Settings (GUI) 153
Viewing Voice and Video Settings (CLI) 153
Configuring SIP-Based CAC 157
Restrictions for SIP-Based CAC 157
Configuring SIP-Based CAC (GUI) 157
Configuring SIP-Based CAC (CLI) 157
Configuring Media Parameters 158

Configuring Media Parameters (GUI) 158
Configuring Voice Prioritization Using Preferred Call Numbers 159
Voice Prioritization Using Preferred Call Numbers 159
Prerequisites for Configuring Voice Prioritization Using Preferred Call Numbers 159
Configuring a Preferred Call Number (GUI) 159
Configuring a Preferred Call Number (CLI) 160
Configuring EDCA Parameters 160
Enhanced Distributed Channel Access Parameters 160
Configuring EDCA Parameters (GUI) 160
Configuring EDCA Parameters (CLI) 161

CHAPTER 17 **Configuring the Cisco Discovery Protocol** 163
Cisco Discovery Protocol 163
Restrictions for Cisco Discovery Protocol 163
Configuring the Cisco Discovery Protocol 165
Configuring the Cisco Discovery Protocol (GUI) 165
Configuring the Cisco Discovery Protocol (CLI) 166
Viewing Cisco Discovery Protocol Information 167
Viewing Cisco Discovery Protocol Information (GUI) 167
Viewing Cisco Discovery Protocol Information (CLI) 169
Getting CDP Debug Information 170

CHAPTER 18 **Configuring Authentication for the Controller and NTP/SNTP Server** 171
Authentication for the Controller and NTP/SNTP Server 171
Guidelines and Restrictions on NTP 171
Configuring the NTP/SNTP Server to Obtain the Date and Time (GUI) 171
Configuring the NTP/SNTP Server for Authentication (CLI) 172

CHAPTER 19 **Configuring RFID Tag Tracking** 173
Information About Configuring RFID Tag Tracking 173
Configuring RFID Tag Tracking (CLI) 174
Viewing RFID Tag Tracking Information (CLI) 175
Debugging RFID Tag Tracking Issues (CLI) 175

CHAPTER 20 **Resetting the Controller to Default Settings** 177

Resetting the Controller to Default Settings 177

Resetting the Controller to Default Settings (GUI) 177

Resetting the Controller to Default Settings (CLI) 177

CHAPTER 21 **Managing Controller Software and Configurations** 179

Upgrading the Controller Software 179

Considerations for Upgrading Controller Software 179

Upgrading Controller Software (GUI) 180

Upgrading Controller Software (CLI) 182

Predownloading an Image to an Access Point 185

Access Point Predownload Process 186

Guidelines and Restrictions for Predownloading an Image to an Access Point 187

Predownloading an Image to Access Points—Global Configuration (GUI) 188

Predownloading an Image to Access Points (CLI) 189

Transferring Files to and from a Controller 190

Downloading a Login Banner File 190

Downloading a Login Banner File (GUI) 191

Downloading a Login Banner File (CLI) 192

Clearing the Login Banner (GUI) 192

Downloading Device Certificates 193

Downloading Device Certificates (GUI) 193

Downloading Device Certificates (CLI) 194

Downloading CA Certificates 195

Download CA Certificates (GUI) 196

Downloading CA Certificates (CLI) 196

Uploading PACs 197

Uploading PACs (GUI) 198

Uploading PACs (CLI) 198

Backing Up and Restoring Controller Configuration 199

Uploading Configuration Files 200

Downloading Configuration Files 201

Saving Configurations 204

Editing Configuration Files 204
Clearing the Controller Configuration 205
Erasing the Controller Configuration 206
Resetting the Controller 206

CHAPTER 22 **Managing User Accounts** 207
Configuring Guest User Accounts 207
Guest Accounts 207
Restrictions on Managing User Accounts 207
Creating a Lobby Ambassador Account 208
Creating a Lobby Ambassador Account (GUI) 208
Creating a Lobby Ambassador Account (CLI) 208
Creating Guest User Accounts as a Lobby Ambassador (GUI) 209
Viewing Guest User Accounts 210
Viewing the Guest Accounts (GUI) 210
Viewing the Guest Accounts (CLI) 210
Configuring Administrator Usernames and Passwords 210
Administrator Usernames and Passwords 210
Configuring Usernames and Passwords (GUI) 210
Configuring Usernames and Passwords (CLI) 211
Restoring Passwords 211
Changing the Default Values for SNMP v3 Users 212
Information About Changing the Default Values for SNMP v3 Users 212
Changing the SNMP v3 User Default Values (GUI) 212
Changing the SNMP v3 User Default Values (CLI) 213
Generating a Certificate Signing Request using OpenSSL 213
Downloading Third-Party Certificate (GUI) 215
Downloading Third-Party Certificate (CLI) 216

CHAPTER 23 **Managing Web Authentication** 217
Obtaining a Web Authentication Certificate 217
Information About Web Authentication Certificates 217
Support for Chained Certificate 218
Obtaining a Web Authentication Certificate (GUI) 218

Obtaining a Web Authentication Certificate (CLI) 218
Web Authentication Process 220
Disabling Security Alert for Web Authentication Process 220
Choosing the Default Web Authentication Login Page 223
Default Web Authentication Login Page 223
Choosing the Default Web Authentication Login Page (GUI) 223
Choosing the Default Web Authentication Login Page (CLI) 224
Example: Creating a Customized Web Authentication Login Page 225
Example: Modified Default Web Authentication Login Page Example 228
Using a Customized Web Authentication Login Page from an External Web Server 229
Information About Customized Web Authentication Login Page 229
Choosing a Customized Web Authentication Login Page from an External Web Server (GUI) 230
Choosing a Customized Web Authentication Login Page from an External Web Server (CLI) 230
Downloading a Customized Web Authentication Login Page 230
Prerequisites for Downloading a Customized Web Authentication Login Page 231
Downloading a Customized Web Authentication Login Page (GUI) 231
Downloading a Customized Web Authentication Login Page (CLI) 232
Example: Customized Web Authentication Login Page 233
Verifying the Web Authentication Login Page Settings (CLI) 233
Assigning Login, Login Failure, and Logout Pages per WLAN 234
Assigning Login, Login Failure, and Logout Pages per WLAN 234
Assigning Login, Login Failure, and Logout Pages per WLAN (GUI) 234
Assigning Login, Login Failure, and Logout Pages per WLAN (CLI) 235
Configuring Authentication for Sleeping Clients 236
Authentication of Sleeping Clients 236
Restrictions for Authenticating Sleeping Clients 237
Configuring Authentication for Sleeping Clients (GUI) 238
Configuring Authentication for Sleeping Clients (CLI) 238

CHAPTER 24 **Configuring Wired Guest Access 241**
Wired Guest Access 241
Prerequisites for Configuring Wired Guest Access 242
Restrictions for Configuring Wired Guest Access 242
Configuring Wired Guest Access (GUI) 242

Configuring Wired Guest Access (CLI) 244
Supporting IPv6 Client Guest Access 247

CHAPTER 25 **Troubleshooting** 249
Interpreting LEDs 249
Information About Interpreting LEDs 249
Interpreting Controller LEDs 249
Interpreting Lightweight Access Point LEDs 250
System Messages 250
Information About System Messages 250
Viewing System Resources 253
Viewing System Resources 253
Viewing System Resources (GUI) 253
Viewing System Resources (CLI) 254
Using the CLI to Troubleshoot Problems 254
Configuring System and Message Logging 255
System and Message Logging 255
Configuring System and Message Logging (GUI) 255
Viewing Message Logs (GUI) 258
Configuring System and Message Logging (CLI) 258
Viewing System and Message Logs (CLI) 262
Viewing Access Point Event Logs 262
Information About Access Point Event Logs 262
Viewing Access Point Event Logs (CLI) 262
Uploading Logs and Crash Files 263
Upload Logs and Crash Files 263
Uploading Logs and Crash Files (GUI) 264
Uploading Logs and Crash Files (CLI) 264
Uploading Core Dumps from the Controller 265
Uploading Core Dumps from the Controller 265
Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI) 266
Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (CLI) 266
Uploading Core Dumps from Controller to a Server (CLI) 267
Uploading Packet Capture Files 268

Uploading Packet Capture Files 268
Restrictions for Uploading Packet Capture Files 269
Uploading Packet Capture Files (GUI) 270
Uploading Packet Capture Files (CLI) 270
Monitoring Memory Leaks 271
Monitoring Memory Leaks (CLI) 271
Troubleshooting CCXv5 Client Devices 272
Information About Troubleshooting CCXv5 Client Devices 272
Restrictions for CCXv5 Client Devices 272
Configuring Diagnostic Channel 273
Configuring the Diagnostic Channel (GUI) 273
Configuring the Diagnostic Channel (CLI) 274
Configuring Client Reporting 278
Configuring Client Reporting (GUI) 278
Configuring Client Reporting (CLI) 279
Configuring Roaming and Real-Time Diagnostics 279
Configuring Roaming and Real-Time Diagnostics (CLI) 280
Using the Debug Facility 282
Using the Debug Facility 282
Configuring the Debug Facility (CLI) 284
Configuring Wireless Sniffing 287
Wireless Sniffing 287
Prerequisites for Wireless Sniffing 287
Restrictions on Wireless Sniffing 288
Configuring Sniffing on an Access Point (GUI) 288
Configuring Sniffing on an Access Point (CLI) 288
Troubleshooting Access Points Using Telnet or SSH 289
Information About Troubleshooting Access Points Using Telnet or SSH 289
Troubleshooting Access Points Using Telnet or SSH (GUI) 290
Troubleshooting Access Points Using Telnet or SSH (CLI) 290
Debugging the Access Point Monitor Service 291
Debugging the Access Point Monitor Service 291
Debugging Access Point Monitor Service Issues (CLI) 291
Troubleshooting Memory Leaks 291

Troubleshooting Memory Leaks 291
Troubleshooting OfficeExtend Access Points 292
Troubleshooting OfficeExtend Access Points 292
Interpreting OfficeExtend LEDs 292
Positioning OfficeExtend Access Points for Optimal RF Coverage 292
Troubleshooting Common Problems 293

PART II **Ports and Interfaces** 295

CHAPTER 26 **Overview of Ports and Interfaces** 297
Ports 297
Distribution System Ports 298
Restrictions for Configuring Distribution System Ports 298
Service Port 299
Interfaces 300
Restrictions on Configuring Interfaces 301
Dynamic AP Management 301
WLANs 301

CHAPTER 27 **Configuring the Management Interface** 305
Management Interface 305
Configuring the Management Interface (GUI) 306
Configuring the Management Interface (CLI) 307

CHAPTER 28 **Configuring the AP-Manager Interface** 311
AP-Manager Interface 311
Restrictions for Configuring AP Manager Interface 311
Configuring the AP-Manager Interface (GUI) 312
Configuring the AP Manager Interface (CLI) 313
Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller 313

CHAPTER 29 **Configuring Virtual Interfaces** 317
Virtual Interface 317
Configuring Virtual Interfaces (GUI) 318

Configuring Virtual Interfaces (CLI) 318

CHAPTER 30 **Configuring Service-Port Interfaces** 319

Service-Port Interfaces 319

Restrictions on Configuring Service-Port Interfaces 320

Configuring Service-Port Interfaces Using IPv4 (GUI) 320

Configuring Service-Port Interfaces Using IPv4 (CLI) 320

Configuring Service-Port Interface Using IPv6 (GUI) 321

Configuring Service-Port Interfaces Using IPv6 (CLI) 322

CHAPTER 31 **Configuring Dynamic Interfaces** 323

Dynamic Interface 323

Prerequisites for Configuring Dynamic Interfaces 324

Restrictions for Configuring Dynamic Interfaces 324

Configuring Dynamic Interfaces (GUI) 324

Configuring Dynamic Interfaces (CLI) 325

CHAPTER 32 **Configuring Ports** 329

Configuring Ports (GUI) 329

CHAPTER 33 **Information About Using Cisco 5500 Series Controller USB Console Port** 331

USB Console OS Compatibility 331

Changing the Cisco USB Systems Management Console COM Port to an Unused Port 332

CHAPTER 34 **Configuring Link Aggregation** 333

Link Aggregation 333

Restrictions on Link Aggregation 333

Configuring Link Aggregation (GUI) 335

Configuring Link Aggregation (CLI) 336

Verifying Link Aggregation Settings (CLI) 336

Configuring Neighbor Devices to Support Link Aggregation 336

Choosing Between Link Aggregation and Multiple AP-Manager Interfaces 337

CHAPTER 35 **Configuring Multiple AP-Manager Interfaces** 339

Information About Multiple AP-Manager Interfaces 339

Restrictions on Configuring Multiple AP Manager Interfaces 339

Creating Multiple AP-Manager Interfaces (GUI) 340

Creating Multiple AP-Manager Interfaces (CLI) 340

CHAPTER 36 **Configuring VLAN Select** 343

Information About VLAN Select 343

Restrictions for Configuring VLAN Select 344

Configuring Interface Groups 344

Interface Groups 344

Restrictions on Configuring Interface Groups 344

Creating Interface Groups (GUI) 345

Creating Interface Groups (CLI) 345

Adding Interfaces to Interface Groups (GUI) 345

Adding Interfaces to Interface Groups (CLI) 346

Viewing VLANs in Interface Groups (CLI) 346

Adding an Interface Group to a WLAN (GUI) 346

Adding an Interface Group to a WLAN (CLI) 346

CHAPTER 37 **Configuring Multicast Optimization** 349

Multicast Optimization 349

Configuring a Multicast VLAN (GUI) 349

Configuring a Multicast VLAN (CLI) 350

PART III **VideoStream** 351

CHAPTER 38 **VideoStream** 353

Information about Media Stream 353

Prerequisites for Media Stream 353

Restrictions for Configuring VideoStream 353

Configuring Media Stream (GUI) 354

Configuring Media Stream (CLI) 357

Viewing and Debugging Media Stream 358

PART IV Security Solutions 361

CHAPTER 39 Cisco Unified Wireless Network Solution Security 363

Security Overview 363

Layer 1 Solutions 363

Layer 2 Solutions 363

Restrictions for Layer 2 Solutions 364

Layer 3 Solutions 364

Integrated Security Solutions 364

CHAPTER 40 Configuring RADIUS 365

Setting up RADIUS 365

Configuring RADIUS (GUI) 367

Configuring RADIUS (CLI) 372

RADIUS Authentication Attributes Sent by the Controller 376

Authentication Attributes Honored in Access-Accept Packets (Airespace) 378

RADIUS Accounting Attributes 384

CHAPTER 41 Configuring TACACS+ 387

Setting up TACACS+ 387

TACACS+ VSA 389

Configuring TACACS+ (GUI) 390

Configuring TACACS+ (CLI) 392

Viewing the TACACS+ Administration Server Logs 393

CHAPTER 42 Configuring Maximum Local Database Entries 397

Maximum Local Database Entries 397

Configuring Maximum Local Database Entries (GUI) 397

Configuring Maximum Local Database Entries (CLI) 397

CHAPTER 43 Configuring Local Network Users on the Controller 399

Local Network Users on Controller 399

Configuring Local Network Users for the Controller (GUI) 399
Configuring Local Network Users for the Controller (CLI) 400

CHAPTER 44 Configuring Password Policies 403
Password Policies 403
Configuring Password Policies (GUI) 404
Configuring Password Policies (CLI) 404

CHAPTER 45 Configuring LDAP 407
LDAP 407
Configuring LDAP (GUI) 408
Configuring LDAP (CLI) 410

CHAPTER 46 Configuring Local EAP 413
Local EAP 413
Restrictions for Local EAP 414
Configuring Local EAP (GUI) 415
Configuring Local EAP (CLI) 418

CHAPTER 47 Configuring the System for SpectraLink NetLink Telephones 423
Information About SpectraLink NetLink Telephones 423
Configuring SpectraLink NetLink Phones 423
Enabling Long Preambles (GUI) 423
Enabling Long Preambles (CLI) 424
Configuring Enhanced Distributed Channel Access (CLI) 424

CHAPTER 48 Configuring RADIUS NAC Support 427
ISE NAC Support 427
Device Registration 427
Central Web Authentication 427
Local Web Authentication 428
Guidelines and Restrictions on ISE NAC Support 429
Configuring ISE NAC Support (GUI) 430
Configuring ISE NAC Support (CLI) 430

CHAPTER 49 **Using Management Over Wireless** 431

Management over Wireless 431

Enabling Management over Wireless (GUI) 431

Enabling Management over Wireless (CLI) 432

CHAPTER 50 **Using Dynamic Interfaces for Management** 433

Using Dynamic Interfaces for Management 433

Configuring Management using Dynamic Interfaces (CLI) 434

CHAPTER 51 **Configuring DHCP Option 82** 435

DHCP Option 82 435

Restrictions on DHCP Option 82 436

Configuring DHCP Option 82 (GUI) 436

Configuring DHCP Option 82 (CLI) 436

CHAPTER 52 **Configuring and Applying Access Control Lists** 439

Information about Access Control Lists 439

Guidelines and Restrictions on Access Control Lists 439

Configuring and Applying Access Control Lists (GUI) 440

Configuring Access Control Lists (GUI) 440

Applying an Access Control List to an Interface (GUI) 443

Applying an Access Control List to the Controller CPU (GUI) 443

Applying an Access Control List to a WLAN (GUI) 444

Applying a Preauthentication Access Control List to a WLAN (GUI) 444

Configuring and Applying Access Control Lists (CLI) 444

Configuring Access Control Lists (CLI) 444

Applying Access Control Lists (CLI) 445

Configuring Layer 2 Access Control Lists 446

Layer 2 Access Control Lists 446

Restrictions on Layer 2 Access Control Lists 447

Configuring Layer 2 Access Control Lists (CLI) 448

CHAPTER 53 **Configuring Management Frame Protection** 449

Protected Management Frames (Management Frame Protection) 449

Restrictions for Management Frame Protection 450

Configuring Infrastructure MFP (GUI) 451

Viewing the Management Frame Protection Settings (GUI) 451

Configuring Infrastructure MFP (CLI) 452

Viewing the Management Frame Protection Settings (CLI) 452

Debugging Management Frame Protection Issues (CLI) 452

CHAPTER 54 **Configuring Client Exclusion Policies** 455

Configuring Client Exclusion Policies (GUI) 455

Configuring Client Exclusion Policies (CLI) 455

CHAPTER 55 **Configuring Identity Networking** 459

Identity Networking 459

RADIUS Attributes Used in Identity Networking 460

CHAPTER 56 **Configuring AAA Override** 465

AAA Override 465

Restrictions for AAA Override 465

Updating the RADIUS Server Dictionary File for Proper QoS Values 466

Configuring AAA Override (GUI) 467

Configuring AAA Override (CLI) 468

CHAPTER 57 **Managing Rogue Devices** 469

Rogue Devices 469

Configuring Rogue Detection (GUI) 474

Configuring Rogue Detection (CLI) 476

CHAPTER 58 **Classifying Rogue Access Points** 481

Rogue Access Point Classification 481

Guidelines and Restrictions for Classifying Rogue Access Points 484

Configuring Rogue Classification Rules (GUI) 484
Viewing and Classifying Rogue Devices (GUI) 487
Configuring Rogue Classification Rules (CLI) 490
Viewing and Classifying Rogue Devices (CLI) 493

CHAPTER 59 **Configuring Cisco TrustSec SXP** 497
Cisco TrustSec 497
Guidelines and Restrictions on Cisco TrustSec 499
Configuring SXP on Cisco WLC (GUI) 499
Creating a New SXP Connection (GUI) 500
Configuring SXP on Cisco WLC (CLI) 500

CHAPTER 60 **Configuring Local Policies** 503
Local Policies 503
Guidelines and Restrictions for Local Policy Classification 504
Configuring Local Policies (GUI) 505
Configuring Local Policies (CLI) 506

CHAPTER 61 **Configuring Cisco Intrusion Detection System** 509
Cisco Intrusion Detection System 509
Shunned Clients 509
Configuring IDS Sensors (GUI) 510
Viewing Shunned Clients (GUI) 510
Configuring IDS Sensors (CLI) 511
Viewing Shunned Clients (CLI) 512

CHAPTER 62 **Configuring IDS Signatures** 515
Intrusion Detection System Signatures 515
Configuring IDS Signatures (GUI) 517
Uploading or Downloading IDS Signatures 517
Enabling or Disabling IDS Signatures 518
Viewing IDS Signature Events (GUI) 520
Configuring IDS Signatures (CLI) 520
Viewing IDS Signature Events (CLI) 522

CHAPTER 63 **Configuring wIPS** 523

Wireless Intrusion Prevention System 523

Restrictions for wIPS 529

Configuring wIPS on an Access Point (GUI) 530

Configuring wIPS on an Access Point (CLI) 530

Viewing wIPS Information (CLI) 531

CHAPTER 64 **Configuring the Wi-Fi Direct Client Policy** 533

Wi-Fi Direct Client Policy 533

Restrictions for the Wi-Fi Direct Client Policy 533

Configuring the Wi-Fi Direct Client Policy (GUI) 534

Configuring the Wi-Fi Direct Client Policy (CLI) 534

Monitoring and Troubleshooting the Wi-Fi Direct Client Policy (CLI) 535

CHAPTER 65 **Configuring Web Auth Proxy** 537

Web Authentication Proxy 537

Configuring the Web Authentication Proxy (GUI) 538

Configuring the Web Authentication Proxy (CLI) 538

CHAPTER 66 **Detecting Active Exploits** 541

Detecting Active Exploits 541

PART V **WLANs** 543

CHAPTER 67 **Configuring WLANs** 545

Prerequisites for WLANs 545

Restrictions for WLANs 545

Information About WLANs 547

Creating and Removing WLANs (GUI) 547

Enabling and Disabling WLANs (GUI) 548

Creating and Deleting WLANs (CLI) 549

Enabling and Disabling WLANs (CLI) 549

Viewing WLANs (CLI) 550

Searching WLANs (GUI) 550
Assigning WLANs to Interfaces 550
Configuring Network Access Identifier (CLI) 551

CHAPTER 68 Setting the Client Count per WLAN 553
Restrictions for Setting Client Count for WLANs 553
Client Count per WLAN 553
Configuring the Client Count per WLAN (GUI) 554
Configuring the Maximum Number of Clients per WLAN (CLI) 554
Configuring the Maximum Number of Clients for each AP Radio per WLAN (GUI) 554
Configuring the Maximum Number of Clients for each AP Radio per WLAN (CLI) 555
Deauthenticating Clients (CLI) 555

CHAPTER 69 Configuring DHCP 557
Restrictions for Configuring DHCP for WLANs 557
Information about Dynamic Host Configuration Protocol 557
Internal DHCP Servers 557
External DHCP Servers 558
DHCP Assignments 558
Configuring DHCP (GUI) 559
Configuring DHCP (CLI) 560
Debugging DHCP (CLI) 560
DHCP Client Handling 561

CHAPTER 70 Configuring DHCP Scopes 563
Restrictions for Configuring Internal DHCP Server 563
Internal DHCP Server 563
Configuring DHCP Scopes (GUI) 564
Configuring DHCP Scopes (CLI) 565

CHAPTER 71 Configuring MAC Filtering for WLANs 567
Restrictions for MAC Filtering 567
MAC Filtering of WLANs 567
Enabling MAC Filtering 567

CHAPTER 72 **Configuring Local MAC Filters** 569

Prerequisites for Configuring Local MAC Filters 569

Local MAC Filters 569

Configuring Local MAC Filters (CLI) 569

CHAPTER 73 **Configuring Timeouts** 571

Configuring a Timeout for Disabled Clients 571

Timeout for Disabled Clients 571

Configuring Timeout for Disabled Clients (CLI) 571

Configuring Session Timeout 571

Session Timeouts 571

Configuring a Session Timeout (GUI) 572

Configuring a Session Timeout (CLI) 572

Configuring the User Idle Timeout 573

User Idle Timeout per WLAN 573

Configuring Per-WLAN User Idle Timeout (CLI) 573

CHAPTER 74 **Configuring the DTIM Period** 575

DTIM Period 575

Configuring the DTIM Period (GUI) 576

Configuring the DTIM Period (CLI) 576

CHAPTER 75 **Configuring Peer-to-Peer Blocking** 577

Restrictions on Peer-to-Peer Blocking 577

Peer-to-Peer Blocking 577

Configuring Peer-to-Peer Blocking (GUI) 578

Configuring Peer-to-Peer Blocking (CLI) 578

CHAPTER 76 **Configuring Layer2 Security** 581

Prerequisites for Layer 2 Security 581

Configuring Static WEP Keys (CLI) 582

Configuring Dynamic 802.1X Keys and Authorization (CLI) 582

Configuring 802.11r BSS Fast Transition 583

Restrictions for 802.11r Fast Transition 583
802.11r Fast Transition 584
Configuring 802.11r Fast Transition (GUI) 586
Configuring 802.11r Fast Transition (CLI) 587
Troubleshooting 802.11r BSS Fast Transition 588
MAC Authentication Failover to 802.1X Authentication 588
Configuring MAC Authentication Failover to 802.1x Authentication (GUI) 588
Configuring MAC Authentication Failover to 802.1X Authentication (CLI) 588
Configuring 802.11w 589
Restrictions for 802.11w 589
802.11w 589
Configuring 802.11w (GUI) 590
Configuring 802.11w (CLI) 591

CHAPTER 77 **Configuring a WLAN for Static WEP** 593
Restrictions for Configuring Static WEP 593
WLAN for Static WEP 593
WPA1 and WPA2 594
Configuring WPA1+WPA2 595
Configuring WPA1+WPA2 (GUI) 595
Configuring WPA1+WPA2 (CLI) 595

CHAPTER 78 **Configuring Sticky Key Caching** 599
Sticky Key Caching 599
Restrictions for Sticky Key Caching 599
Configuring Sticky Key Caching (CLI) 600

CHAPTER 79 **Configuring CKIP** 603
Cisco Key Integrity Protocol 603
Configuring CKIP (GUI) 604
Configuring CKIP (CLI) 604

CHAPTER 80 **Configuring Layer 3 Security** 607

Configuring Layer 3 Security Using Web Authentication 607
Prerequisites for Configuring Web Authentication on a WLAN 607
Restrictions for Configuring Web Authentication on a WLAN 608
Information About Web Authentication 608
Configuring Web Authentication 608
Configuring Web Authentication (GUI) 608
Configuring Web Authentication (CLI) 608

CHAPTER 81 **Configuring Captive Bypassing** 611
Captive Bypassing 611
Configuring Captive Bypassing (CLI) 612

CHAPTER 82 **Configuring a Fallback Policy with MAC Filtering and Web Authentication** 613
Fallback Policy with MAC Filtering and Web Authentication 613
Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI) 613
Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI) 614

CHAPTER 83 **Assigning a QoS Profile to a WLAN** 617
QoS Profiles 617
Assigning a QoS Profile to a WLAN (GUI) 618
Assigning a QoS Profile to a WLAN (CLI) 619

CHAPTER 84 **Configuring QoS Enhanced BSS** 621
Prerequisites for Using QoS Enhanced BSS on Cisco 7921 and 7920 Wireless IP Phones 621
Restrictions for QoS Enhanced BSS 622
QoS Enhanced BSS 622
Configuring QBSS (GUI) 623
Configuring QBSS (CLI) 623

CHAPTER 85 **Configuring Media Session Snooping and Reporting** 625
Media Session Snooping and Reporting 625
Restrictions for Media Session Snooping and Reporting 625
Configuring Media Session Snooping (GUI) 626
Configuring Media Session Snooping (CLI) 626

CHAPTER 86 **Configuring Key Telephone System-Based CAC** 631
Restrictions for Key Telephone System-Based CAC 631
Key Telephone System-Based CAC 631
Configuring KTS-based CAC (GUI) 632
Configuring KTS-based CAC (CLI) 632
Related Commands 633

CHAPTER 87 **Configuring Reanchoring of Roaming Voice Clients** 635
Restrictions for Configuring Reanchoring of Roaming Voice Clients 635
Information About Reanchoring of Roaming Voice Clients 635
Configuring Reanchoring of Roaming Voice Clients (GUI) 636
Configuring Reanchoring of Roaming Voice Clients (CLI) 636

CHAPTER 88 **Configuring Seamless IPv6 Mobility** 637
Prerequisites for Configuring IPv6 Mobility 637
Restrictions on Configuring IPv6 Mobility 637
IPv6 Client Mobility 638
Configuring IPv6 Globally 638
Configuring IPv6 Globally (GUI) 638
Configuring IPv6 Globally (CLI) 639
Configuring RA Guard for IPv6 Clients 639
RA Guard 639
Configuring RA Guard (GUI) 639
Configuring RA Guard (CLI) 640
Configuring RA Throttling for IPv6 Clients 640
RA Throttling 640
Configuring RA Throttling (GUI) 640
Configuring the RA Throttle Policy (CLI) 641
Configuring IPv6 Neighbor Discovery Caching 641
IPv6 Neighbor Discovery 641
Configuring Neighbor Binding (GUI) 641
Configuring Neighbor Binding (CLI) 642

CHAPTER 89 **Configuring Cisco Client Extensions** 643

Prerequisites for Configuring Cisco Client Extensions 643

Guidelines and Restrictions for Configuring Cisco Client Extensions 643

Cisco Client Extensions 644

Configuring CCX Aironet IEs (GUI) 644

Viewing a Client's CCX Version (GUI) 644

Configuring CCX Aironet IEs (CLI) 644

Viewing a Client's CCX Version (CLI) 645

CHAPTER 90 **Configuring Remote LANs** 647

Prerequisites for Configuring Remote LANs 647

Restrictions for Configuring Remote LANs 647

Remote LANs 647

Configuring a Remote LAN (GUI) 648

Configuring a Remote LAN (CLI) 649

CHAPTER 91 **AP Groups** 651

Access Point Groups 651

Prerequisites for Configuring AP Groups 651

AP Groups Supported on Controller Platforms 651

Restrictions on Configuring Access Point Groups 652

Configuring Access Point Groups 653

Creating Access Point Groups (GUI) 653

Creating Access Point Groups (CLI) 655

Viewing Access Point Groups (CLI) 656

802.1Q-in-Q VLAN Tagging 656

Restrictions for 802.1Q-in-Q VLAN Tagging 656

Configuring 802.1Q-in-Q VLAN Tagging (GUI) 657

Configuring 802.1Q-in-Q VLAN Tagging (CLI) 657

CHAPTER 92 **Configuring RF Profiles** 659

Prerequisites for Configuring RF Profiles 659

Restrictions on Configuring RF Profiles 659

RF Profiles 660
Configuring an RF Profile (GUI) 662
Configuring an RF Profile (CLI) 663
Applying an RF Profile to AP Groups (GUI) 665
Applying RF Profiles to AP Groups (CLI) 665

CHAPTER 93 **Configuring Web Redirect with 8021.X Authentication** 667
Web Redirect with 802.1X Authentication 667
Conditional Web Redirect 667
Splash Page Web Redirect 668
Configuring the RADIUS Server (GUI) 668
Configuring Web Redirect 669
Configuring Web Redirect (GUI) 669
Configuring Web Redirect (CLI) 669
Disabling Accounting Servers per WLAN (GUI) 670
Disabling Coverage Hole Detection per WLAN 670
Disabling Coverage Hole Detection on a WLAN (GUI) 670
Disabling Coverage Hole Detection on a WLAN (CLI) 671

CHAPTER 94 **Configuring NAC Out-of-Band Integration** 673
Prerequisites for NAC Out Of Band 673
Restrictions for NAC Out of Band 674
NAC Out-of-Band Integration 674
Configuring NAC Out-of-Band Integration (GUI) 675
Configuring NAC Out-of-Band Integration (CLI) 677

CHAPTER 95 **Configuring Passive Clients** 679
Restrictions for Passive Clients 679
Passive Clients 679
Configuring Passive Clients (GUI) 680
Enabling the Multicast-Multicast Mode (GUI) 680
Enabling the Global Multicast Mode on Controllers (GUI) 681
Enabling the Passive Client Feature on the Controller (GUI) 681
Configuring Passive Clients (CLI) 681

CHAPTER 96 **Configuring Client Profiling** 683

Prerequisites for Configuring Client Profiling 683

Restrictions for Configuring Client Profiling 684

Client Profiling 684

Configuring Client Profiling 685

Configuring Client Profiling (GUI) 685

Configuring Client Profiling (CLI) 685

CHAPTER 97 **Configuring Per-WLAN RADIUS Source Support** 687

Prerequisites for Per-WLAN RADIUS Source Support 687

Per-WLAN RADIUS Source Support 687

Configuring Per-WLAN RADIUS Source Support (CLI) 688

Monitoring the Status of Per-WLAN RADIUS Source Support (CLI) 688

CHAPTER 98 **Configuring Mobile Concierge** 691

Mobile Concierge 691

Configuring Mobile Concierge (802.11u) 691

Configuring Mobile Concierge (802.11u) (GUI) 691

Configuring Mobile Concierge (802.11u) (CLI) 692

Configuring 802.11u Mobility Services Advertisement Protocol 694

802.11u MSAP 694

Configuring 802.11u MSAP (GUI) 694

Configuring MSAP (CLI) 694

Configuring 802.11u HotSpot 695

Information About 802.11u HotSpot 695

Configuring 802.11u HotSpot (GUI) 695

Configuring HotSpot 2.0 (CLI) 696

Configuring Access Points for HotSpot2 (GUI) 697

Configuring Access Points for HotSpot2 (CLI) 698

Downloading the Icon File (CLI) 701

CHAPTER 99 **Configuring Assisted Roaming** 703

Restrictions for Assisted Roaming 703

Assisted Roaming 703
Configuring Assisted Roaming (CLI) 704

PART VI Lightweight Access Points 707

CHAPTER 100 Using Access Point Communication Protocols 709
CAPWAP 709
Restrictions for Access Point Communication Protocols 710
Data Encryption 710
Restrictions on Data Encryption 711
Upgrading or Downgrading DTLS Images for Cisco 5508 WLC 712
Guidelines When Upgrading to or from a DTLS Image 712
Configuring Data Encryption (GUI) 712
Configuring Data Encryption (CLI) 713
Viewing CAPWAP Maximum Transmission Unit Information 713
Debugging CAPWAP 714
Controller Discovery Process 714
Guidelines and Restrictions on Controller Discovery Process 715
Verifying that Access Points Join the Controller 716
Verifying that Access Points Join the Controller (GUI) 716
Verifying that Access Points Join the Controller (CLI) 716

CHAPTER 101 Searching for Access Points 717
Information About Searching for Access Points 717
Searching the AP Filter (GUI) 717
Monitoring the Interface Details 719
Searching for Access Point Radios 722
Information About Searching for Access Point Radios 722
Searching for Access Point Radios (GUI) 722

CHAPTER 102 Configuring Global Credentials for Access Points 725
Global Credentials for Access Points 725
Restrictions for Global Credentials for Access Points 726
Configuring Global Credenitals for Access Points 726

Configuring Global Credentials for Access Points (GUI) 726
Configuring Global Credentials for Access Points (CLI) 727

CHAPTER 103 Configuring Authentication for Access Points 729
AP 802.1X Supplicant 729
Prerequisites for Configuring Authentication for Access Points 730
Restrictions for Authenticating Access Points 731
Configuring Authentication for Access Points (GUI) 731
Configuring Authentication for Access Points (CLI) 732
Configuring the Switch for Authentication 733

CHAPTER 104 Configuring Embedded Access Points 735
Embedded Access Points 735

CHAPTER 105 Converting Autonomous Access Points to Lightweight Mode 737
Converting Autonomous Access Points to Lightweight Mode 737
Restrictions for Converting Autonomous Access Points to Lightweight Mode 738
Converting Autonomous Access Points to Lightweight Mode 738
Reverting from Lightweight Mode to Autonomous Mode 739
Reverting to a Previous Release (CLI) 739
Reverting to a Previous Release Using the MODE Button and a TFTP Server 739
Authorizing Access Points 740
Authorizing Access Points Using SSCs 740
Authorizing Access Points for Virtual Controllers Using SSC 740
Configuring SSC (GUI) 741
Configuring SSC (CLI) 741
Authorizing Access Points Using MICs 741
Authorizing Access Points Using LSCs 741
Configuring Locally Significant Certificates (GUI) 742
Configuring Locally Significant Certificates (CLI) 743
Authorizing Access Points (GUI) 745
Authorizing Access Points (CLI) 746
Configuring VLAN Tagging for CAPWAP Frames from Access Points 746
VLAN Tagging for CAPWAP Frames from Access Points 746

Configuring VLAN Tagging for CAPWAP Frames from Access Points (GUI) 747
Configuring VLAN Tagging for CAPWAP Frames from Access Points (CLI) 747
Using DHCP Option 43 and DHCP Option 60 748
Troubleshooting the Access Point Join Process 748
Configuring the Syslog Server for Access Points (CLI) 750
Viewing Access Point Join Information 750
Viewing Access Point Join Information (GUI) 750
Viewing Access Point Join Information (CLI) 751
Sending Debug Commands to Access Points Converted to Lightweight Mode 753
Understanding How Converted Access Points Send Crash Information to the Controller 753
Understanding How Converted Access Points Send Radio Core Dumps to the Controller 753
Retrieving Radio Core Dumps (CLI) 753
Uploading Radio Core Dumps (GUI) 754
Uploading Radio Core Dumps (CLI) 754
Uploading Memory Core Dumps from Converted Access Points 755
Uploading Access Point Core Dumps (GUI) 755
Uploading Access Point Core Dumps (CLI) 756
Viewing the AP Crash Log Information 756
Viewing the AP Crash Log information (GUI) 756
Viewing the AP Crash Log information (CLI) 756
Displaying MAC Addresses for Converted Access Points 757
Disabling the Reset Button on Access Points Converted to Lightweight Mode 757
Configuring a Static IP Address on a Lightweight Access Point 757
Configuring a Static IP Address (GUI) 758
Configuring a Static IP Address (CLI) 758
Supporting Oversized Access Point Images 760
Recovering the Access Point—Using the TFTP Recovery Procedure 760

CHAPTER 106 **Configuring Packet Capture** 761
Information About Packet Capture 761
Restrictions for Packet Capture 762
Configuring Packet Capture (CLI) 762

CHAPTER 107 **OfficeExtend Access Points** 765

Information About OfficeExtend Access Points 765
OEAP 600 Series Access Points 766
OEAP in Local Mode 767
Supported WLAN Settings for 600 Series OfficeExtend Access Point 767
WLAN Security Settings for the 600 Series OfficeExtend Access Point 768
Authentication Settings 771
Supported User Count on 600 Series OfficeExtend Access Point 772
Remote LAN Settings 772
Channel Management and Settings 773
Firewall Settings 774
Additional Caveats 774
Implementing Security 775
Licensing for an OfficeExtend Access Point 775
Configuring OfficeExtend Access Points 776
Configuring OfficeExtend Access Points (GUI) 776
Configuring OfficeExtend Access Points (CLI) 778
Configuring Split Tunneling for a WLAN or a Remote LAN 780
Configuring Split Tunneling for a WLAN or a Remote LAN (GUI) 780
Configuring Split Tunneling for a WLAN or a Remote LAN (CLI) 780
Configuring a Personal SSID on an OfficeExtend Access Point Other than 600 Series OEAP 781
Viewing OfficeExtend Access Point Statistics 782
Remote LANs 782
Configuring a Remote LAN (GUI) 783
Configuring a Remote LAN (CLI) 784

CHAPTER 108 **Using Cisco Workgroup Bridges** 785
Information About Cisco Workgroup Bridges 785
Restrictions for Cisco Workgroup Bridges 787
WGB Configuration Example 788
Viewing the Status of Workgroup Bridges (GUI) 789
Viewing the Status of Workgroup Bridges (CLI) 789
Debugging WGB Issues (CLI) 789

CHAPTER 109 **Using Non-Cisco Workgroup Bridges** 791

Non-Cisco Workgroup Bridges 791
Restrictions for Non-Cisco Workgroup Bridges 792

CHAPTER 110 Configuring Backup Controllers 793
Backup Controllers 793
Restrictions for Configuring Backup Controllers 794
Configuring Backup Controllers (GUI) 794
Configuring Backup Controllers (CLI) 795

CHAPTER 111 High Availability 799
Information About High Availability 799
Restrictions for High Availability 803
Configuring High Availability (GUI) 806
Enabling High Availability (CLI) 807
Configuring High Availability Parameters 809
Replacing the Primary Controller in an HA Setup 810

CHAPTER 112 Configuring Failover Priority for Access Points 811
Failover Priority for Access Points 811
Configuring Failover Priority for Access Points (GUI) 811
Configuring Failover Priority for Access Points (CLI) 812
Viewing Failover Priority Settings (CLI) 812

CHAPTER 113 Configuring AP Retransmission Interval and Retry Count 815
AP Retransmission Interval and Retry Count 815
Restrictions for Access Point Retransmission Interval and Retry Count 815
Configuring the AP Retransmission Interval and Retry Count (GUI) 816
Configuring the Access Point Retransmission Interval and Retry Count (CLI) 816

CHAPTER 114 Country Codes 819
Information About Configuring Country Codes 819
Restrictions for Configuring Country Codes 820
Configuring Country Codes (GUI) 820
Configuring Country Codes (CLI) 821

CHAPTER 115 **Optimizing RFID Tracking on Access Points** 825
Optimizing RFID Tracking on Access Points 825
Optimizing RFID Tracking on Access Points (GUI) 825
Optimizing RFID Tracking on Access Points (CLI) 826

CHAPTER 116 **Configuring Probe Request Forwarding** 827
Probe Request Forwarding 827
Configuring Probe Request Forwarding (CLI) 827

CHAPTER 117 **Retrieving the Unique Device Identifier on Controllers and Access Points** 829
Retrieving the Unique Device Identifier on Controllers and Access Points 829
Retrieving the Unique Device Identifier on Controllers and Access Points (GUI) 829
Retrieving the Unique Device Identifier on Controllers and Access Points (CLI) 830

CHAPTER 118 **Performing a Link Test** 831
Link Test 831
Performing a Link Test (GUI) 832
Performing a Link Test (CLI) 832

CHAPTER 119 **Configuring Link Latency** 835
Link Latency 835
Restrictions for Link Latency 836
Configuring Link Latency (GUI) 836
Configuring Link Latency (CLI) 836

CHAPTER 120 **Configuring the TCP MSS** 839
TCP Adjust MSS 839
Configuring TCP Adjust MSS (GUI) 839
Configuring TCP Adjust MSS (CLI) 840

CHAPTER 121 **Configuring Power Over Ethernet** 841
Information About Configuring Power over Ethernet 841

Configuring Power over Ethernet (GUI) 843
Configuring Power over Ethernet (CLI) 844

CHAPTER 122 **Viewing Clients** 847
Viewing Clients (GUI) 847
Viewing Clients (CLI) 848

CHAPTER 123 **Configuring LED States for Access Points** 849
Configuring LED States 849
LED States for Access Points 849
Configuring the LED State for Access Points in a Network Globally (GUI) 849
Configuring the LED State for Access Point in a Network Globally (CLI) 849
Configuring LED State on a Specific Access Point (GUI) 850
Configuring LED State on a Specific Access Point (CLI) 850
Configuring Flashing LEDs 850
Information About Configuring Flashing LEDs 850
Configuring Flashing LEDs (CLI) 850

CHAPTER 124 **Configuring Access Points with Dual-Band Radios** 853
Configuring Access Points with Dual-Band Radios (GUI) 853
Configuring Access Points with Dual-Band Radios (CLI) 853

PART VII **Radio Resource Management** 855

CHAPTER 125 **Configuring RRM** 857
Information about Radio Resource Management 857
Radio Resource Monitoring 858
Transmit Power Control 858
Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings 859
Dynamic Channel Assignment 859
Coverage Hole Detection and Correction 861
Benefits of RRM 861
RRM NDP and RF Grouping 861
Information About Configuring RRM 862

Restrictions for Configuring RRM 862
Configuring the RF Group Mode (GUI) 863
Configuring the RF Group Mode (CLI) 863
Configuring Transmit Power Control (GUI) 864
Configuring Off-Channel Scanning Defer 866
Off-Channel Scanning Deferral 866
Configuring Off-Channel Scanning Defer for WLANs 866
Configuring Off-Channel Scanning Deferral for a WLAN (GUI) 866
Configuring Off Channel Scanning Deferral for a WLAN (CLI) 867
Configuring Dynamic Channel Assignment (GUI) 867
Configuring Coverage Hole Detection (GUI) 870
Configuring RRM Profile Thresholds, Monitoring Channels, and Monitor Intervals (GUI) 871
Configuring RRM (CLI) 873
Viewing RRM Settings (CLI) 877
Debug RRM Issues (CLI) 877

CHAPTER 126 **Configuring RRM Neighbor Discovery Packets** 879
RRM NDP and RF Grouping 879
Configuring RRM NDP (CLI) 880

CHAPTER 127 **Configuring RF Groups** 881
Information About RF Groups 881
RF Group Leader 882
RF Group Name 883
Controllers and APs in RF Groups 883
Configuring RF Groups 884
Configuring an RF Group Name (GUI) 884
Configuring an RF Group Name (CLI) 884
Viewing the RF Group Status 885
Viewing the RF Group Status (GUI) 885
Viewing the RF Group Status (CLI) 885
Configuring Rogue Access Point Detection in RF Groups 886
Rogue Access Point Detection in RF Groups 886
Configuring Rogue Access Point Detection in RF Groups 886

Enabling Rogue Access Point Detection in RF Groups (GUI) 886
Configuring Rogue Access Point Detection in RF Groups (CLI) 887

CHAPTER 128 **Overriding RRM** 889
Overriding RRM 889
Prerequisites for Overriding RRM 889
Statically Assigning Channel and Transmit Power Settings to Access Point Radios 890
Statically Assigning Channel and Transmit Power Settings (GUI) 890
Statically Assigning Channel and Transmit Power Settings (CLI) 891
Disabling Dynamic Channel and Power Assignment Globally for a Cisco Wireless LAN Controller 894
Disabling Dynamic Channel and Power Assignment (GUI) 894
Disabling Dynamic Channel and Power Assignment (CLI) 895

CHAPTER 129 **Configuring CCX Radio Management Features** 897
CCX Radio Management 897
Radio Measurement Requests 897
Location Calibration 898
Configuring CCX Radio Management 898
Configuring CCX Radio Management (GUI) 898
Configuring CCX Radio Management (CLI) 899
Viewing CCX Radio Management Information (CLI) 899
Debugging CCX Radio Management Issues (CLI) 900

PART VIII **Cisco CleanAir** 903

CHAPTER 130 **Information About CleanAir** 905
CleanAir 905
Role of the Cisco Wireless LAN Controller in a Cisco CleanAir System 906
Interference Types that Cisco CleanAir Can Detect 906
Persistent Devices 907
Persistent Devices Detection 907
Persistent Devices Propagation 907
Detecting Interferers by an Access Point 908

CHAPTER 131 **Prerequisites and Restrictions for CleanAir** 909

Prerequisites for CleanAir 909

Restrictions for CleanAir 910

CHAPTER 132 **Cisco CleanAir** 913

Configuring Cisco CleanAir on the Controller 913

Configuring Cisco CleanAir on Cisco WLC (GUI) 913

Configuring Cisco CleanAir on Cisco WLC (CLI) 915

Configuring Cisco CleanAir on an Access Point 919

Configuring Cisco CleanAir on an Access Point (GUI) 919

Configuring Cisco CleanAir on an Access Point (CLI) 920

CHAPTER 133 **Monitoring the Interference Devices** 921

Prerequisites for Monitoring the Interference Devices 921

Monitoring the Interference Device (GUI) 921

Monitoring the Interference Device (CLI) 923

Detecting Interferers by an Access Point 923

Detecting Interferers by Device Type 923

Detecting Persistent Sources of Interference 925

Monitoring Persistent Devices (GUI) 925

Monitoring Persistent Devices (CLI) 925

Monitoring the Air Quality of Radio Bands 926

Monitoring the Air Quality of Radio Bands (GUI) 926

Monitoring the Air Quality of Radio Bands (CLI) 927

Viewing a Summary of the Air Quality 927

Viewing Air Quality for all Access Points on a Radio Band 927

Viewing Air Quality for an Access Point on a Radio Band (CLI) 927

Monitoring the Worst Air Quality of Radio Bands (GUI) 927

Monitoring the Worst Air Quality of Radio Bands (CLI) 928

Viewing a Summary of the Air Quality (CLI) 928

Viewing the Worst Air Quality Information for all Access Points on a Radio Band (CLI) 928

Viewing the Air Quality for an Access Point on a Radio Band (CLI) 928

Viewing the Air Quality for an Access Point by Device Type (CLI) 928

Detecting Persistent Sources of Interference (CLI) 929

CHAPTER 134 Configuring a Spectrum Expert Connection 931

Spectrum Expert Connection 931

Configuring Spectrum Expert (GUI) 931

PART IX FlexConnect 935

CHAPTER 135 FlexConnect 937

Information About FlexConnect 937

FlexConnect Authentication Process 939

Restrictions on FlexConnect 942

Configuring FlexConnect 944

Configuring the Switch at a Remote Site 944

Configuring the Controller for FlexConnect 945

Configuring the Controller for FlexConnect for a Centrally Switched WLAN Used for Guest Access 946

Configuring the Controller for FlexConnect (GUI) 946

Configuring the Controller for FlexConnect (CLI) 948

Configuring an Access Point for FlexConnect 950

Configuring an Access Point for FlexConnect (GUI) 950

Configuring an Access Point for FlexConnect (CLI) 952

Configuring an Access Point for Local Authentication on a WLAN (GUI) 954

Configuring an Access Point for Local Authentication on a WLAN (CLI) 954

Connecting Client Devices to WLANs 955

CHAPTER 136 Configuring FlexConnect ACLs 957

FlexConnect Access Control Lists 957

Restrictions for FlexConnect Access Control Lists 957

Configuring FlexConnect Access Control Lists (GUI) 959

Configuring FlexConnect Access Control Lists (CLI) 960

Viewing and Debugging FlexConnect Access Control Lists (CLI) 962

CHAPTER 137 Configuring FlexConnect Groups 963

Information About FlexConnect Groups 963
FlexConnect Groups and Backup RADIUS Servers 964
FlexConnect Groups and CCKM 964
FlexConnect Groups and Opportunistic Key Caching 964
FlexConnect Groups and Local Authentication 965
Configuring FlexConnect Groups 966
Configuring FlexConnect Groups (GUI) 966
Configuring FlexConnect Groups (CLI) 969
Configuring VLAN-ACL Mapping on FlexConnect Groups 971
Configuring VLAN-ACL Mapping on FlexConnect Groups (GUI) 971
Configuring VLAN-ACL Mapping on FlexConnect Groups (CLI) 972
Viewing VLAN-ACL Mappings (CLI) 972
Configuring WLAN-VLAN Mappings on FlexConnect Groups 972
Configuring WLAN-VLAN Mapping on FlexConnect Groups (GUI) 972
Configuring WLAN-VLAN Mapping on FlexConnect Groups (CLI) 973

CHAPTER 138 **Configuring AAA Overrides for FlexConnect** 975
Authentication, Authorization, Accounting Overrides 975
Restrictions on AAA Overrides for FlexConnect 977
Configuring AAA Overrides for FlexConnect on an Access Point (GUI) 979
Configuring VLAN Overrides for FlexConnect on an Access Point (CLI) 979

CHAPTER 139 **FlexConnect AP Image Upgrades** 981
Information About FlexConnect AP Image Upgrades 981
Restrictions on FlexConnect AP Image Upgrades 981
Configuring FlexConnect AP Upgrades (GUI) 982
Configuring FlexConnect AP Upgrades (CLI) 983

PART X **Mobility Groups** 985

CHAPTER 140 **Mobility Groups** 987
Information About Mobility Groups 987
Prerequisites for Configuring Mobility Groups 990
Configuring Mobility Groups (GUI) 992

Configuring Mobility Groups (CLI) 994
Viewing Mobility Group Statistics (GUI) 995
Viewing Mobility Group Statistics (CLI) 997

CHAPTER 141 Viewing Mobility Group Statistics 999
Viewing Mobility Group Statistics (GUI) 999
Viewing Mobility Group Statistics (CLI) 1000

CHAPTER 142 Auto-Anchor Mobility 1003
Information about Auto-Anchor Mobility 1003
Restrictions for Auto-Anchor Mobility 1004
Configuring Auto-Anchor Mobility (GUI) 1005
Configuring Auto-Anchor Mobility (CLI) 1006

CHAPTER 143 Validating WLAN Mobility Security Values 1009
WLAN Mobility Security Values 1009

CHAPTER 144 Using Symmetric Mobility Tunneling 1011
Information About Symmetric Mobility Tunneling 1011
Guidelines and Limitations 1012
Verifying Symmetric Mobility Tunneling (GUI) 1012
Verifying if Symmetric Mobility Tunneling is Enabled (CLI) 1012

CHAPTER 145 Running Mobility Ping Tests 1013
Mobility Ping Tests 1013
Restrictions for Mobility Ping Tests 1013
Running Mobility Ping Tests (CLI) 1014

CHAPTER 146 Configuring Dynamic Anchoring for Clients with Static IP Addresses 1015
Dynamic Anchoring for Clients with Static IP 1015
How Dynamic Anchoring of Static IP Clients Works 1015
Restrictions on Dynamic Anchoring for Clients With Static IP Addresses 1016
Configuring Dynamic Anchoring of Static IP Clients (GUI) 1016

Configuring Dynamic Anchoring of Static IP Clients (CLI) 1017

CHAPTER 147 Configuring Foreign Mappings 1019

Information About Foreign Mappings 1019

Configuring Foreign Controller MAC Mapping (GUI) 1019

Configuring Foreign Controller MAC Mapping (CLI) 1019

CHAPTER 148 Configuring Proxy Mobile IPv6 1021

Proxy Mobile IPv6 1021

Restrictions on Proxy Mobile IPv6 1023

Configuring Proxy Mobile IPv6 (GUI) 1023

Configuring Proxy Mobile IPv6 (CLI) 1025

CHAPTER 149 Configuring New Mobility 1029

Information About New Mobility 1029

Restrictions for New Mobility 1029

Configuring New Mobility (GUI) 1030

Configuring New Mobility (CLI) 1031

Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation. This chapter includes the following sections:

- Audience, on page xlix
- Conventions, on page xlix
- Related Documentation, on page l

Audience

This publication is for experienced network administrators who configure and maintain Cisco wireless controllers and Cisco lightweight access points.

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
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.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string. Otherwise, the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.

Convention	Indication
[]	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.

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 perform an action that could result in equipment damage or loss of data.

Related Documentation

- Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless releases

  http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-release-notes-list.html

- Cisco Wireless Solutions Software Compatibility Matrix

  https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

- Wireless and Mobility home page

  https://www.cisco.com/c/en/us/products/wireless/index.html

- Cisco Wireless Controller Configuration Guides

  http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-installation-and-configuration-guides-list.html

- Cisco Wireless Controller Command References

  http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html

- Cisco Wireless Controller System Message Guides and Trap Logs

  http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-system-message-guides-list.html

- Cisco Wireless Release Technical References

  http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html

- Cisco Wireless Mesh Access Point Design and Deployment Guides

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html

- Cisco Prime Infrastructure

  http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/tsd-products-support-series-home.html

- Cisco Connected Mobile Experiences

  http://www.cisco.com/c/en_in/solutions/enterprise-networks/connected-mobile-experiences/index.html

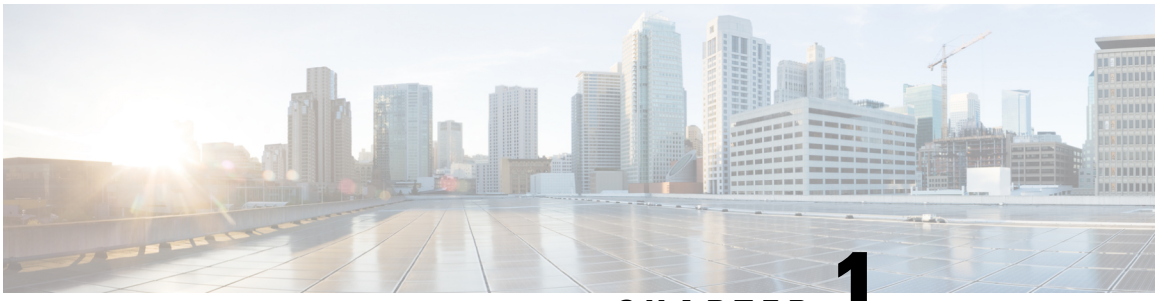
Preface

PART I

System Management

- Cisco Wireless Solution Overview, on page 1
- Getting Started, on page 11
- Managing Licenses, on page 51
- Configuring 802.11 Bands, on page 69
- Configuring 802.11 Parameters, on page 77
- Configuring DHCP Proxy, on page 85
- Configuring SNMP, on page 89
- Configuring Aggressive Load Balancing, on page 95
- Configuring Fast SSID Changing, on page 99
- Configuring 802.3 Bridging, on page 101
- Configuring Multicast, on page 103
- Configuring Client Roaming, on page 123
- Configuring IP-MAC Address Binding, on page 129
- Configuring Quality of Service, on page 131
- Configuring Application Visibility and Control, on page 139
- Configuring Media and EDCA Parameters, on page 145
- Configuring the Cisco Discovery Protocol, on page 163
- Configuring Authentication for the Controller and NTP/SNTP Server, on page 171
- Configuring RFID Tag Tracking, on page 173
- Resetting the Controller to Default Settings, on page 177
- Managing Controller Software and Configurations, on page 179
- Managing User Accounts, on page 207
- Managing Web Authentication, on page 217
- Configuring Wired Guest Access, on page 241

• Troubleshooting, on page 249



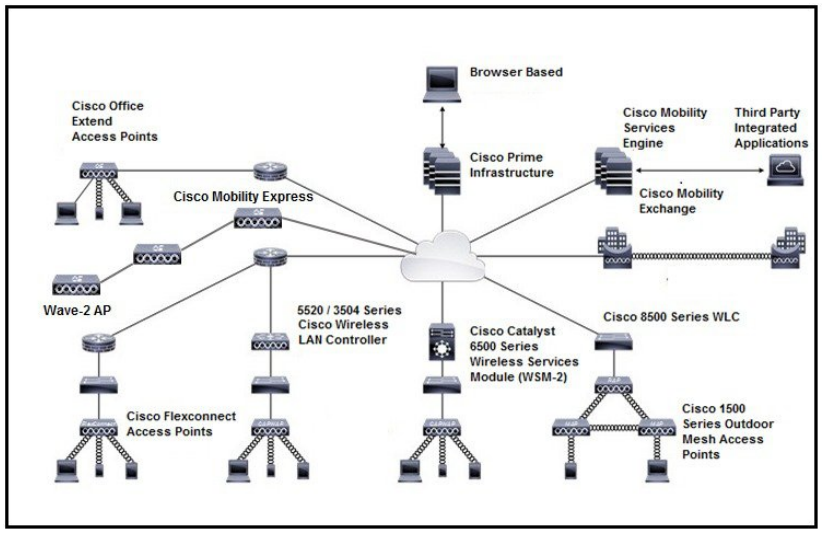
CHAPTER 1

Cisco Wireless Solution Overview

Cisco Wireless Solution is designed to provide 802.11 wireless networking solutions for enterprises and service providers. Cisco Wireless Solution simplifies deploying and managing large-scale wireless LANs and enables a unique best-in-class security infrastructure. The operating system manages all data client, communications, and system administration functions, performs radio resource management (RRM) functions, manages system-wide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework.

This figure shows a sample architecture of a Cisco Wireless Enterprise Network:

Figure 1: Sample Cisco Wireless Enterprise Network Architecture



The interconnected elements that work together to deliver a unified enterprise-class wireless solution include:

- Client devices
- Access points (APs)
- Network unification through Cisco Wireless Controllers (WLCs)
- Network management
- Mobility services

Beginning with a base of client devices, each element adds capabilities as the network needs to evolve and grow, interconnecting with the elements above and below it to create a comprehensive, secure WLAN solution.

- Core Components, on page 2
- Operating System Software, on page 5
- Operating System Security, on page 5
- Layer 2 and Layer 3 Operation, on page 6
- Cisco Wireless Controllers, on page 7
- Cisco Wireless Solution WLANs, on page 8
- File Transfers, on page 9
- Power over Ethernet, on page 9
- Cisco Wireless Controller Memory, on page 9
- Cisco Wireless Controller Failover Protection, on page 9

Core Components

A Cisco Wireless network consists of the following core components:

- Cisco Wireless Controllers—Controllers are enterprise-class high-performance wireless switching platforms that support 802.11a/n/ac and 802.11b/g/n protocols. They operate under control of the operating system, which includes the radio resource management (RRM), creating a Cisco Wireless solution that can automatically adjust to real-time changes in the 802.11 RF environment. Controllers are built around high-performance network and security hardware, resulting in highly reliable 802.11 enterprise networks with unparalleled security.

  The following controllers are supported:

  - Cisco 2504 Wireless Controller
  - Cisco 5508 Wireless Controller
  - Cisco Flex 7510 Wireless Controller
  - Cisco 8510 Wireless Controller
  - Cisco Virtual Wireless Controller
  - Catalyst Wireless Services Module 2 (WiSM2)

- Cisco Aironet Access Points (APs)—Cisco Aironet series wireless access points can be deployed in a distributed or centralized network for a branch office, campus, or large enterprise. For more information about APs, see https://www.cisco.com/c/en/us/products/wireless/access-points/index.html
- Cisco Prime Infrastructure (PI)—Cisco Prime Infrastructure can be used to configure and monitor one or more controllers and associated APs. Cisco PI has tools to facilitate large-system monitoring and control. When you use Cisco PI in your Cisco wireless solution, controllers periodically determine the client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco PI database. For more information about Cisco PI, see http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/tsd-products-support-series-home.html.
- Cisco Connected Mobile Experiences (CMX)—Cisco Connected Mobile Experiences (CMX) acts as a platform to deploy and run Cisco Connected Mobile Experiences (Cisco CMX). Cisco Connected Mobile Experiences (CMX) is delivered in two modes—the physical appliance (box) and the virtual appliance (deployed using VMware vSphere Client) . Using your Cisco wireless network and location intelligence

from Cisco MSE, Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services. For more information about Cisco CMX, see https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/tsd-products-support-series-home.html.

- Cisco DNA Spaces—Cisco DNA Spaces is a multichannel engagement platform that enables you to connect, know, and engage with visitors at their physical business locations. It covers various verticals of business such as retail, manufacturing, hospitality, healthcare, education, financial services, enterprise work spaces, and so on. Cisco DNA Spaces also provides solutions for monitoring and managing the assets in your premises.

  The Cisco DNA Spaces: Connector enables Cisco DNA Spaces to communicate with multiple Cisco Wireless Controller (controller) efficiently by allowing each controller to transmit high intensity client data without missing any client information.

  For information about how to configure Cisco DNA Spaces and the Connector, see https://www.cisco.com/c/en/us/support/wireless/dna-spaces/products-installation-and-configuration-guides-list.html.

For more information about design considerations for enterprise mobility, see the *Enterprise Mobility Design Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide.html

Overview of Cisco Mobility Express

The Cisco Mobility Express wireless network solution comprises of at least one 802.11ac Wave 2 Cisco Aironet Series access point (AP) with an in-built software-based wireless controller managing other APs in the network.

The AP acting as the controller is referred to as the primary AP while the other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as subordinate APs.

In addition to acting as a controllers, the primary AP also operates as an AP to serve clients along with the subordinate APs.

Cisco Mobility Express provides most features of a controllers and has the capability to interface with the following:

- Cisco Prime Infrastructure—For simplified network management, including managing AP groups
- Cisco Identity Services Engine—For advanced policy enforcement
- Connected Mobile Experiences (CMX)—For providing presence analytics and guest access using Connect & Engage

For more information about using Cisco Mobility Express, see the user guide for relevant releases at: https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-installation-and-configuration-guides-list.html

Single-Controller Deployments

A standalone controller can support lightweight access points across multiple floors and buildings simultaneously and support the following features:

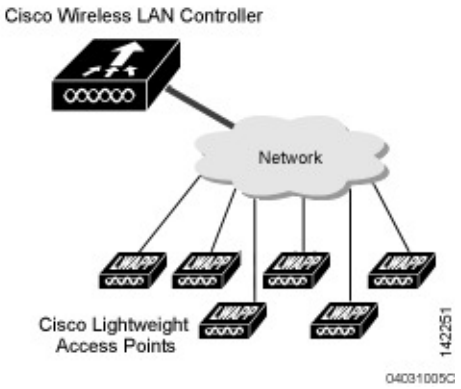
- Autodetecting and autoconfiguring lightweight access points as they are added to the network.

- Full control of lightweight access points.
- Lightweight access points connect to controllers through the network. The network equipment may or may not provide Power over Ethernet (PoE) to the access points.

Some controllers use redundant Gigabit Ethernet connections to bypass single network failures.

Note Some controllers can connect through multiple physical ports to multiple subnets in the network. This feature can be helpful when you want to confine multiple VLANs to separate subnets.

Figure 2: Single-Controller Deployment



This figure shows a typical single-controller deployment.

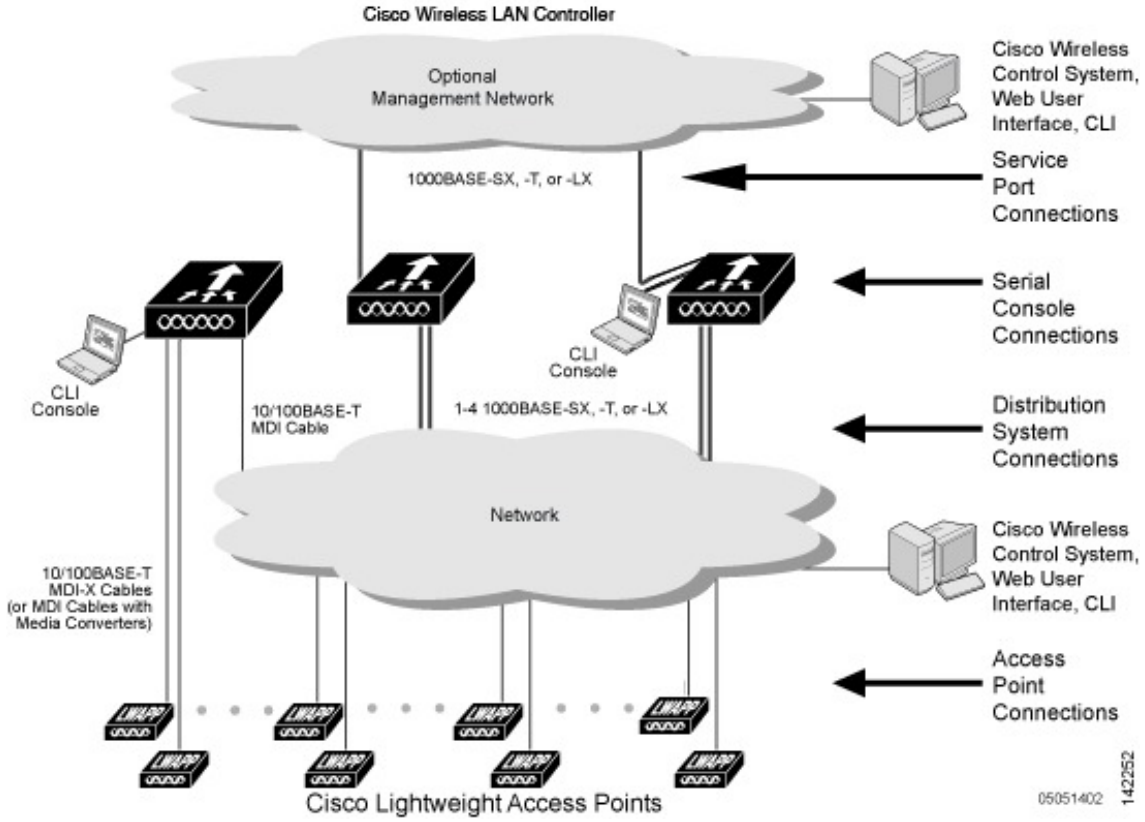
Multiple-Controller Deployments

Each controller can support lightweight access points across multiple floors and buildings simultaneously. However, full functionality of the Cisco wireless LAN solution occurs when it includes multiple controllers. A multiple-controller system has the following additional features:

- Autodetecting and autoconfiguring RF parameters as the controllers are added to the network.
- Same-subnet (Layer 2) roaming and inter-subnet (Layer 3) roaming.
- Automatic access point failover to any redundant controller with a reduced access point load.

Figure 3: Typical Multiple-Controller Deployment

The following figure shows a typical multiple-controller deployment. The figure also shows an optional dedicated management network and the three physical connection types between the network and the controllers.



Operating System Software

The operating system software controls controllers and lightweight access points. It includes full operating system security and radio resource management (RRM) features.

Operating System Security

Operating system security bundles Layer 1, Layer 2, and Layer 3 security components into a simple, Cisco WLAN solution-wide policy manager that creates independent security policies for each of up to 16 wireless LANs.

The 802.11 Static WEP weaknesses can be overcome using the following robust industry-standard security solutions:

- 802.1X dynamic keys with extensible authentication protocol (EAP).
- Wi-Fi protected access (WPA) dynamic keys. The Cisco WLAN solution WPA implementation includes:
  - Temporal key integrity protocol (TKIP) and message integrity code checksum dynamic keys
  - WEP keys, with or without a preshared key passphrase
- RSN with or without a preshared key

- Optional MAC filtering

The WEP problem can be further solved using the following industry-standard Layer 3 security solutions:

- Passthrough VPNs
- Local and RADIUS MAC address filtering
- Local and RADIUS user/password authentication
- Manual and automated disabling to block access to network services. In manual disabling, you block access using client MAC addresses. In automated disabling, which is always active, the operating system software automatically blocks access to network services for a user-defined period of time when a client fails to authenticate for a fixed number of consecutive attempts. This feature can be used to deter brute-force login attacks.

These and other security features use industry-standard authorization and authentication methods to ensure the highest possible security for your business-critical wireless LAN traffic.

Layer 2 and Layer 3 Operation

Lightweight Access Point Protocol (LWAPP) communications between the controller and lightweight access points can be conducted at Layer 2 or Layer 3. Control and Provisioning of Wireless Access Points protocol (CAPWAP) communications between the controller and lightweight access points are conducted at Layer 3. Layer 2 mode does not support CAPWAP.

Note The IPv4 network layer protocol is supported for transport through a CAPWAP or LWAPP controller system. IPv6 (for clients only) and AppleTalk are also supported but only on Cisco 5500 Series Controllers and the Cisco WiSM2. Other Layer 3 protocols (such as IPX, DECnet Phase IV, OSI CLNP, and so on) and Layer 2 (bridged) protocols (such as LAT and NetBeui) are not supported.

Operational Requirements

The requirement for Layer 3 LWAPP communications is that the controller and lightweight access points can be connected through Layer 2 devices on the same subnet or connected through Layer 3 devices across subnets. Another requirement is that the IP addresses of access points should be either statically assigned or dynamically assigned through an external DHCP server.

The requirement for Layer 3 CAPWAP communications is that the controller and lightweight access points can be connected through Layer 2 devices on the same subnet or connected through Layer 3 devices across subnets.

Configuration Requirements

When you are operating the Cisco wireless LAN solution in Layer 2 mode, you must configure a management interface to control your Layer 2 communications.

When you are operating the Cisco wireless LAN solution in Layer 3 mode, you must configure an AP-manager interface to control lightweight access points and a management interface as configured for Layer 2 mode.

Cisco Wireless Controllers

When you are adding lightweight access points to a multiple-Cisco WLC deployment network, it is convenient to have all lightweight access points associate with one primary Cisco WLC on the same subnet. That way, you do not have to log into multiple Cisco WLCs to find out which controller the newly-added lightweight access points associated with.

One Cisco WLC in each subnet can be assigned as the primary Cisco WLC while adding lightweight access points. As long as a primary Cisco WLC is active on the same subnet, all new access points without a primary, secondary, and tertiary controller assigned automatically attempt to associate with the primary Cisco WLC.

You can monitor the primary Cisco WLC using the Cisco Prime Infrastructure and watch as access points associate with the primary Cisco WLC. You can then verify the access point configuration and assign a primary, secondary, and tertiary Cisco WLC to the access point, and reboot the access point so it reassociates with its primary, secondary, or tertiary Cisco WLC.

Note Lightweight access points without a primary, secondary, and tertiary Cisco WLC assigned always search for a primary Cisco WLC first upon reboot. After adding lightweight access points through the primary Cisco WLC, you should assign primary, secondary, and tertiary Cisco WLCs to each access point. We recommend that you disable the primary setting on all Cisco WLCs after initial configuration.

Client Location

When you use Cisco Prime Infrastructure in your Cisco wireless LAN solution, Cisco WLCs periodically determine the client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco Prime Infrastructure database.

Cisco Mobility Services Engine (Cisco MSE) acts as a platform to deploy and run Cisco Connected Mobile Experiences (Cisco CMX). Cisco MSE is delivered in two modes—the physical appliance (box) and the virtual appliance (deployed using VMware vSphere Client) . Using your Cisco wireless network and location intelligence from Cisco MSE, Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services. For more information about Cisco CMX, see

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/tsd-products-support-series-home.html.

Cisco WLC Platforms

Cisco WLCs are enterprise-class high-performance wireless switching platforms that support 802.11a/n/ac and 802.11b/g/n protocols. They operate under control of the operating system, which includes the radio resource management (RRM), creating a Cisco Wireless solution that can automatically adjust to real-time changes in the 802.11 RF environment. Cisco WLCs are built around high-performance network and security hardware, resulting in highly reliable 802.11 enterprise networks with unparalleled security.

The following Cisco WLCs are supported:

- Cisco 2504 Wireless Controller
- Cisco 5508 Wireless Controller
- Cisco Flex 7510 Wireless Controller

- Cisco 8510 Wireless Controller
- Cisco Virtual Wireless Controller
- Catalyst Wireless Services Module 2 (WiSM2)

Client Location

When you use Cisco Prime Infrastructure in your Cisco wireless LAN solution, controllers periodically determine the client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco Prime Infrastructure database.

Cisco WLC Platforms

Cisco WLCs are enterprise-class high-performance wireless switching platforms that support 802.11a/n/ac and 802.11b/g/n protocols. They operate under control of the operating system, which includes the radio resource management (RRM), creating a Cisco Wireless solution that can automatically adjust to real-time changes in the 802.11 RF environment. Cisco WLCs are built around high-performance network and security hardware, resulting in highly reliable 802.11 enterprise networks with unparalleled security.

The following Cisco WLCs are supported:

- Cisco 2504 Wireless Controller
- Cisco 5508 Wireless Controller
- Cisco Flex 7510 Wireless Controller
- Cisco 8510 Wireless Controller
- Cisco Virtual Wireless Controller
- Catalyst Wireless Services Module 2 (WiSM2)

Cisco Wireless Solution WLANs

The Cisco Wireless solution can control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID and can be assigned with unique security policies. The lightweight access points broadcast all active Cisco Wireless solution WLAN SSIDs and enforce the policies defined for each WLAN.

Note We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers operate with optimum performance and ease of management.

If management over wireless is enabled across the Cisco Wireless solution, you can manage the system across the enabled WLAN using CLI and Telnet, HTTP/HTTPS, and SNMP.

File Transfers

You can upload and download operating system code, configuration, and certificate files to and from the controller using the GUI, CLI, or Cisco Prime Infrastructure.

Power over Ethernet

Lightweight access points can receive power through their Ethernet cables from 802.3af-compatible Power over Ethernet (PoE) devices, which can reduce the cost of discrete power supplies, additional wiring, conduits, outlets, and installation time. The 802.11ac radio on the 3600 series access points have to depend on 803.at-compatible PoE devices because the 803.af power source is not sufficient. PoE frees you from having to mount lightweight access points or other powered equipment near AC outlets, which provides greater flexibility in positioning the access points for maximum coverage.

When you are using PoE, you run a single CAT-5 cable from each lightweight access point to PoE-equipped network elements, such as a PoE power hub or a Cisco WLAN solution single-line PoE injector. When the PoE equipment determines that the lightweight access point is PoE-enabled, it sends 48 VDC over the unused pairs in the Ethernet cable to power the access point.

The PoE cable length is limited by the 100BASE-T or 10BASE-T specification to 100 m or 200 m, respectively.

Cisco Wireless Controller Memory

The controller contains two kinds of memory: volatile RAM, which holds the current, active controller configuration, and NVRAM (nonvolatile RAM), which holds the reboot configuration. When you are configuring the operating system in the controller, you are modifying volatile RAM; you must save the configuration from the volatile RAM to the NVRAM to ensure that the controller reboots in the current configuration.

Knowing which memory you are modifying is important when you are doing the following tasks:

- Using the configuration wizard
- Clearing the controller configuration
- Saving configurations
- Resetting the controller
- Logging out of the CLI

Cisco Wireless Controller Failover Protection

During installation, we recommend that you connect all lightweight access points to a dedicated controller, and configure each lightweight access point for final operation. This step configures each lightweight access point for a primary, secondary, and tertiary controller and allows it to store the configured mobility group information.

During the failover recovery, the following tasks are performed:

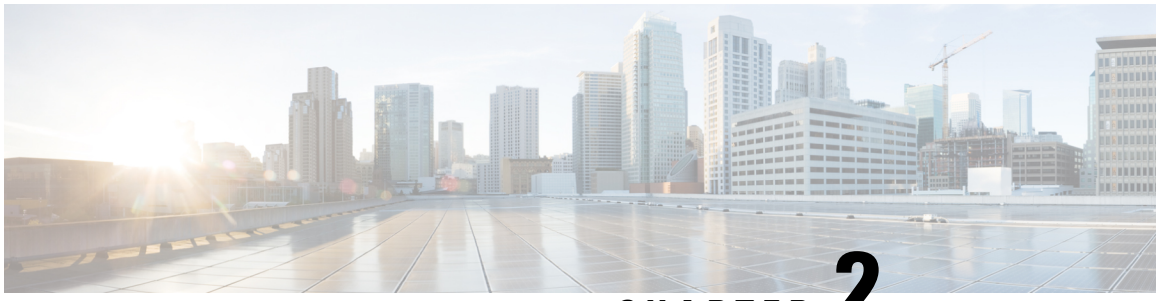
- The configured access point attempts to contact the primary, secondary, and tertiary controllers, and then attempts to contact the IP addresses of the other controllers in the mobility group.
- DNS is resolved with the controller IP address.
- DHCP servers get the controller IP addresses (vendor-specific option 43 in DHCP offer).

In multiple-controller deployments, if one controller fails, the access points perform the following tasks:

- If the lightweight access point has a primary, secondary, and tertiary controller assigned, it attempts to associate with that controller.
- If the access point has no primary, secondary, or tertiary controllers assigned or if its primary, secondary, or tertiary controllers are unavailable, it attempts to associate with a primary controller.
- If the access point finds no primary controller, it attempts to contact stored mobility group members by the IP address.
- If the mobility group members are available, and if the lightweight access point has no primary, secondary, and tertiary controllers assigned and there is no primary controller active, it attempts to associate with the least-loaded controller to respond to its discovery messages.

When controllers are deployed, if one controller fails, active access point client sessions are momentarily dropped while the dropped access point associates with another controller, allowing the client device to immediately reassociate and reauthenticate.

To know more about high availability, see http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107250-ha-wlc.html.



CHAPTER 2

Getting Started

- Configuring the Controller Using the Configuration Wizard, on page 11
- Connecting the Console Port of the Controller, on page 11
- Configuring the Controller (GUI), on page 12
- Configuring the Controller—Using the CLI Configuration Wizard, on page 23
- Using the Controller GUI, on page 25
- Loading an Externally Generated SSL Certificate, on page 29
- Loading an Externally Generated SSL Certificate, on page 29
- Loading an SSL Certificate (GUI), on page 30
- Loading an SSL Certificate (CLI), on page 30
- Using the Controller CLI, on page 31
- Using the AutoInstall Feature for Controllers Without a Configuration, on page 35
- Information About the AutoInstall Feature, on page 36
- Restrictions on AutoInstall, on page 36
- Managing the Controller System Date and Time, on page 39
- Telnet and Secure Shell Sessions, on page 44
- Managing the Controller Wirelessly, on page 49

Configuring the Controller Using the Configuration Wizard

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

Connecting the Console Port of the Controller

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

Note On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller's USB console port and the other end of the cable into the PC's USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

Step 1 Connect one end of a null-modem serial cable to the controller's console port and the other end to your PC's serial port.

Step 2 Start the PC's VT-100 terminal emulation program.

Step 3 Configure the terminal emulation program for these parameters:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

Step 4 Plug the AC power cord into the controller and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet.Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self test verification) and basic configuration.

If the controller passes the power-on self test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.

Configuring the Controller (GUI)

Step 1 Connect your PC to the service port and configure it to use the same subnet as the controller.

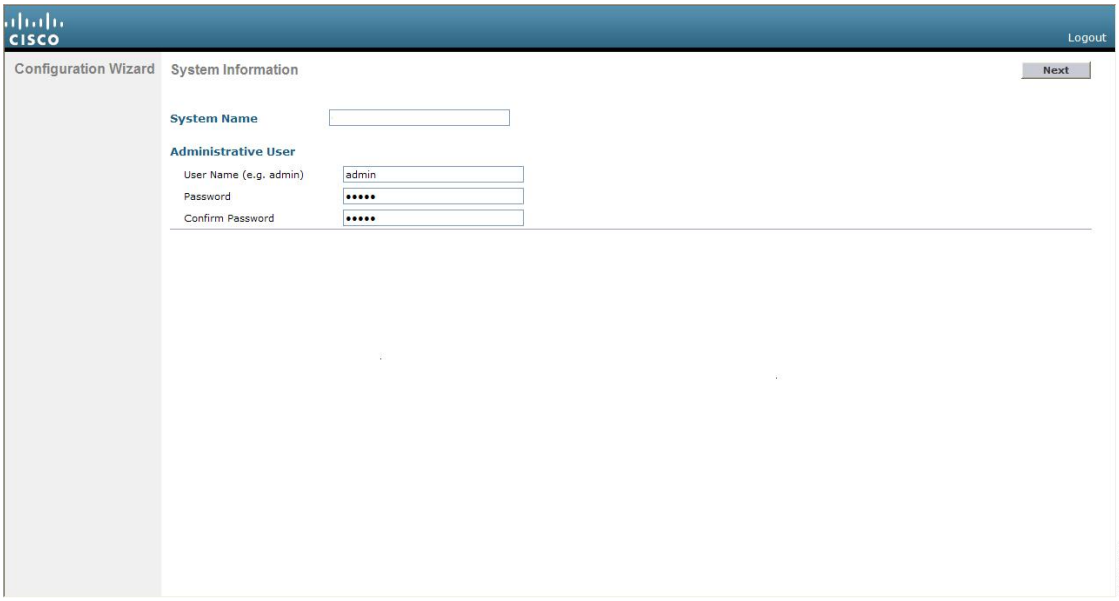
Note In case of Cisco 2504 Wireless Controller, connect your PC to the port 2 on the controller and configure to use the same subnet.

Step 2 Browse to http://192.168.1.1. The configuration wizard appears.

Note You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled. The default IP address to connect to the service port interface is 192.168.1.1.

Note For the initial GUI Configuration Wizard only, you cannot access the controller using IPv6 address.

Figure 4: Configuration Wizard — System Information Page



Step 3 In the **System Name** box, enter the name that you want to assign to this controller. You can enter up to 31 ASCII characters.

Step 4 In the **User Name** box, enter the administrative username to be assigned to this controller. You can enter up to 24 ASCII characters. The default username is *admin*.

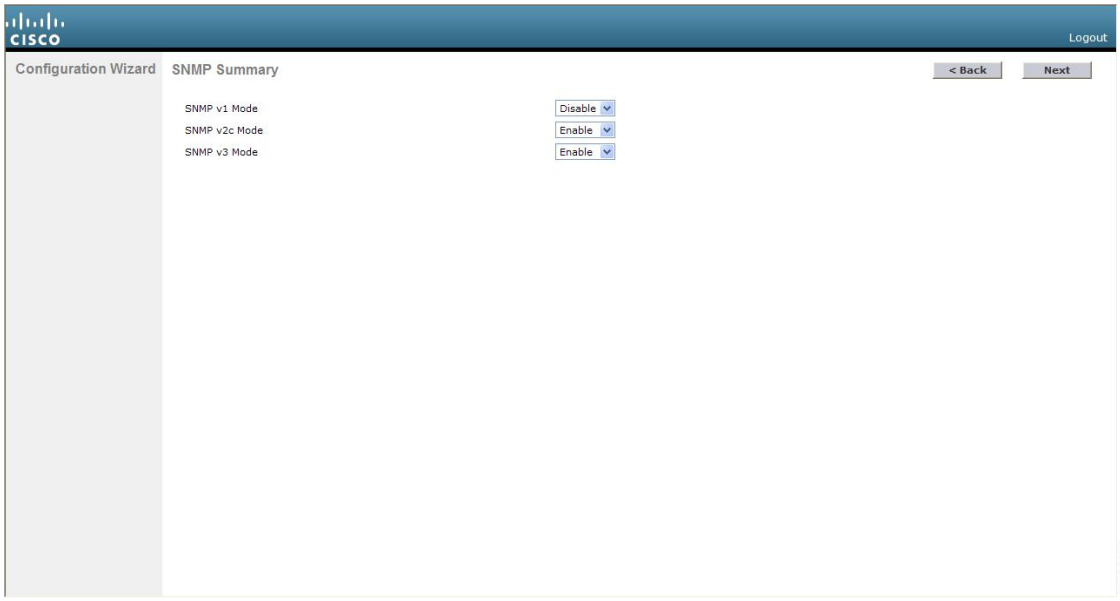
Step 5 In the **Password** and **Confirm Password** boxes, enter the administrative password to be assigned to this controller. You can enter up to 24 ASCII characters. The default password is *admin*.

Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 6 Click **Next**. The **SNMP Summary** page is displayed.

Figure 5: Configuration Wizard—SNMP Summary Page



Step 7 If you want to enable Simple Network Management Protocol (SNMP) v1 mode for this controller, choose **Enable** from the **SNMP v1 Mode** drop-down list. Otherwise, leave this parameter set to **Disable**.

Note SNMP manages nodes (servers, workstations, routers, switches, and so on) on an IP network. Currently, there are three versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3.

Step 8 If you want to enable SNMPv2c mode for this controller, leave this parameter set to **Enable**. Otherwise, choose **Disable** from the **SNVP v2c Mode** drop-down list.

Step 9 If you want to enable SNMPv3 mode for this controller, leave this parameter set to **Enable**. Otherwise, choose **Disable** from the **SNVP v3 Mode** drop-down list.

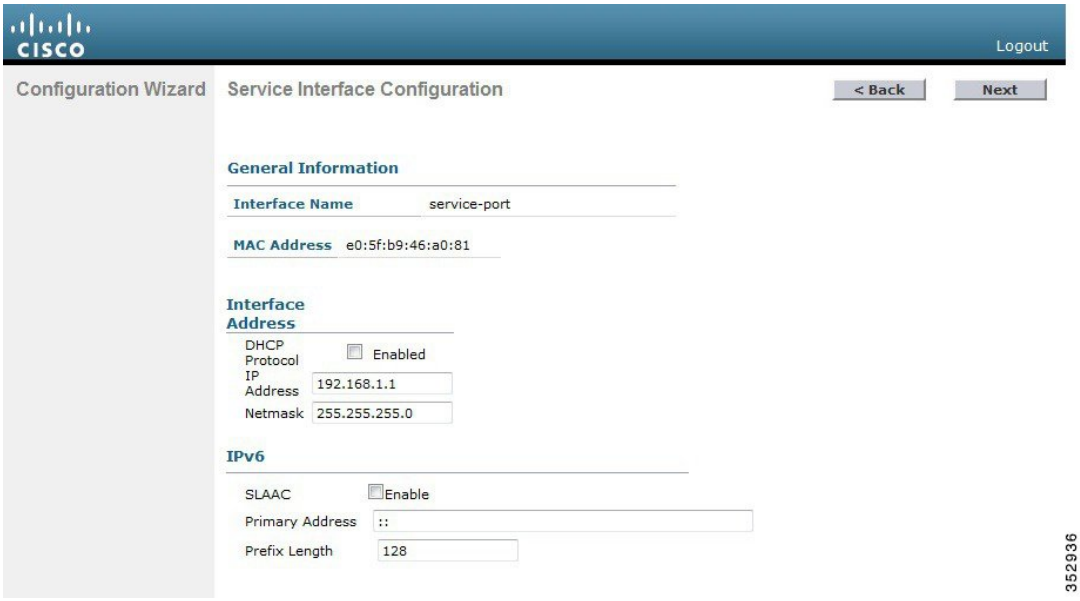
Step 10 Click **Next**.

Step 11 When the following message appears, click **OK**:

```
Default values are present for v1/v2c community strings.
Please make sure to create new v1/v2c community strings once the system comes up.
Please make sure to create new v3 users once the system comes up.
```

The **Service Interface Configuration** page is displayed.

Figure 6: Configuration Wizard-Service Interface Configuration Page



Step 12 If you want the controller's service-port interface to obtain an IP address from a DHCP server, check the **DHCP Protocol Enabled** check box. If you do not want to use the service port or if you want to assign a static IP address to the service port, leave the check box unchecked.

Note The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

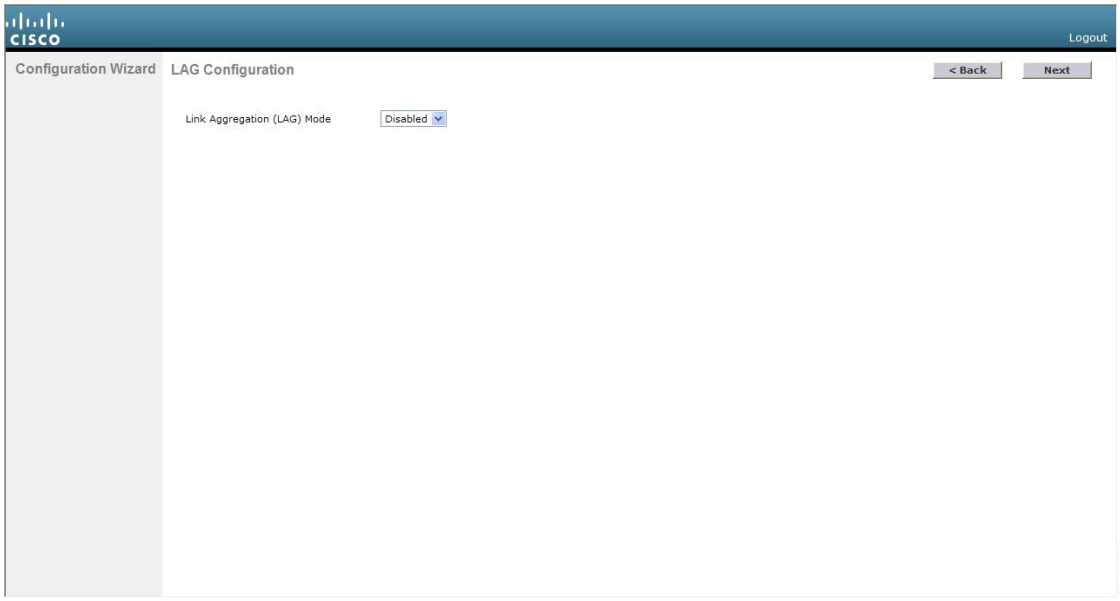
Step 13 Perform one of the following:

- If you enabled DHCP, clear out any entries in the IP Address and Netmask text boxes, leaving them blank.
- If you disabled DHCP, enter the static IP address and netmask for the service port in the IP Address and Netmask text boxes.

Step 14 Click **Next**.

The **LAG Configuration** page is displayed.

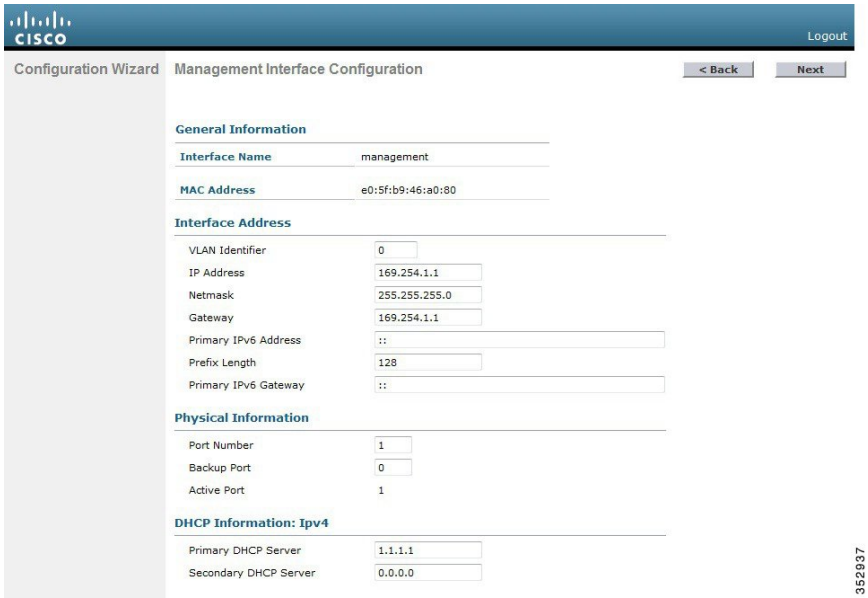
Figure 7: Configuration Wizard—LAG Configuration Page



Step 15 To enable link aggregation (LAG), choose **Enabled** from the Link Aggregation (LAG) Mode drop-down list. To disable LAG, leave this text box set to **Disabled**.

Step 16 Click **Next**.

The **Management Interface Configuration** page is displayed.



Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

Step 17 In the **VLAN Identifier** box, enter the VLAN identifier of the management interface (either a valid VLAN identifier or **0** for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Step 18 In the **IP Address** box, enter the IP address of the management interface.

Step 19 In the **Netmask** box, enter the IP address of the management interface netmask.

Step 20 In the **Gateway** box, enter the IP address of the default gateway.

Step 21 In the **Port Number** box, enter the number of the port assigned to the management interface. Each interface is mapped to at least one primary port.

Step 22 In the **Backup Port** box, enter the number of the backup port assigned to the management interface. If the primary port for the management interface fails, the interface automatically moves to the backup port.

Step 23 In the **Primary DHCP Server** box, enter the IP address of the default DHCP server that will supply IP addresses to clients, the controller's management interface, and optionally, the service port interface.

Step 24 In the **Secondary DHCP Server** box, enter the IP address of an optional secondary DHCP server that will supply IP addresses to clients, the controller's management interface, and optionally, the service port interface.

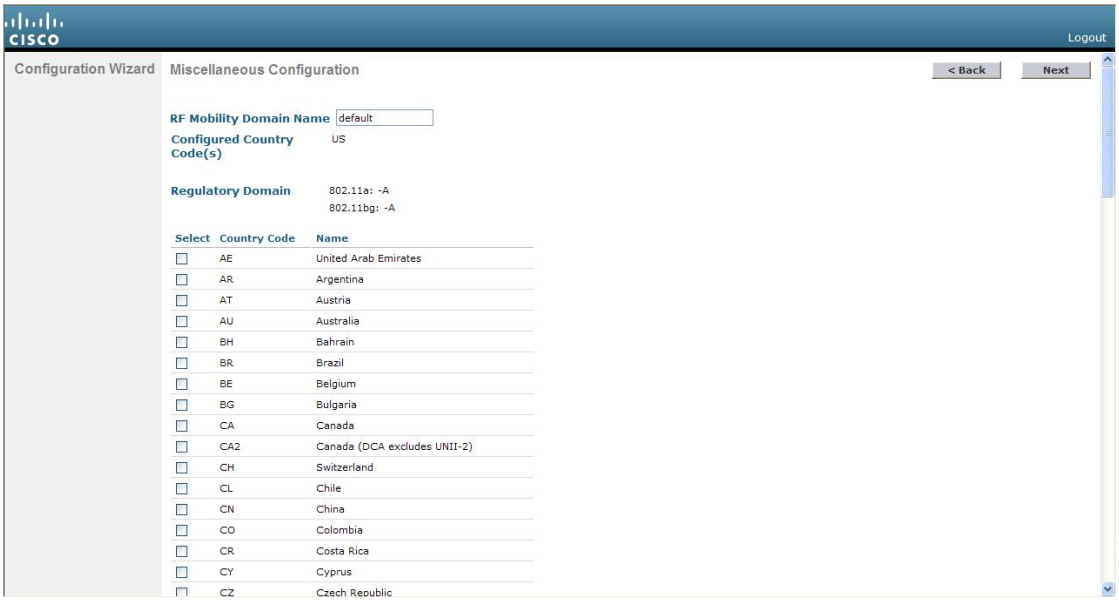
Step 25 Click **Next**. The **AP-Manager Interface Configuration** page is displayed.

Note This screen does not appear for Cisco 5508 WLCs because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 26 In the **IP Address** box, enter the IP address of the AP-manager interface.

Step 27 Click **Next**. The **Miscellaneous Configuration** page is displayed.

Figure 8: Configuration Wizard—Miscellaneous Configuration Page



Step 28 In the **RF Mobility Domain Name** box, enter the name of the mobility group/RF group to which you want the controller to belong.

Note Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 29 The **Configured Country Code(s)** box shows the code for the country in which the controller will be used. If you want to change the country of operation, check the check box for the desired country.

Note You can choose more than one country code if you want to manage access points in multiple countries from a single controller. After the configuration wizard runs, you must assign each access point joined to the controller to a specific country.

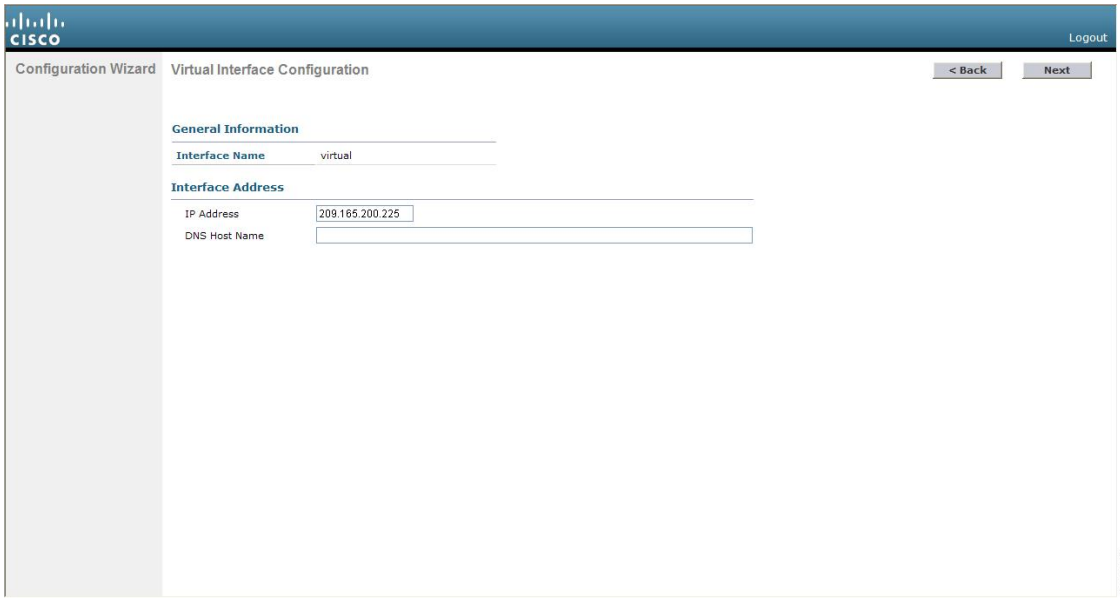
Step 30 Click **Next**.

Step 31 When the following message appears, click **OK**:

```
Warning! To maintain regulatory compliance functionality, the country code
setting may only be modified by a network administrator or qualified IT professional.
Ensure that proper country codes are selected before proceeding.?
```

The **Virtual Interface Configuration** page is displayed.

Figure 9: Configuration Wizard — Virtual Interface Configuration Page



Step 32 In the **IP Address** box, enter the IP address of the controller's virtual interface. You should enter a fictitious, unassigned IP address.

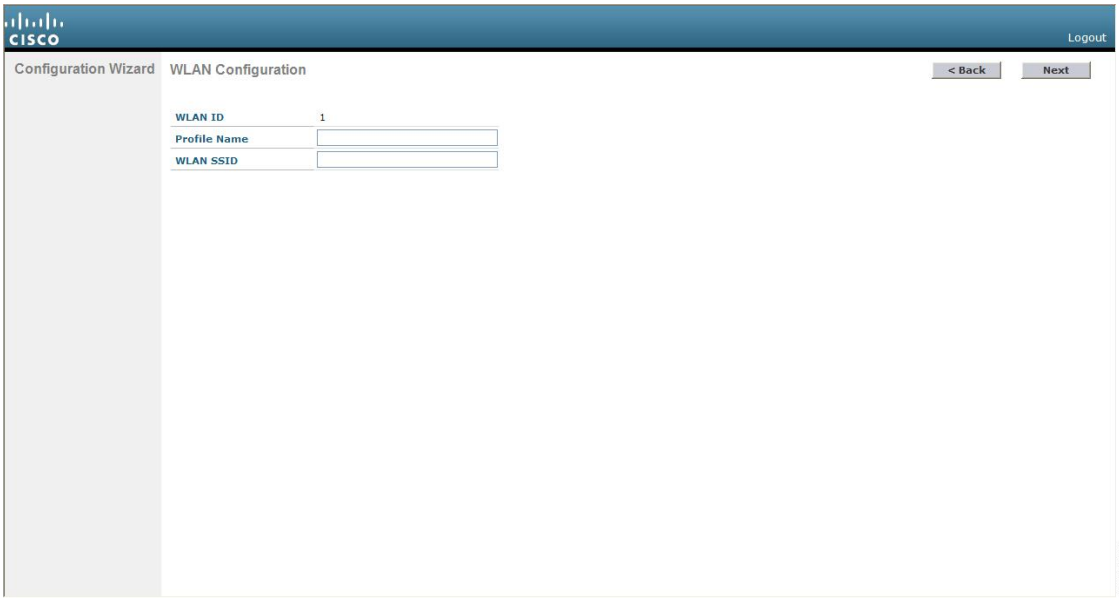
Note The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 33 In the **DNS Host Name** box, enter the name of the Domain Name System (DNS) gateway used to verify the source of certificates when Layer 3 web authorization is enabled.

Note To ensure connectivity and web authentication, the DNS server should always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then the same DNS hostname must be configured on the DNS servers used by the client.

Step 34 Click **Next**. The **WLAN Configuration** page is displayed.

Figure 10: Configuration Wizard — WLAN Configuration Page



Step 35 In the **Profile Name** box, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN.

Step 36 In the **WLAN SSID** box, enter up to 32 alphanumeric characters for the network name, or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

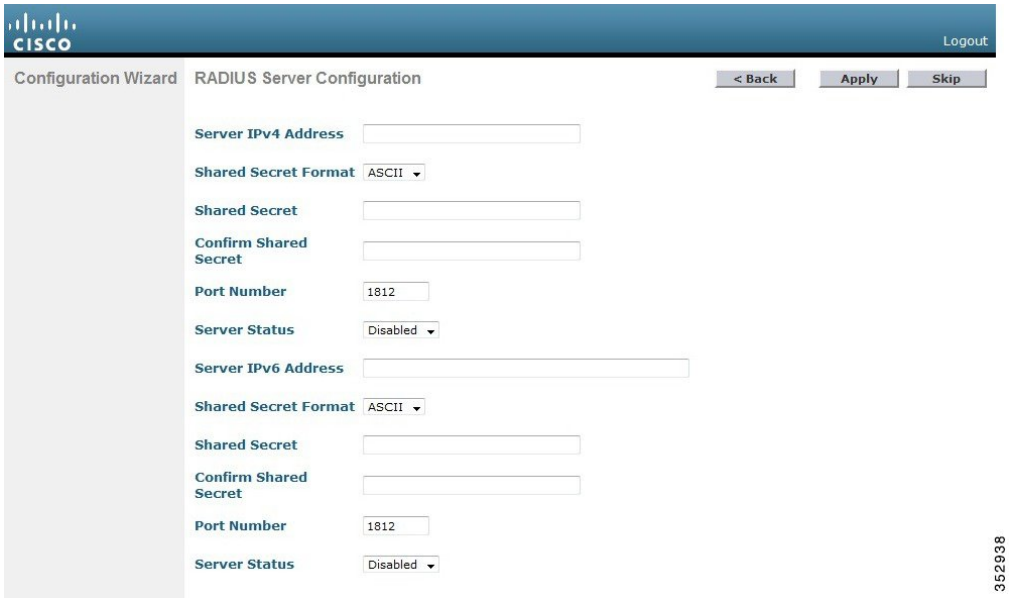
Step 37 Click **Next**.

Step 38 When the following message appears, click **OK**:

```
Default Security applied to WLAN is: [WPA2(AES)][Auth(802.1x)]. You can change
this after the wizard is complete and the system is rebooted.?
```

The **RADIUS Server Configuration** page is displayed.

Figure 11: Configuration Wizard-RADIUS Server Configuration Page



Step 39 In the **Server IP Address** box, enter the IP address of the RADIUS server.

Step 40 From the **Shared Secret Format** drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret.

Note Due to security reasons, the RADIUS shared secret key reverts to ASCII mode even if you have selected HEX as the shared secret format from the Shared Secret Format drop-down list.

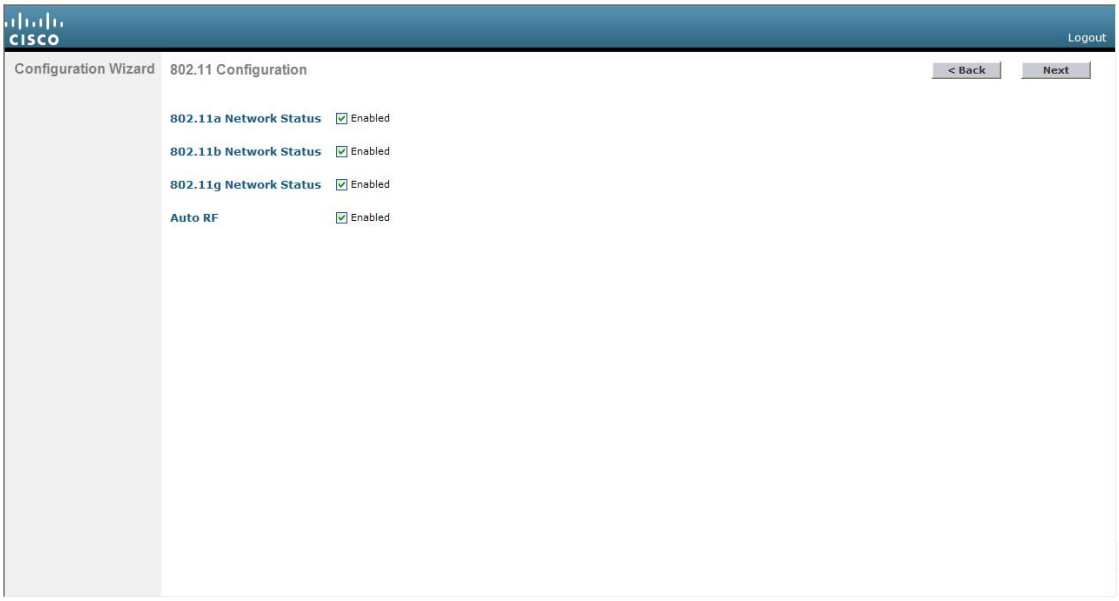
Step 41 In the **Shared Secret** and **Confirm Shared Secret** boxes, enter the secret key used by the RADIUS server.

Step 42 In the **Port Number** box, enter the communication port of the RADIUS server. The default value is 1812.

Step 43 To enable the RADIUS server, choose **Enabled** from the **Server Status** drop-down list. To disable the RADIUS server, leave this box set to **Disabled**.

Step 44 Click **Apply**. The **802.11 Configuration** page is displayed.

Figure 12: Configuration Wizard—802.11 Configuration Page



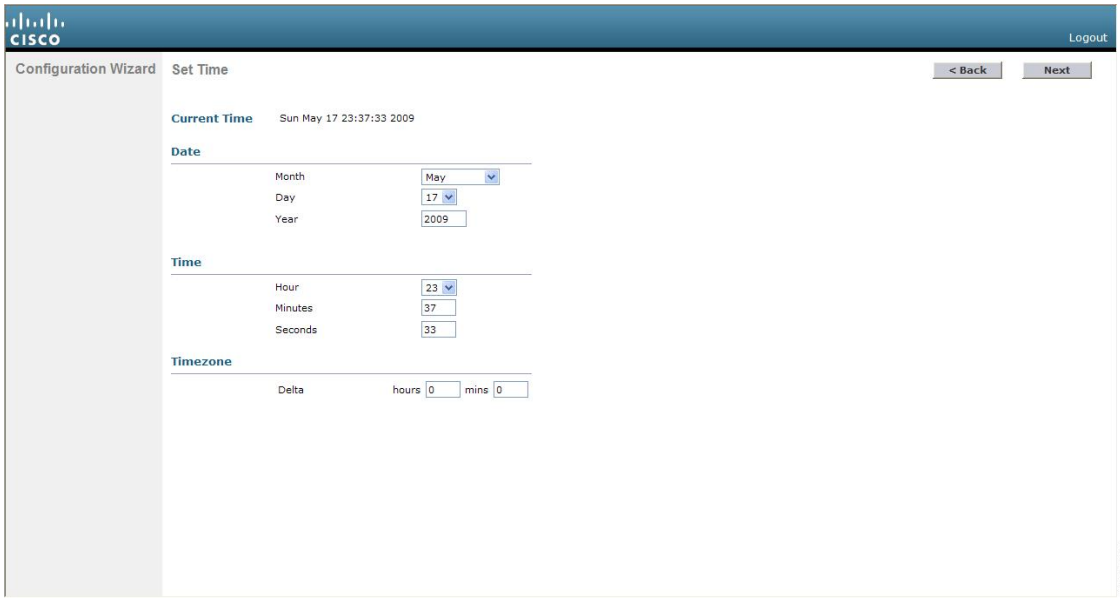
Step 45 To enable the 802.11a, 802.11b, and 802.11g lightweight access point networks, leave the **802.11a Network Status**, **802.11b Network Status**, and **802.11g Network Status** check boxes checked. To disable support for any of these networks, uncheck the check boxes.

Step 46 To enable the controller's radio resource management (RRM) auto-RF feature, leave the **Auto RF** check box selected. To disable support for the auto-RF feature, uncheck this check box.

Note The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 47 Click **Next**. The **Set Time** page is displayed.

Figure 13: Configuration Wizard — Set Time Screen



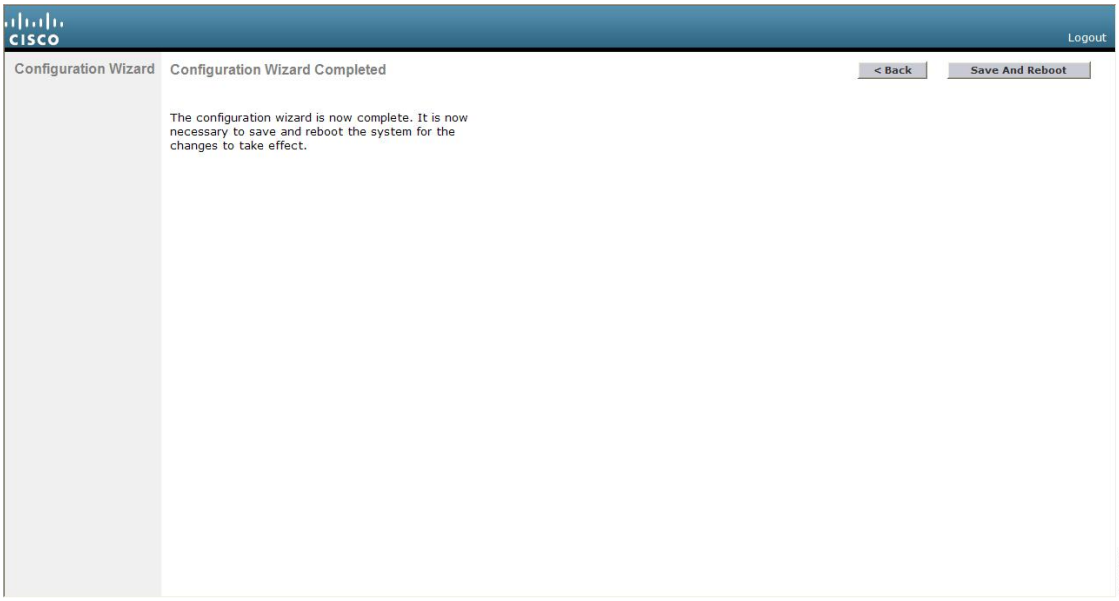
Step 48 To manually configure the system time on your controller, enter the current date in Month/DD/YYYY format and the current time in HH:MM:SS format.

Step 49 To manually set the time zone so that Daylight Saving Time (DST) is not set automatically, enter the local hour difference from Greenwich Mean Time (GMT) in the **Delta Hours** box and the local minute difference from GMT in the **Delta Mins** box.

Note When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/–). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

Step 50 Click **Next**. The **Configuration Wizard Completed** page is displayed.

Figure 14: Configuration Wizard—Configuration Wizard Completed Page



Step 51 Click **Save and Reboot** to save your configuration and reboot the controller.

Step 52 When the following message appears, click **OK**:

```
Configuration will be saved and the controller will be
rebooted. Click ok to confirm.?
```

The controller saves your configuration, reboots, and prompts you to log on.

Configuring the Controller—Using the CLI Configuration Wizard

Before you begin

- The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.
- If you enter an incorrect response, the controller provides you with an appropriate error message, such as “Invalid Response”, and returns you to the wizard prompt.
- Press the **hyphen** key if you ever need to return to the previous command line.

Step 1 When prompted to terminate the AutoInstall process, enter **yes**. If you do not enter **yes**, the AutoInstall process begins after 30 seconds.

Note The AutoInstall feature downloads a configuration file from a TFTP server and then loads the configuration onto the controller automatically.

Step 2 Enter the system name, which is the name that you want to assign to the controller. You can enter up to 31 ASCII characters.

Step 3 Enter the administrative username and password to be assigned to this controller. You can enter up to 24 ASCII characters for each.

Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 4 If you want the controller's service-port interface to obtain an IP address from a DHCP server, enter **DHCP**. If you do not want to use the service port or if you want to assign a static IP address to the service port, enter none.

Note The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

Step 5 If you entered none in *Step 4*, enter the IP address and netmask for the service-port interface on the next two lines.

Step 6 Enable or disable link aggregation (LAG) by choosing yes or NO.

Step 7 Enter the IP address of the management interface.

Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

Step 8 Enter the IP address of the management interface netmask.

Step 9 Enter the IP address of the default router.

Step 10 Enter the VLAN identifier of the management interface (either a valid VLAN identifier or 0 for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Step 11 Enter the IP address of the default DHCP server that will supply IP addresses to clients, the management interface of the controller, and optionally, the service port interface. Enter the IP address of the AP-manager interface.

Note This prompt does not appear for Cisco 5508 WLCs because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 12 Enter the IP address of the controller's virtual interface. You should enter a fictitious unassigned IP address.

Note The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 13 If desired, enter the name of the mobility group/RF group to which you want the controller to belong.

Note Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 14 Enter the network name or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

Step 15 Enter YES to allow clients to assign their own IP address or no to require clients to request an IP address from a DHCP server.

Step 16 To configure a RADIUS server now, enter YES and then enter the IP address, communication port, and secret key of the RADIUS server. Otherwise, enter no. If you enter no, the following message appears: "Warning! The default WLAN security policy requires a RADIUS server. Please see the documentation for more details."

Step 17 Enter the code for the country in which the controller will be used.

Note Enter help to view the list of available country codes.

Note You can enter more than one country code if you want to manage access points in multiple countries from a single controller. To do so, separate the country codes with a comma (for example, US,CA,MX). After the configuration wizard runs, you need to assign each access point joined to the controller to a specific country.

Step 18 Enable or disable the 802.11b, 802.11a, and 802.11g lightweight access point networks by entering **YES** or **no**.

Step 19 Enable or disable the controller's radio resource management (RRM) auto-RF feature by entering **YES** or **no**.

Note The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 20 If you want the controller to receive its time setting from an external Network Time Protocol (NTP) server when it powers up, enter **YES** to configure an NTP server. Otherwise, enter **no**.

Note The controller network module installed in a Cisco Integrated Services Router does not have a battery and cannot save a time setting. Therefore, it must receive a time setting from an external NTP server when it powers up.

Step 21 If you entered **no** in *Step 20* and want to manually configure the system time on your controller now, enter **YES**. If you do not want to configure the system time now, enter **no**.

Step 22 If you entered **YES** in *Step 21*, enter the current date in the MM/DD/YY format and the current time in the HH:MM:SS format.

Step 23 When prompted to verify that the configuration is correct, enter **yes** or **NO**.

The controller saves your configuration when you enter **yes**, reboots, and prompts you to log on.

Using the Controller GUI

A browser-based GUI is built into each controller.

It allows up to five users to simultaneously browse into the controller HTTP or HTTPS (HTTP + SSL) management pages to configure parameters and monitor the operational status for the controller and its associated access points.

For detailed descriptions of the Controller GUI, see the Online Help. To access the online help, click **Help** on the Controller GUI.

- The Cisco WLC GUI is supported on the following web browsers:
  - Microsoft Internet Explorer 10 or a later version (Windows)
  - Mozilla Firefox, Version 32 or a later version (Windows, Mac)
  - Google Chrome, Version 38.x or a later version (Windows, Mac)
  - Apple Safari, Version 7 or a later version (Mac)

Note We recommend that you enable the HTTPS interface and disable the HTTP interface to ensure more robust security.

Restrictions on using Controller GUI

Follow these guidelines when using the controller GUI:

- The controller Web UI is compatible with the following web browsers
  - Microsoft Internet Explorer 11 and later versions
  - Mozilla Firefox 32 and later versions
- To view the Main Dashboard that is introduced in Release 8.1.102.0, you must enable JavaScript on the web browser.

  Note Ensure that the screen resolution is set to 1280x800 or more. Lesser resolutions are not supported.
- You can use either the service port interface or the management interface to access the GUI.
- You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.
- Click **Help** at the top of any page in the GUI to display online help. You might need to disable your browser's pop-up blocker to view the online help.

Logging On to the GUI

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

Step 1 Enter the controller IP address in your browser's address bar. For a secure connection, enter **`https://ip-address`**. For a less secure connection, enter **`https://ip-address`**.

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

The **Summary** page is displayed.

Note The administrative username and password that you created in the configuration wizard are case sensitive.

Logging out of the GUI

Step 1 Click **Logout** in the top right corner of the page.

Step 2 Click **Close** to complete the log out process and prevent unauthorized users from accessing the controllercontroller GUI.

Step 3 When prompted to confirm your decision, click **Yes**.

Enabling Web and Secure Web Modes

This section provides instructions to enable the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.

You can configure web and secure web mode using the controller GUI or CLI.

This section contains the following subsections:

Enabling Web and Secure Web Modes (GUI)

Step 1 Choose **Management** > **HTTP-HTTPS**.

The **HTTP-HTTPS Configuration** page is displayed.

Step 2 To enable web mode, which allows users to access the controller GUI using "http://*ip-address*," choose **Enabled** from the **HTTP Access** drop-down list. Otherwise, choose **Disabled**. The default value is Disabled. Web mode is not a secure connection.

Step 3 To enable secure web mode, which allows users to access the controller GUI using "https://*ip-address*," choose **Enabled** from the **HTTPS Access** drop-down list. Otherwise, choose **Disabled**. The default value is Enabled. Secure web mode is a secure connection.

Step 4 In the **Web Session Timeout** field, enter the amount of time, in minutes, before the web session times out due to inactivity. You can enter a value between 10 and 160 minutes (inclusive). The default value is 30 minutes.

Step 5 Click **Apply**.

Step 6 If you enabled secure web mode in Step 3, the controller generates a local web administration SSL certificate and automatically applies it to the GUI. The details of the current certificate appear in the middle of the **HTTP-HTTPS Configuration** page.

Note If desired, you can delete the current certificate by clicking **Delete Certificate** and have the controller generate a new certificate by clicking **Regenerate Certificate**. You have the option to use server side SSL certificate that you can download to controller. If you are using HTTPS, you can use SSC or MIC certificates.

Step 7 Click **Save Configuration**.

Enabling Web and Secure Web Modes (CLI)

Step 1 Enable or disable web mode by entering this command:

config network webmode {**enable** | **disable**}

This command allows users to access the controller GUI using "http://*ip-address*." The default value is disabled. Web mode is not a secure connection.

Step 2 Enable or disable secure web mode by entering this command:

config network secureweb {**enable** | **disable**}

This command allows users to access the controller GUI using "https://*ip-address*." The default value is enabled. Secure web mode is a secure connection.

Step 3 Enable or disable secure web mode with increased security by entering this command:

config network secureweb cipher-option high {**enable** | **disable**}

This command allows users to access the controller GUI using "https://*ip-address*" but only from browsers that support 128-bit (or larger) ciphers. The default value is disabled.

When high ciphers is enabled, SHA1, SHA256, SHA384 keys continue to be listed and TLSv1.0 is disabled. This is applicable to webauth and webadmin but not for NMSP.

Step 4 Enable or disable SSLv2 for web administration by entering this command:

config network secureweb cipher-option sslv2 {**enable** | **disable**}

If you disable SSLv2, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is disabled.

Step 5 Enable 256 bit ciphers for a SSH session by entering this command:

config network ssh cipher-option high {**enable** | **disable**}

Step 6 [Optional] Disable telnet by entering this command:

config network telnet{**enable** | **disable**}

Step 7 Enable or disable preference for RC4-SHA (Rivest Cipher 4-Secure Hash Algorithm) cipher suites (over CBC cipher suites) for web authentication and web administration by entering this command:

config network secureweb cipher-option rc4-preference {**enable** | **disable**}

Step 8 Verify that the controller has generated a certificate by entering this command:

show certificate summary

Information similar to the following appears:

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

Step 9 (Optional) Generate a new certificate by entering this command:

config certificate generate webadmin

After a few seconds, the controller verifies that the certificate has been generated.

Step 10 Save the SSL certificate, key, and secure web password to nonvolatile RAM (NVRAM) so that your changes are retained across reboots by entering this command:

save config

Step 11 Reboot the controller by entering this command:

reset system

Loading an Externally Generated SSL Certificate

This section describes how to load an externally generated SSL certificate.

Loading an Externally Generated SSL Certificate

You can use a supported transfer method such as TFTP server to download an externally generated SSL certificate to the controller. Follow these guidelines for using TFTP:

- If you load the certificate through the service port, the TFTP server must be on the same subnet as the controller because the service port is not routable, or you must create static routes on the controller. Also, if you load the certificate through the distribution system network port, the TFTP server can be on any subnet.
- A third-party TFTP server cannot run on the same PC as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

Note Chained certificates are supported for web authentication and management certificate.

CSR compliance with RFC-5280

With all parameters in CSR aligned with RFC-5280, there are some restrictions as follows:

- *emailAddress* in CSR can only be 128 characters long.

- If the CSR is generated using the CLI, the maximum number of characters (of all input combined for CSR) is limited to 500 including **config certificate generate csr-*****.

Related Documentation

Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC—https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html

Loading an SSL Certificate (GUI)

Step 1 Choose **Security** > **Web Auth** > **Certificate**.

Step 2 On the **Web Authentication Certificate** page, check the **Download SSL Certificate** check box.

Note On the controller GUI, only TFTP transfer mode is used. You can use other methods such as FTP, and so on, on the controller CLI.

Step 3 In the **Server IP Address** field, enter the IP address of the TFTP server.

Step 4 In the **Maximum Retries** field, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 5 In the **Timeout** field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 6 In the **Certificate File Path** field, enter the directory path of the certificate.

Step 7 In the **Certificate File Name** field, enter the name of the certificate (webadmincert_name.pem).

Step 8 (Optional) In the **Certificate Password** field, enter a password to encrypt the certificate.

Step 9 Save the configuration.

Step 10 Choose **Commands** > **Reboot** > **Reboot** > **Save and Reboot** to reboot the controller for your changes to take effect,

Loading an SSL Certificate (CLI)

The procedure described in this section is similar for both webauthcert and webadmincert installation, with the difference being in the download of the datatype.

Step 1 Use a password to encrypt the HTTPS certificate in a .PEM-encoded file. The PEM-encoded file is called a web administration certificate file (`webadmincert_name.pem`).

Step 2 Move the `webadmincert_name.pem` file to the default directory on your TFTP server.

Step 3 To view the current download settings, enter this command and answer **n** to the prompt:

transfer download start

Information similar to the following appears:

```
Mode..................................... TFTP
Data Type................................ Admin Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
```

```
TFTP Path..................................... <directory path>
TFTP Filename.................................
Are you sure you want to start? (y/n) n
Transfer Canceled
```

Step 4 Use these commands to change the download settings:

transfer download mode *tftp*

transfer download datatype *webadmincert*

transfer download serverip *TFTP_server IP_address*

transfer download path *absolute_TFTP_server_path_to_the_update_file*

transfer download filename *webadmincert_name.pem*

Step 5 To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, enter this command:

transfer download certpassword *private_key_password*

Step 6 To confirm the current download settings and start the certificate and key download, enter this command and answer **y** to the prompt:

transfer download start

Information similar to the following appears:

```
Mode.......................................... TFTP
Data Type..................................... Site Cert
TFTP Server IP................................ xxx.xxx.xxx.xxx
TFTP Path..................................... directory path
TFTP Filename................................. webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

Step 7 To save the SSL certificate, key, and secure web password to NVRAM so that your changes are retained across reboots, enter this command:

save config

Step 8 To reboot the controller, enter this command:

reset system

Using the Controller CLI

A Cisco UWN solution command-line interface (CLI) is built into each controller. The CLI enables you to use a VT-100 terminal emulation program to locally or remotely configure, monitor, and control individual controllers and its associated lightweight access points. The CLI is a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulation programs to access the controller.

Note For more information about specific commands, see the *Cisco Wireless Controller Command Reference* for relevant releases at:

https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html

Logging on to the Controller CLI

You can access the controller CLI using either of the following methods:

- A direct serial connection to the controller console port
- A remote session over the network using Telnet or SSH through the preconfigured service port or the distribution system ports

For more information about ports and console connection options on controllers, see the relevant controller platform's installation guide.

Using a Serial or USB Console Connection on Cisco WLC

On Cisco 5508 WLCs, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller's USB console port and the other end of the cable into the PC's USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

See the Telnet and Secure Shell Sessions section for information on enabling Telnet sessions.

Using a Local Serial Connection

Before you begin

You need these items to connect to the serial port:

- A computer that is running a terminal emulation program such as Putty, SecureCRT, or similar
- A standard Cisco console serial cable with an RJ45 connector

To log on to the controller CLI through the serial port, follow these steps:

Step 1 Connect console cable—Connect one end of a standard Cisco console serial cable with an RJ45 connector to the controller's console port and the other end to your PC's serial port.

Step 2 Configure terminal emulator program with default settings:

- 9600 baud
- 8 data bits
- 1 stop bit

- No parity
- No hardware flow control

Note The controller serial port is set for a 9600 baud rate and a short timeout. If you would like to change either of these values, run the **config serial baudrate** *value* and **config serial timeout** *value* to make your changes. If you set the serial timeout value to 0, serial sessions never time out.

If you change the console speed to a value other than 9600, the console speed used by controller will be 9600 during boot and will only change upon the completion of boot process. Therefore, we recommend that you do not change the console speed, except as a temporary measure on an as-needed basis.

Step 3 Log on to the CLI—When prompted, enter a valid username and password to log on to the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note The default username is admin, and the default password is admin.

The CLI displays the root level system prompt:

(Cisco Controller) >

Note The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

Using a Remote Telnet or SSH Connection

Before you begin

You need these items to connect to a controller remotely:

- A PC with network connectivity to either the management IP address, the service port address, or if management is enabled on a dynamic interface of the controller in question
- The IP address of the controller
- A VT-100 terminal emulation program or a DOS shell for the Telnet session

Note By default, controllers block Telnet sessions. You must use a local connection to the serial port to enable Telnet sessions.

Note The **aes-cbc ciphers** are not supported on WLC. The SSH client which is used to log in to the WLC should have minimum a non-aes-cbc cipher.

Step 1 Verify that your VT-100 terminal emulation program or DOS shell interface is configured with these parameters:

- Ethernet address
- Port 23

Step 2 Use the controller IP address to Telnet to the CLI.

Step 3 When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note The default username is admin, and the default password is admin.

The CLI displays the root level system prompt.

Note The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

Logging Out of the CLI

When you finish using the CLI, navigate to the root level and enter **logout**. The system prompts you to save any changes you made to the volatile RAM.

Note The CLI automatically logs you out without saving any changes after 5 minutes of inactivity. You can set the automatic logout from 0 (never log out) to 160 minutes using the **config serial timeout** command.

To prevent SSH or Telnet sessions from timing out, run the **config sessions timeout***0* command.

Navigating the CLI

- When you log into the CLI, you are at the root level. From the root level, you can enter any full command without first navigating to the correct command level.
- If you enter a top-level keyword such as **config**, **debug**, and so on without arguments, you are taken to the submode of that corresponding keyword.
- **`Ctrl + Z`** or entering **exit** returns the CLI prompt to the default or root level.
- When navigating to the CLI, enter **`?`** to see additional options available for any given command at the current level.
- You can also enter the space or tab key to complete the current keyword if unambigious.
- Enter **help** at the root level to see available command line editing options.

The following table lists commands you use to navigate the CLI and to perform common tasks.

Table 2: Commands for CLI Navigation and Common Tasks

Command	Action
help	At the root level, view system wide navigation commands
?	View commands available at the current level
command ?	View parameters for a specific command
exit	Move down one level

Command	Action
Ctrl + Z	Return from any level to the root level
save config	At the root level, save configuration changes from active working RAM to nonvolatile RAM (NVRAM) so they are retained after reboot
reset system	At the root level, reset the controller without logging out
logout	Logs you out of the CLI

Using the AutoInstall Feature for Controllers Without a Configuration

When you boot up a controller that does not have a configuration, the AutoInstall feature can download a configuration file from a TFTP server and then load the configuration onto the controller automatically.

If you create a configuration file on a controller that is already on the network (or through a Prime Infrastructure filter), place that configuration file on a TFTP server, and configure a DHCP server so that a new controller can get an IP address and TFTP server information, the AutoInstall feature can obtain the configuration file for the new controller automatically.

When the controller boots, the AutoInstall process starts. The controller does not take any action until AutoInstall is notified that the configuration wizard has started. If the wizard has not started, the controller has a valid configuration.

If AutoInstall is notified that the configuration wizard has started (which means that the controller does not have a configuration), AutoInstall waits for an additional 30 seconds. This time period gives you an opportunity to respond to the first prompt from the configuration wizard:

```
Would you like to terminate autoinstall? [yes]:
```

When the 30-second terminate timeout expires, AutoInstall starts the DHCP client. You can terminate the AutoInstall task even after this 30-second timeout if you enter **Yes** at the prompt. However, AutoInstall cannot be terminated if the TFTP task has locked the flash and is in the process of downloading and installing a valid configuration file.

Note The AutoInstall process and manual configuration using both the GUI and CLI of controller can occur in parallel. As part of the AutoInstall cleanup process, the service port IP address is set to 192.168.1.1 and the service port protocol configuration is modified. Because the AutoInstall process takes precedence over the manual configuration, whatever manual configuration is performed is overwritten by the AutoInstall process.

Information About the AutoInstall Feature

When you boot up a controller that does not have a configuration, the AutoInstall feature can download a configuration file from a TFTP server and then load the configuration onto the controller automatically.

If you create a configuration file on a controller that is already on the network (or through a Prime Infrastructure filter), place that configuration file on a TFTP server, and configure a DHCP server so that a new controller can get an IP address and TFTP server information, the AutoInstall feature can obtain the configuration file for the new controller automatically.

When the controller boots, the AutoInstall process starts. The controller does not take any action until AutoInstall is notified that the configuration wizard has started. If the wizard has not started, the controller has a valid configuration.

If AutoInstall is notified that the configuration wizard has started (which means that the controller does not have a configuration), AutoInstall waits for an additional 30 seconds. This time period gives you an opportunity to respond to the first prompt from the configuration wizard:

```
Would you like to terminate autoinstall? [yes]:
```

When the 30-second termination timeout expires, AutoInstall starts the DHCP client. You can terminate the AutoInstall task even after this 30-second timeout if you enter **Yes** at the prompt. However, AutoInstall cannot be terminated if the TFTP task has locked the flash and is in the process of downloading and installing a valid configuration file.

Note The AutoInstall process and manual configuration using both the GUI and CLI of Cisco WLC can occur in parallel. As part of the AutoInstall cleanup process, the service port IP address is set to 192.168.1.1 and the service port protocol configuration is modified. Because the AutoInstall process takes precedence over the manual configuration, whatever manual configuration is performed is overwritten by the AutoInstall process.

Restrictions on AutoInstall

- In Cisco 5508 WLCs, the following interfaces are used:
  - eth0—Service port (untagged)
  - dtl0—Gigabit port 1 through the NPU (untagged)
- AutoInstall is not supported on Cisco 2504 WLC.

Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server

AutoInstall attempts to obtain an IP address from the DHCP server until the DHCP process is successful or until you terminate the AutoInstall process. The first interface to successfully obtain an IP address from the DHCP server registers with the AutoInstall task. The registration of this interface causes AutoInstall to begin the process of obtaining TFTP server information and downloading the configuration file.

Following the acquisition of the DHCP IP address for an interface, AutoInstall begins a short sequence of events to determine the host name of the controller and the IP address of the TFTP server. Each phase of this sequence gives preference to explicitly configured information over default or implied information and to explicit host names over explicit IP addresses.

The process is as follows:

- If at least one Domain Name System (DNS) server IP address is learned through DHCP, AutoInstall creates a /etc/resolv.conf file. This file includes the domain name and the list of DNS servers that have been received. The Domain Name Server option provides the list of DNS servers, and the Domain Name option provides the domain name.
- If the domain servers are not on the same subnet as the controller, static route entries are installed for each domain server. These static routes point to the gateway that is learned through the DHCP Router option.
- The host name of the controller is determined in this order by one of the following:
  - If the DHCP Host Name option was received, this information (truncated at the first period [.]) is used as the host name for the controller.
  - A reverse DNS lookup is performed on the controller IP address. If DNS returns a hostname, this name (truncated at the first period [.]) is used as the hostname for the controller.
- The IP address of the TFTP server is determined in this order by one of the following:
  - If AutoInstall received the DHCP TFTP Server Name option, AutoInstall performs a DNS lookup on this server name. If the DNS lookup is successful, the returned IP address is used as the IP address of the TFTP server.
  - If the DHCP Server Host Name (sname) text box is valid, AutoInstall performs a DNS lookup on this name. If the DNS lookup is successful, the IP address that is returned is used as the IP address of the TFTP server.
  - If AutoInstall received the DHCP TFTP Server Address option, this address is used as the IP address of the TFTP server.
  - AutoInstall performs a DNS lookup on the default TFTP server name (cisco-wlc-tftp). If the DNS lookup is successful, the IP address that is received is used as the IP address of the TFTP server.
  - If the DHCP server IP address (siaddr) text box is nonzero, this address is used as the IP address of the TFTP server.
  - The limited broadcast address (255.255.255.255) is used as the IP address of the TFTP server.
- If the TFTP server is not on the same subnet as the controller, a static route (/32) is installed for the IP address of the TFTP server. This static route points to the gateway that is learned through the DHCP Router option.

Selecting a Configuration File

After the hostname and TFTP server have been determined, AutoInstall attempts to download a configuration file. AutoInstall performs three full download iterations on each interface that obtains a DHCP IP address. If the interface cannot download a configuration file successfully after three attempts, the interface does not attempt further.

The first configuration file that is downloaded and installed successfully triggers a reboot of the controller. After the reboot, the controller runs the newly downloaded configuration.

AutoInstall searches for configuration files in the order in which the names are listed:

- The filename that is provided by the DHCP Boot File Name option
- The filename that is provided by the DHCP File text box
- *host name*-confg
- *host name*.cfg
- *base MAC addres*s-confg (for example, 0011.2233.4455-confg)
- *serial number*-confg
- ciscowlc-confg
- ciscowlc.cfg

AutoInstall runs through this list until it finds a configuration file. It stops running if it does not find a configuration file after it cycles through this list three times on each registered interface.

Note

- The downloaded configuration file can be a complete configuration, or it can be a minimal configuration that provides enough information for the controller to be managed by the Cisco Prime Infrastructure. Full configuration can then be deployed directly from the Prime Infrastructure.
- AutoInstall does not expect the switch connected to the controller to be configured for either channels. AutoInstall works with a service port in LAG configuration.
- Cisco Prime Infrastructure provides AutoInstall capabilities for controllers. A Cisco Prime Infrastructure administrator can create a filter that includes the host name, the MAC address, or the serial number of the controller and associate a group of templates (a configuration group) to this filter rule. The Prime Infrastructure pushes the initial configuration to the controller when the controller boots up initially. After the controller is discovered, the Prime Infrastructure pushes the templates that are defined in the configuration group. For more information about the AutoInstall feature and Cisco Prime Infrastructure, see the Cisco Prime Infrastructure documentation.

Example: AutoInstall Operation

The following is an example of an AutoInstall process from start to finish:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Filename ==> 'abcd-confg'
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Server IP ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'service-port' - setting DHCP yiaddr ==> 172.19.29.253
AUTO-INSTALL: interface 'service-port' - setting DHCP Netmask ==> 255.255.255.0
```

```
AUTO-INSTALL: interface 'service-port' - setting DHCP Gateway ==> 172.19.29.1
AUTO-INSTALL: interface 'service-port' registered
AUTO-INSTALL: interation 1 -- interface 'service-port'
AUTO-INSTALL: DNS reverse lookup 172.19.29.253 ===> 'wlc-1'
AUTO-INSTALL: hostname 'wlc-1'
AUTO-INSTALL: TFTP server 1.100.108.2 (from DHCP Option 150)
AUTO-INSTALL: attempting download of 'abcd-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: interface 'management' - setting DHCP file ==> 'bootfile1'
AUTO-INSTALL: interface 'management' - setting DHCP TFTP Filename ==> 'bootfile2-confg'
AUTO-INSTALL: interface 'management' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[1] ==> 1.100.108.3
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[2] ==> 1.100.108.4
AUTO-INSTALL: interface 'management' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'management' - setting DHCP yiaddr ==> 1.100.108.238
AUTO-INSTALL: interface 'management' - setting DHCP Netmask ==> 255.255.254.0
AUTO-INSTALL: interface 'management' - setting DHCP Gateway ==> 1.100.108.1
AUTO-INSTALL: interface 'management' registered
AUTO-INSTALL: TFTP status - 'Config file transfer failed - Error from server: File not
found' (3)
AUTO-INSTALL: attempting download of 'wlc-1-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... updating configuration.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... storing in flash.' (2)
AUTO-INSTALL: TFTP status - 'System being reset.' (2)
Resetting system
```

Managing the Controller System Date and Time

You can configure the controller system date and time at the time of configuring the controller using the configuration wizard. If you did not configure the system date and time through the configuration wizard or if you want to change your configuration, you can follow the instructions in this section to configure the controller to obtain the date and time from a Network Time Protocol (NTP) server or to configure the date and time manually. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

You can also configure an authentication mechanism between various NTP servers.

Information About Controller System Date and Time

You can configure the controller system date and time at the time of configuring the controller using the configuration wizard. If you did not configure the system date and time through the configuration wizard or if you want to change your configuration, you can follow the instructions in this section to configure the controller to obtain the date and time from a Network Time Protocol (NTP) server or to configure the date and time manually. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

You can also configure an authentication mechanism between various NTP servers.

Restrictions on Configuring the Controller Date and Time

- If you are configuring wIPS, you must set the controller time zone to UTC.

- Cisco Aironet lightweight access points might not connect to the controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.
- You can configure an authentication channel between the controller and the NTP server.

Configuring the NTP/SNTP Server to Obtain the Date and Time (CLI)

Use these commands to configure an NTP/SNTP server to obtain the date and time:

Procedure

- To specify the NTP/SNTP server for the controller, enter this command:

  config time ntp server *index ip-address*

- (Optional) To specify the polling interval (in seconds), enter this command:

  config time ntp *interval*

- To enable or disable NTP/SNTP server authentication, enter these commands:
  - **config time ntp auth enable** *server-index key-index*—Enables NTP/SNTP authentication on a given NTP/SNTP server.
  - **config time ntp key-auth add** *key-index* **md5** {**ascii** | **hex**} *key*—Adds an authentication key. By default MD5 is used. The key format can be ASCII or hexadecimal.
  - **config time ntp key-auth delete** *key-index*—Deletes authentication keys.
  - **config time ntp auth disable** *server-index*—Disables NTP/SNTP authentication.
  - **show ntp-keys**—Displays the NTP/SNTP authentication related parameter.

- To delete an NTP server IP address or DNS server from the controller, enter this command:

  config time ntp delete *NTP_server index*

Configuring NTP/SNTP Authentication (GUI)

Step 1 Choose **Controller > NTP > Servers** to open the **NTP Servers** page.
Step 2 Click **New** to add an NTP server.
Step 3 Choose a server priority from the **Server Index (Priority)** drop-down list.
Step 4 Enter the NTP server IPv4/IPv6 address in the **Server IP Address (IPv4/IPv6)** text box.
Step 5 Enable NTP server authentication by checking the **NTP Server Authentication** check box.
Step 6 Click **Apply**.
Step 7 Choose **Controller** > **NTP** > **Keys**.
Step 8 Click **New** to create a key.
Step 9 Enter the key index in the **Key Index** text box.
Step 10 Choose the key format from the **Key Format** drop-down list.

Step 11 Enter the key in the **Key** text box.

Step 12 Click **Apply**.

Configuring NTP/SNTP Authentication (CLI)

Note By default, MD5 is used.

- **config time ntp auth enable** *server-index key-index*
- **config time ntp auth disable** *server-index*
- **config time ntp key-auth add key-index md5** *key-format key*
- Delete an authentication key by entering this command:

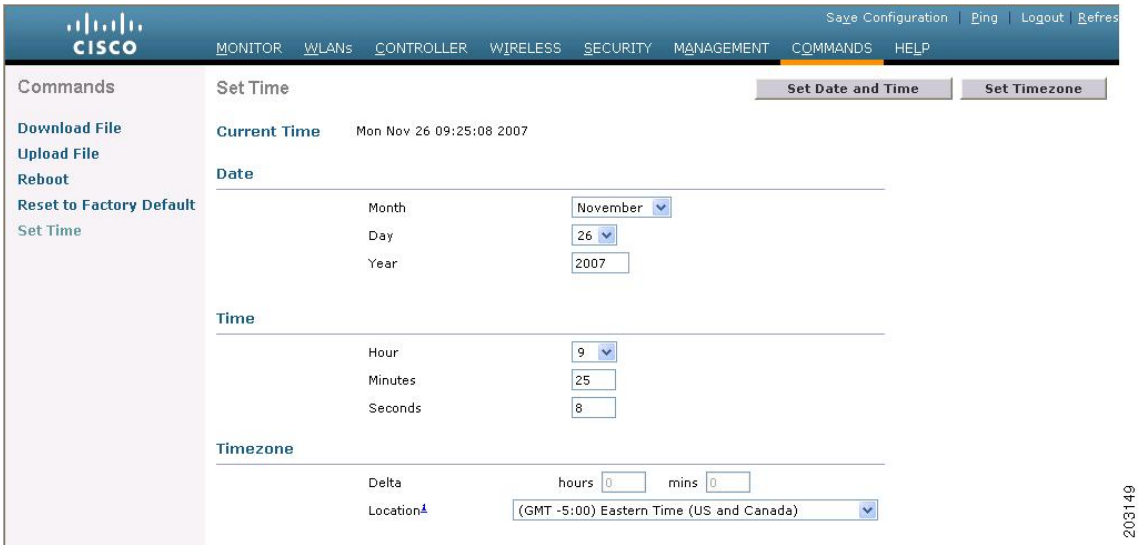
  config time ntp key-auth delete *key-index*
- View the list of NTP/SNTP key Indices by entering this command:

  show ntp-keys

Configuring the Date and Time (GUI)

Step 1 Choose **Commands > Set Time** to open the **Set Time** page.

Figure 15: Set Time Page



The current date and time appear at the top of the page.

Step 2 In the **Timezone** area, choose your local time zone from the **Location** drop-down list.

Note When you choose a time zone that uses Daylight Saving Time (DST), the controller automatically sets its system clock to reflect the time change when DST occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

Note You cannot set the time zone delta on the controller GUI. However, if you do so on the controller CLI, the change is reflected in the **Delta Hours** and **Mins** boxes on the controller GUI.

Step 3 Click **Set Timezone** to apply your changes.

Step 4 In the **Date** area, choose the current local month and day from the **Month** and **Day** drop-down lists, and enter the year in the **Year** box.

Step 5 In the **Time** area, choose the current local hour from the **Hour** drop-down list, and enter the minutes and seconds in the **Minutes** and **Seconds** boxes.

Note If you change the time zone location after setting the date and time, the values in the Time area are updated to reflect the time in the new time zone location. For example, if the controller is currently configured for noon Eastern time and you change the time zone to Pacific time, the time automatically changes to 9:00 a.m.

Step 6 Click **Set Date and Time** to apply your changes.

Step 7 Click **Save Configuration**.

Configuring the Date and Time (CLI)

Step 1 Configure the current local date and time in GMT on the controller by entering this command:

config time manual *mm/dd/yy hh:mm:ss*

Note When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8:00 a.m. Pacific time in the United States, you would enter 16:00 because the Pacific time zone is 8 hours behind GMT.

Step 2 Perform one of the following to set the time zone for the controller:

- Set the time zone location in order to have Daylight Saving Time (DST) set automatically when it occurs by entering this command:

  config time timezone location *location_index*

  where *location_index* is a number representing one of the following time zone locations:

  a. (GMT-12:00) International Date Line West

  b. (GMT-11:00) Samoa

  c. (GMT-10:00) Hawaii

  d. (GMT-9:00) Alaska

  e. (GMT-8:00) Pacific Time (US and Canada)

  f. (GMT-7:00) Mountain Time (US and Canada)

  g. (GMT-6:00) Central Time (US and Canada)

  h. (GMT-5:00) Eastern Time (US and Canada)

i. (GMT-4:00) Atlantic Time (Canada)

j. (GMT-3:00) Buenos Aires (Argentina)

k. (GMT-2:00) Mid-Atlantic

l. (GMT-1:00) Azores

m. (GMT) London, Lisbon, Dublin, Edinburgh (default value)

n. (GMT +1:00) Amsterdam, Berlin, Rome, Vienna

o. (GMT +2:00) Jerusalem

p. (GMT +3:00) Baghdad

q. (GMT +4:00) Muscat, Abu Dhabi

r. (GMT +4:30) Kabul

s. (GMT +5:00) Karachi, Islamabad, Tashkent

t. (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi

u. (GMT +5:45) Katmandu

v. (GMT +6:00) Almaty, Novosibirsk

w. (GMT +6:30) Rangoon

x. (GMT +7:00) Saigon, Hanoi, Bangkok, Jakarta

y. (GMT +8:00) Hong Kong, Beijing, Chongqing

z. (GMT +9:00) Tokyo, Osaka, Sapporo

aa. (GMT +9:30) Darwin

ab. (GMT+10:00) Sydney, Melbourne, Canberra

ac. (GMT+11:00) Magadan, Solomon Is., New Caledonia

ad. (GMT+12:00) Kamchatka, Marshall Is., Fiji

ae. (GMT+12:00) Auckland (New Zealand)

Note If you enter this command, the controller automatically sets its system clock to reflect DST when it occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

- Manually set the time zone so that DST is not set automatically by entering this command:

  config time timezone *delta_hours delta_mins*

  where *delta_hours* is the local hour difference from GMT, and *delta_mins* is the local minute difference from GMT.

  When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/–). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

  Note You can manually set the time zone and prevent DST from being set only on the controller CLI.

Step 3 Save your changes by entering this command:

save config

Step 4 Verify that the controller shows the current local time with respect to the local time zone by entering this command:

show time

Information similar to the following appears:

```
Time..................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
Timezone location........................ (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata

NTP Servers
    NTP Polling Interval.........................     3600

     Index     NTP Key Index     NTP Server       NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              1           209.165.200.225      AUTH SUCCESS
```

Note If you configured the time zone location, the Timezone Delta value is set to "0:0." If you manually configured the time zone using the time zone delta, the Timezone Location is blank.

Telnet and Secure Shell Sessions

Telnet and Secure Shell Sessions

Telnet is a network protocol used to provide access to the controller's CLI. Secure Shell (SSH) is a more secure version of Telnet that uses data encryption and a secure channel for data transfer. You can use the controller GUI or CLI to configure Telnet and SSH sessions.

This section contains the following subsections:

Restrictions

- When the tool **Putty** is used as an SSH client to connect to the controller running versions 8.6 and above, you may observe disconnects from **Putty** when a large output is requested with paging disabled. This is observed when the controller has lots of configurations and/ or has a high count of APs and clients. We recomend you to use alternate SSH clients in such situations.
- In Release 8.6, controllers are migrated from OpenSSH to libssh, and libssh does not support these key exchange (KEX) algorithms: *ecdh-sha2-nistp384* and *ecdh-sha2-nistp521*. Only *ecdh-sha2-nistp256* is supported.

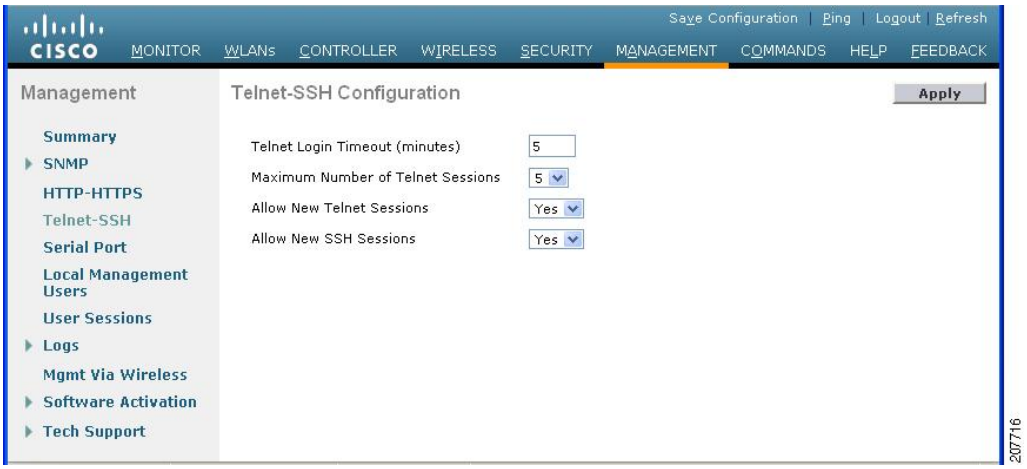
Restrictions on Telnet and SSH

- Only the FIPS approved algorithm aes128-cbc is supported when using SSH to control WLANs.
- The controller does not support raw Telnet mode.

Configuring Telnet and SSH Sessions (GUI)

Step 1 Choose **Management** > **Telnet-SSH** to open the Telnet-SSH Configuration page.

Figure 16: Telnet-SSH Configuration Page



Step 2 In the **Telnet Login Timeout** text box, enter the number of minutes that a Telnet session is allowed to remain inactive before being terminated. The valid range is 0 to 160 minutes (inclusive), and the default value is 5 minutes. A value of 0 indicates no timeout.

Step 3 From the **Maximum Number of Sessions** drop-down list, choose the number of simultaneous Telnet or SSH sessions allowed. The valid range is 0 to 5 sessions (inclusive), and the default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

Step 4 To forcefully close current login sessions, choose **Management** > **User Sessions** > **close** from the CLI session drop-down list.

Step 5 From the **Allow New Telnet Sessions** drop-down list, choose **Yes** or **No** to allow or disallow new Telnet sessions on the controller. The default value is No.

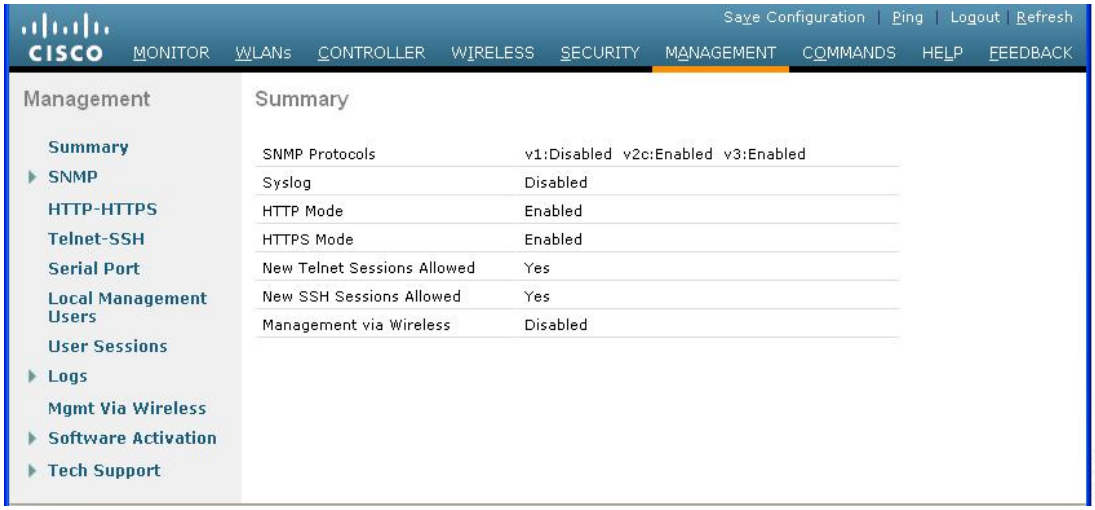
Step 6 From the \ drop-down list, choose **Yes** or **No** to allow or disallow new SSH sessions on the controller. The default value is Yes.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Step 9 To see a summary of the Telnet configuration settings, choose **Management** > **Summary**. The Summary page appears.

Figure 17: Summary Page



This page shows whether additional Telnet and SSH sessions are permitted.

Configuring Telnet and SSH Sessions (CLI)

Step 1 Allow or disallow new Telnet sessions on the controller by entering this command:

config network telnet {**enable** | **disable**}

The default value is disabled.

Step 2 Allow or disallow new SSH sessions on the controller by entering this command:

config network ssh {**enable** | **disable**}

The default value is enabled.

Note Use the **config network ssh cipher-option high** {**enable** | **disable**} command to enable sha2 which is supported in WLC.

Step 3 (Optional) Specify the number of minutes that a Telnet session is allowed to remain inactive before being terminated by entering this command:

config sessions timeout *timeout*

where *timeout* is a value between 0 and 160 minutes (inclusive). The default value is 5 minutes. A value of 0 indicates no timeout.

Step 4 (Optional) Specify the number of simultaneous Telnet or SSH sessions allowed by entering this command:

config sessions maxsessions *session_num*

where *session_num* is a value between 0 and 5 (inclusive). The default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

Step 5 Save your changes by entering this command:

save config

Step 6 You can close all the Telnet or SSH sessions by entering this command:

config loginsession close {*session-id* | *all*}

The *session-id* can be taken from the **show login-session** command.

Managing and Monitoring Remote Telnet and SSH Sessions

Step 1 See the Telnet and SSH configuration settings by entering this command:

show network summary

Information similar to the following appears:

```
RF-Network Name............................. TestNetwork1
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Shell (ssh).......................... Enable
Telnet...................................... Disable
...
```

Step 2 See the Telnet session configuration settings by entering this command:

show sessions

Information similar to the following appears:

```
CLI Login Timeout (minutes)............. 5
Maximum Number of CLI Sessions....... 5
```

Step 3 See all active Telnet sessions by entering this command:

show login-session

Information similar to the following appears:

```
ID    User Name     Connection From   Idle Time    Session Time
-- ---------------  ---------------  ------------  ------------
00    admin        EIA-232       00:00:00      00:19:04
```

Configuring Telnet Privileges for Selected Management Users (GUI)

Using the controller, you can configure Telnet privileges to selected management users. To do this, you must have enabled Telnet privileges at the global level. By default, all management users have Telnet privileges enabled.

Note SSH sessions are not affected by this feature.

Step 1 Choose **Management** > **Local Management Users**.

Step 2 On the **Local Management Users** page, select or unselect the **Telnet Capable** check box for a management user.

Step 3 Save the configuration.

Configuring Telnet Privileges for Selected Management Users (CLI)

Procedure

- Configure Telnet privileges for a selected management user by entering this command:
  config mgmtuser telnet *user-name* {**enable** | **disable**}

Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- The **upgrade** command cannot be used when a Telnet or SSH session is enabled.

Troubleshooting Access Points Using Telnet or SSH (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the **All APs** page.

Step 2 Click the name of the access point for which you want to enable Telnet or SSH.

Step 3 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 4 Select the **Telnet** check box to enable Telnet connectivity on this access point. The default value is unchecked.

Step 5 Select the **SSH** check box to enable SSH connectivity on this access point. The default value is unchecked.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Troubleshooting Access Points Using Telnet or SSH (CLI)

Step 1 Enable Telnet or SSH connectivity on an access point by entering this command:

config ap {**telnet** | **ssh**} **enable** *Cisco_AP*

The default value is disabled.

Note Disable Telnet or SSH connectivity on an access point by entering this command: **config ap** {**telnet** | **ssh**} **disable** *Cisco_AP*

Step 2 Save your changes by entering this command:

save config

Step 3 See whether Telnet or SSH is enabled on an access point by entering this command:

show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 5
Cisco AP Name.................................... AP33
Country code..................................... Multiple Countries:US,AE,AR,AT,AU,BH
Reg. Domain allowed by Country................... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 2
MAC Address...................................... 00:19:2f:11:16:7a
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.22.8.133
IP NetMask....................................... 255.255.248.0
Gateway IP Addr.................................. 10.22.8.1
Domain.......................................
Name Server.....................................
Telnet State..................................... Enabled
Ssh State........................................ Enabled
...
```

Managing the Controller Wirelessly

You can monitor and configure controllers using a wireless client. This feature is supported for all management tasks except uploads from and downloads to the controller.

Before you can open the GUI or the CLI from a wireless client device, you must configure the controller to allow the connection.

Enabling Wireless Connections (GUI)

Step 1 Log onto the GUI.

Step 2 Choose **Management** > **Mgmt Via Wireless** page.

Step 3 Enable the Controller Management to be accessible from wireless clients.

Step 4 Click **Apply**.

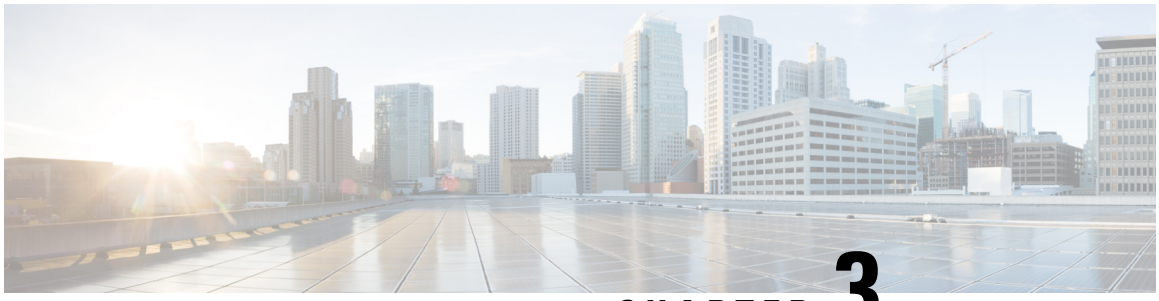
Enabling Wireless Connections (CLI)

Step 1 Log onto the CLI.

Step 2 Enter the **config network mgmt-via-wireless enable** command.

Step 3 Use a wireless client to associate to a lightweight access point connected to the controller.

Step 4 On the wireless client, open a Telnet session to the controller, or browse to the controller GUI.



CHAPTER 3

Managing Licenses

- Installing and Configuring Licenses, on page 51
- Rehosting Licenses, on page 64

Installing and Configuring Licenses

Information About Installing and Configuring Licenses

You can order Cisco 5508 WLCs with support for 12, 25, 50, 100, 250 or 500 access points as the controller's base capacity. You can add additional access point capacity through capacity adder licenses available at 25, 50, 100 and 250 access point capacities. You can add the capacity adder licenses to any base license in any combination to arrive at the maximum capacity of 500 access points. The base and adder licenses are supported through both rehosting and RMAs.

The base license supports the standard base software set, and the premium software set is included as part of the base feature set, which includes this functionality:

- Datagram Transport Layer Security (DTLS) data encryption for added security across remote WAN and LAN links.
- The availability of data DTLS is as follows:
  - Cisco 5508 WLC—The Cisco 5508 WLC is available with two licensing options: One with data DTLS capabilities and another image without data DTLS.
  - Cisco 2504 WLC and Cisco WiSM2—These platforms by default do not contain DTLS. To turn on data DTLS, you must install a license. These platforms will have a single image with data DTLS turned off. To use data DTLS, you must have a license.
  - Cisco Flex 7510 and Cisco 8510 WLCs—The DTLS license is in-built. You are not required to install DTLS license separately.
- Support for OfficeExtend access points, which are used for secure mobile teleworking.

All features included in a Wireless LAN Controller WPLUS license are now included in the base license. There are no changes to Cisco Prime Infrastructure BASE and PLUS licensing. These WPlus license features are included in the base license:

- OfficeExtend AP

- Enterprise Mesh
- CAPWAP Data Encryption

For information about upgrade and capacity adder licenses, see the product data sheet of your controller model.

Restrictions for Using Licenses

The following are the restrictions you must keep in mind when using licenses for the controllers:

- The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines:
  - If you have a WPlus license and you upgrade from 6.0.x.x to 7.x.x.x, your license file contains both Basic and WPlus license features. There is no disruption in feature availability and operation.
  - If you have a WPlus license and you downgrade from 7.x.x.x to 6.0.196.0 or 6.0.188.0 or 6.0.182.0, your license file contains only base license, and you will lose all WPlus features.
  - If you have a base license and you downgrade from 6.0.196.0 to 6.0.188.0 or 6.0.182.0, when you downgrade, you lose all WPlus features.
- In the controller software 7.0.116.0 and later releases, the AP association trap is ciscoLwappApAssociated. In prior releases, the trap was bsnAPAssociated.
- The ap-count licenses and their corresponding image-based licenses are installed together. The controller keeps track of the licensed access point count and does not allow more than the number of access points to associate to it.
- The Cisco 5508 WLC is shipped with both permanent and evaluation base and base-ap-count licenses. If desired, you can activate the evaluation licenses, which are designed for temporary use and set to expire after 60 days.
- No licensing steps are required after you receive your Cisco 5508 WLC because the licenses you ordered are installed at the factory. In addition, licenses and product authorization keys (PAKs) are preregistered to serial numbers. However, as your wireless network evolves, you might want to add support for additional access points or upgrade from the standard software set to the base software set. To do so, you must obtain and install an upgrade license.

Obtaining an Upgrade or Capacity Adder License

This section describes how to get an upgrade or capacity adder license.

Information About Obtaining an Upgrade or Capacity Adder License

A certificate with a product authorization key (PAK) is required before you can obtain an upgrade license.

You can use the capacity adder licenses to increase the number of access points supported by the controller up to a maximum of 500 access points. The capacity adder licenses are available in access point capacities of 10, 25, 50, 100 and 250 access points. You can add these licenses to any of the base capacity licenses of 12, 25, 50, 100 and 250 access points.

For example, if your controller was initially ordered with support for 100 access points (base license AIR-CT5508-100-K9), you could increase the capacity to 500 access points by purchasing a 250 access point,

100 access point, and a 50 access point additive capacity license (LIC-CT5508-250A, LIC-CT5508-100A, and LIC-CT5508-50A).

You can find more information on ordering capacity adder licenses at this URL: http://www.cisco.com/c/en/us/products/wireless/5500-series-wireless-controllers/datasheet-listing.html

Note If you skip any tiers when upgrading (for example, if you do not install the -25U and -50U licenses along with the -100U), the license registration for the upgraded capacity fails.

For a single controller, you can order different upgrade licenses in one transaction (for example, -25U, -50U, -100U, and -250U), for which you receive one PAK with one license. Then you have only one license (instead of four) to install on your controller.

If you have multiple controllers and want to upgrade all of them, you can order multiple quantities of each upgrade license in one transaction (for example, you can order 10 each of the -25U, -50U, -100U, and -250 upgrade licenses), for which you receive one PAK with one license. You can continue to register the PAK for multiple controllers until it is exhausted.

For more information about the base license SKUs and capacity adder licenses, see the respective controller's data sheet.

Obtaining and Registering a PAK Certificate

Step 1 Order the PAK certificate for an upgrade license through your Cisco channel partner or your Cisco sales representative, or order it online at this URL:

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

Step 2 If you are ordering online, begin by choosing the primary upgrade SKU **L-LIC-CT5508-UPG or LIC CT5508-UPG**. Then, choose any number of the following options to upgrade one or more controllers under one PAK. After you receive the certificate, use one of the following methods to register the PAK:

- **Licensing portal**—This alternative method enables you to manually obtain and install licenses on your controller. If you want to use the licensing portal to register the PAK, follow the instructions in *Step 3*.

Step 3 Use the licensing portal to register the PAK as follows:

a) Go to http://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet
b) On the main Product License Registration page, enter the PAK mailed with the certificate in the Product Authorization Key (PAK) text box and click **Submit**.
c) On the Validate Features page, enter the number of licenses that you want to register in the Qty text box and click **Update**.
d) To determine the controller's product ID and serial number, choose **Controller** > **Inventory** on the controller GUI or enter the **show license udi** command on the controller CLI.

Information similar to the following appears on the controller CLI:

```
Device#          PID                SN                 UDI
-------  ------------------- ---------------  ------------------------
*0          AIR-CT5508-K9      CW1308L030     AIR-CT5508-K9:FCW1308L030
```

e) On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to install the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click **Submit**.
f) On the Finish and Submit page, verify that all information is correct and click **Submit**.
g) When a message appears indicating that the registration is complete, click **Download License**. The license is e-mailed within 1 hour to the address that you specified.
h) When the e-mail arrives, follow the instructions provided.
i) Copy the license file to your TFTP server.

Installing a License

Installing a License (GUI)

Step 1 Choose **Management** > **Software Activation** > **Commands** to open the License Commands page.

Step 2 From the Action drop-down list, choose **Install License**. The Install License from a File section appears.

Step 3 In the File Name to Install text box, enter the path to the license (*.lic) on the TFTP server.

Step 4 Click **Install License**. A message appears to show whether the license was installed successfully. If the installation fails, the message provides the reason for the failure, such as the license is an existing license, the path was not found, the license does not belong to this device, you do not have correct permissions for the license, and so on.

Step 5 If the end-user license agreement (EULA) acceptance dialog box appears, read the agreement and click **Accept** to accept the terms of the agreement.

Note Typically, you are prompted to accept the EULA for evaluation, extension, and rehost licenses. The EULA is also required for permanent licenses, but it is accepted during license generation.

Step 6 Save a backup copy of all installed licenses as follows:

a) From the Action drop-down list, choose **Save License**.
b) In the File Name to Save text box, enter the path on the TFTP server where you want the licenses to be saved.

Note You cannot save evaluation licenses.

c) Click **Save Licenses**.

Step 7 Reboot the controller.

Note We recommend that you reset the system to ensure that the newly installed license file is saved in the WLC.

Installing a License (CLI)

Step 1 Install a license on the controller by entering this command:

license install *url*

where *url* is tftp://*server_ip*/*path*/*filename*.

Note To remove a license from the controller, enter the **license clear** *license_name* command. For example, you might want to delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

Step 2 If you are prompted to accept the end-user license agreement (EULA), read and accept the terms of the agreement.

Note Typically, you are prompted to accept the EULA for evaluation, extension, and rehost licenses. The EULA is also required for permanent licenses, but it is accepted during license generation.

Step 3 Add comments to a license or delete comments from a license by entering this command:

license comment {**add** | **delete**} *license_name comment_string*

Step 4 Save a backup copy of all installed licenses by entering this command:

license save *url*

where *url* is tftp://*server_ip*/*path*/*filename*.

Step 5 Reboot the controller by entering this command:

reset system.

Note We recommend that you reset the system to ensure that the newly installed license file is saved in the WLC.

Viewing Licenses

Viewing Licenses (GUI)

Step 1 Choose **Management** > **Software Activation** > **Licenses** to open the Licenses page.

This page lists all the licenses that are installed on the controller. For each license, it shows the license type, expiration, count (the maximum number of access points that are allowed for this license), priority (low, medium, or high), and status (in use, not in use, inactive, or EULA not accepted).

Note Controller platforms do not support the status of "grace period" or "extension" as a license type. The license status always shows as "evaluation" even if a grace period or an extension evaluation license is installed.

If you ever want to remove a license from the controller, hover your cursor over the blue drop-down arrow for the license and click **Remove**. For example, you might want to delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

In Cisco 2504 and 5508 Wireless Controllers, the license section is limited to display 10 licenses only. Also, these licenses cannot be deleted from the controller.

Step 2 Click the link for the desired license to view more details for a particular license. The License Detail page appears.

This page shows the following additional information for the license:

- The license type (permanent, evaluation, or extension)
- The license version

- The status of the license (in use, not in use, inactive, or EULA not accepted).
- The length of time before the license expires

  Note Permanent licenses never expire.

- Whether the license is a built-in license.
- The maximum number of access points allowed for this license
- The number of access points currently using this license

Step 3 If you want to enter a comment for this license, type it in the Comment text box and click **Apply**.

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

Viewing Licenses (CLI)

Procedure

- See the license level, license type, and number of access points licensed on the controller by entering this command:

  See the license level, license type, and number of access points licensed on the controller by entering this command:

  show sysinfo

  This example shows a sample output of the command run on Cisco 8540 Wireless Controller using Release 8.3:

```
Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.3.100.0
RTOS Version..................................... 8.3.100.0
Bootloader Version............................... 8.0.110.0
Emergency Image Version.......................... 8.0.110.0

OUI File Last Update Time........................ Sun Sep 07 10:44:07 IST 2014


Build Type....................................... DATA + WPS

System Name...................................... TestSpartan8500Dev1
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.1615
Redundancy Mode.................................. Disabled
IP Address....................................... 8.1.4.2
IPv6 Address..................................... ::
System Up Time................................... 0 days 17 hrs 20 mins 58 secs

--More-- or (q)uit
System Timezone Location.........................
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... Multiple Countries : IN,US
Operating Environment............................ Commercial (10 to 35 C)
```

```
Internal Temp Alarm Limits..................... 10 to 38 C
Internal Temperature........................... +21 C
Fan Status..................................... OK

RAID Volume Status
Drive 0........................................ Good
Drive 1........................................ Good

State of 802.11b Network....................... Enabled
State of 802.11a Network....................... Enabled
Number of WLANs................................ 7
Number of Active Clients....................... 1

OUI Classification Failure Count................ 0

Burned-in MAC Address.......................... F4:CF:E2:0A:27:00
Power Supply 1................................. Present, OK

--More-- or (q)uit
Power Supply 2................................. Present, OK
Maximum number of APs supported................ 6000
System Nas-Id..................................
WLC MIC Certificate Types...................... SHA1/SHA2
Licensing Type................................. RTU
```

Note The Operating Environment and Internal Temp Alarm Limits data are not displayed for Cisco Flex 7510 WLCs.

- See a brief summary of all active licenses installed on the controller by entering this command:

  show license summary

  Information similar to the following appears:

```
Index 1 Feature: wplus
        Period left: 0 minute 0 second
Index 2 Feature: wplus-ap-count
  Period left: 0 minute 0 second
Index3   Feature: base
  Period left: Life time
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
Index 4 Feature: base-ap-count
  Period left: 6 weeks, 4 days
  License Type: Evaluation
  License State: Active, In Use
  License Count: 250/250/0
  License Priority: High
```

- See all of the licenses installed on the controller by entering this command:

  show license all

  Information similar to the following appears:

```
License Store: Primary License Storage
```

```
StoreIndex:  1  Feature: base   Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium

StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  3 days
        License Count: 250/0/0
        License Priority: High
```

- See the details for a particular license by entering this command:

  show license detail *license_name*

  Information similar to the following appears:

```
Index:  1       Feature: base-ap-count   Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: 12/0/0
        License Priority: Medium
        Store Index: 0
        Store Name: Primary License Storage

Index:  2       Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: 250/0/0
        License Priority: Low
        Store Index: 3
           Store Name: Evaluation License Storage
```

- See all expiring, evaluation, permanent, or in-use licenses by entering this command:

  show license {**expiring** | **evaluation** | **permanent** | **in-use**}

  Information similar to the following appears for the **show license in-use** command:

```
StoreIndex:  2  Feature: base-ap-count   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: 12/12/0
        License Priority: Medium
StoreIndex:  3  Feature: base Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted License Priority: Medium
```

Note Controller platforms do not support the status of “grace period” or “extension” as a license type. The license status will always show “evaluation” even if a grace period or an extension evaluation license is installed.

- See the maximum number of access points allowed for this license on the controller, the number of access points currently joined to the controller, and the number of access points that can still join the controller by entering this command:

  show license capacity

  Information similar to the following appears:

```
Licensed Feature    Max Count      Current Count       Remaining Count
----------------    ---------      -------------       ---------------
AP Count              250              4                    246
```

- See statistics for all licenses on the controller by entering this command:

  show license statistics

- See a summary of license-enabled features by entering this command:

  show license feature

Configuring the Maximum Number of Access Points Supported

Configuring Maximum Number of Access Points to be Supported (GUI)

You can configure the maximum number APs that can be supported on a controller. The controller limits the number of APs that are supported based on the licensing information and the controller model. The maximum number of APs supported that is specified in the licensing information overrides the number that you configure if the configured value is greater than the licensed value. By default, this feature is disabled. You must reboot the controller if you change the configuration.

Step 1 Choose **Controller** > **General**.

Step 2 Enter a value in the **Maximum Allowed APs** field.

Step 3 Save the configuration.

Configuring Maximum Number of Access Points to be Supported (CLI)

Procedure

- Configure the maximum number of access points to be supported on a controller by entering this command:
  config ap max-count *count*
- See the maximum number of access points that are supported on the controller by entering this command:
  show ap max-count summary

Troubleshooting Licensing Issues

Procedure

- Configure debugging of licensing core events and core errors by entering this command:

debug license core {**all** | **errors** | **events**} {**enable** | **disable**}

- Configure debugging of licensing errors by entering this command:

  debug license errors {**enable** | **disable**}

- Configure debugging of licensing events by entering this command:

  debug license events {**enable** | **disable**}

Activating an AP-Count Evaluation License

Information About Activating an AP-Count Evaluation License

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50-access-point count and want to try an evaluation license with a 100-access-point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the controller uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license.

Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

Activating an AP-Count Evaluation License (GUI)

Step 1 Choose **Management** > **Software Activation** > **Licenses** to open the Licenses page.

The Status column shows which licenses are currently in use, and the Priority column shows the current priority of each license.

Step 2 Activate an ap-count evaluation license as follows:

a) Click the link for the ap-count evaluation license that you want to activate. The License Detail page appears.
b) Choose **High** from the Priority drop-down list and click **Set Priority**.

Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

c) Click **OK** when prompted to confirm your decision about changing the priority of the license.
d) When the EULA appears, read the terms of the agreement and then click **Accept**.
e) When prompted to reboot the controller, click **OK**.
f) Reboot the controller in order for the priority change to take effect.

g) Click **Licenses** to open the Licenses page and verify that the ap-count evaluation license now has a high priority and is in use. You can use the evaluation license until it expires.

Step 3 If you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:

a) On the Licenses page, click the link for the ap-count evaluation license that is in use.

b) Choose **Low** from the Priority drop-down list and click **Set Priority**.

Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

c) Click **OK** when prompted to confirm your decision about changing the priority of the license.

d) When the EULA appears, read the terms of the agreement and then click **Accept**.

e) When prompted to reboot the controller, click **OK**.

f) Reboot the controller in order for the priority change to take effect.

g) Click **Licenses** to open the Licenses page and verify that the ap-count evaluation license now has a low priority and is not in use. Instead, the ap-count permanent license should be in use.

Activating an AP-Count Evaluation License (CLI)

Step 1 See the current status of all the licenses on your controller by entering this command:

show license all

Information similar to the following appears:

```
License Store: Primary License Storage
StoreIndex:  0  Feature: base-ap-count   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: 12/0/0
        License Priority: Medium
StoreIndex:  1  Feature: base   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
StoreIndex:  2  Feature: base   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
  License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: 250/0/0
            License Priority: Low
```

The **License State** text box shows the licenses that are in use, and the **License Priority** text box shows the current priority of each license.

Step 2 Activate an ap-count evaluation license as follows:

a) Raise the priority of the base-ap-count evaluation license by entering this command:

license modify priority *license_name* **high**

Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

b) Reboot the controller in order for the priority change to take effect by entering this command:

reset system

c) Verify that the ap-count evaluation license now has a high priority and is in use by entering this command:

show license all

You can use the evaluation license until it expires.

Step 3 If you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:

a) Lower the priority of the ap-count evaluation license by entering this command:

license modify priority *license_name* **low**

b) Reboot the controller in order for the priority change to take effect by entering this command:

reset system

c) Verify that the ap-count evaluation license now has a low priority and is not in use by entering this command:

show license all

Instead, the ap-count permanent license should be in use.

Configuring Right to Use Licensing

Right to Use Licensing

Right to Use (RTU) licensing is a model in which licenses are not tied to a unique device identifier (UDI), product ID, or serial number. Use RTU licensing to enable a desired AP license count on the controller after you accept the End User License Agreement (EULA). This allows you to add AP counts on a controller interacting with external tools.

RTU licensing is supported only on the following Cisco Wireless Controller platforms:

- Cisco 5520 WLC
- Cisco Flex 7510 WLC
- Cisco 8510 WLC
- Cisco 8540 WLC
- Cisco vWLC

In the RTU licensing model, the following types of licenses are available:

- Permanent or base licenses—These licenses are programmed into the controller hardware at the time of manufacturing. These licenses are base count licenses that cannot be deleted or transferred.
- Adder licenses—These licenses are wireless access point count licenses that you can activate by accepting the RTU EULA. The EULA states that you are obliged to purchase the specified access point count licenses at the time of activation. You must activate these licenses for the purchased access points count and accept the EULA.

  You can remove an adder license from one controller and transfer the license to another controller in the same product family. For example, an adder license such as LIC-CT7500-100A can be transferred (partially or fully) from one Cisco Flex 7500 Series Controller to another Cisco Flex 7500 Series Controller.

  Note Licenses embedded in the controller at the time of shipment is not transferrable.

- Evaluation licenses—These licenses are demo or trial mode licenses that are valid for 90 days. Fifteen days prior to the expiry of the 90-day period, you are notified about the requirement to buy the permanent license. These evaluation licenses are installed with the license image. You can activate the evaluation licenses anytime with a command. A EULA is prompted after you run the activation command on the controller CLI. The EULA states that you are obligated to pay for the specified license count within 90 days of usage. The countdown starts after you accept the EULA.

Whenever you add or delete an access point adder license on the controller, you are prompted with an RTU EULA. You can either accept or decline the RTU EULA for each add or delete operation.

For high-availability (HA) controllers when you enable HA, the controllers synchronize with the enabled license count of the primary controller and support high availability for up to the license count enabled on the primary controller.

You can view the RTU licenses through the controller GUI or CLI. You can also view these licenses across multiple wireless controllers through Cisco Prime Infrastructure.

With Release 8.1, the license management for Cisco Virtual Wireless Controller is changed from license-file based management to Right-to-Use-based management. The previous licenses are still valid, and when you upgrade to Release 8.1 from an earlier release, you are required to only accept an end-user license agreement again to the quantity installed before.

Configuring Right to Use Licensing (GUI)

Step 1 Choose **Management** > **Software Activation** > **Licenses** to open the **Licenses** page.

Step 2 In the Adder License area, choose to add or delete the number of APs that an AP license can support, enter a value, and click **Set Count**.

Step 3 Save the configuration.

Configuring Right to Use Licensing (CLI)

Procedure

- Add or delete the number of APs that an AP license can support by entering this command:

  license {**add** | **delete**} **ap-count** *count*

- Add or delete a license for a feature by entering this command:

  license {**add** | **delete**} **feature** *license_name*

- Activate or deactivate an evaluation AP count license by entering this command:

  license {**activate** | **deactivate**} **ap-count eval**

Note When you activate the license, you are prompted to accept or reject the End User License Agreement (EULA) for the given license. If you activate a license that supports fewer number of APs than the current number of APs connected to the controller, the activation command fails.

- Activate or deactivate a feature license by entering this command:

  license {**activate** | **deactivate**} **feature** *license_name*

- See the licensing information by entering this command:

  show license all

What to do next

Note After you add or delete the license, WLC must use the **save config** command to save the license.

Rehosting Licenses

This section describes how to rehost licenses.

Information About Rehosting Licenses

Revoking a license from one controller and installing it on another is called *rehosting*. You might want to rehost a license in order to change the purpose of a controller. For example, if you want to move your OfficeExtend or indoor mesh access points to a different controller, you could transfer the adder license from one controller to another controller of the same model (intramodel transfer). This can be done in the case of RMA or a network rearchitecture that requires you to transfer licenses from one appliance to another. It is not possible to rehost base licenses in normal scenarios of network rearchitecture. The only exception where the transfer of base licenses is allowed is for RMA when you get a replacement hardware when your existing appliance has a failure.

Evaluation licenses cannot be rehosted.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.

Note A revoked license cannot be reinstalled on the same controller.

Note Starting in the release 7.3, the Right-to-Use licensing is supported on the Cisco Flex 7510 WLCs, thereby the rehosting behavior changes on these controllers. If you require to rehost licenses, you need to plan rehosting the installed adder licenses prior to an upgrade.

Rehosting a License

Rehosting a License (GUI)

Step 1 Choose **Management** > **Software Activation** > **Commands** to open the License Commands page.

Step 2 From the Action drop-down list, choose **Rehost**. The Revoke a License from the Device and Generate Rehost Ticket area appears.

Step 3 In the File Name to Save Credentials text box, enter the path on the TFTP server where you want the device credentials to be saved and click **Save Credentials**.

Step 4 To obtain a permission ticket to revoke the license, follow these steps:

a) Click **Cisco Licensing** (https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet).

b) On the Product License Registration page, click **Look Up a License** under Manage Licenses.

c) Enter the product ID and serial number for your controller.

Note To find the controller's product ID and serial number, choose **Controller** > **Inventory** on the controller GUI.

d) Open the device credential information file that you saved in Step 3 and copy and paste the contents of the file into the Device Credentials text box.

e) Enter the security code in the blank box and click **Continue**.

f) Choose the licenses that you want to revoke from this controller and click **Start License Transfer**.

g) On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost text box and click **Continue**.

h) On the Designate Licensee page, enter the product ID and serial number of the controller for which you plan to revoke the license, read and accept the conditions of the End User License Agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.

i) On the Review and Submit page, verify that all information is correct and click **Submit**.

j) When a message appears indicating that the registration is complete, click **Download Permission Ticket**. The rehost permission ticket is e-mailed within 1 hour to the address that you specified.

k) After the e-mail arrives, copy the rehost permission ticket to your TFTP server.

Step 5 Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows:

a) In the Enter Saved Permission Ticket File Name text box, enter the TFTP path and filename (*.lic) for the rehost permission ticket that you generated in Step 4.
b) In the Rehost Ticket File Name text box, enter the TFTP path and filename (*.lic) for the ticket that will be used to rehost this license on another controller.
c) Click **Generate Rehost Ticket**.
d) When the End User License Agreement (EULA) acceptance dialog box appears, read the agreement and click **Accept** to accept the terms of the agreement.

Step 6 Use the rehost ticket generated in Step 5 to obtain a license installation file, which can then be installed on another controller as follows:

a) Click **Cisco Licensing**.
b) On the Product License Registration page, click **Upload Rehost Ticket** under Manage Licenses.
c) On the Upload Ticket page, enter the rehost ticket that you generated in Step 5 in the Enter Rehost Ticket text box and click **Continue**.
d) On the Validate Features page, verify that the license information for your controller is correct, enter the rehost quantity, and click **Continue**.
e) On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to use the license, read and accept the conditions of the End User License Agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.
f) On the Review and Submit page, verify that all information is correct and click **Submit**.
g) When a message appears indicating that the registration is complete, click **Download License**. The rehost license key is e-mailed within 1 hour to the address that you specified.
h) After the e-mail arrives, copy the rehost license key to your TFTP server.
i) Follow the instructions in the Installing a License section to install this on another controller.

Step 7 After revoking the license on original controller, correspondent evaluation licence appear with High pritority. Lower the priority of the evaluation license so that the parmanent license is in "In Use" status.

Rehosting a License (CLI)

Step 1 Save device credential information to a file by entering this command:

license save credential *url*

where *url* is tftp://*server_ip*/*path*/*filename*.

Step 2 Obtain a permission ticket to revoke the license as follows:

a) Go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet. The Product License Registration page appears.
b) Under Manage Licenses, click **Look Up a License**.
c) Enter the product ID and serial number for your controller.

Note To find the controller's product ID and serial number, enter the **show license udi** command on the controller CLI.

d) Open the device credential information file that you saved in Step 1 and copy and paste the contents of the file into the Device Credentials text box.
e) Enter the security code in the blank box and click **Continue**.
f) Choose the licenses that you want to revoke from this controller and click **Start License Transfer**.

g) On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost text box and click **Continue**.
h) On the Designate Licensee page, enter the product ID and serial number of the controller for which you plan to revoke the license, read and accept the conditions of the End-User License Agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.
i) On the Review and Submit page, verify that all information is correct and click **Submit**.
j) When a message appears indicating that the registration is complete, click **Download Permission Ticket**. The rehost permission ticket is e-mailed within 1 hour to the address that you specified.
k) After the e-mail arrives, copy the rehost permission ticket to your TFTP server.

Step 3 Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows:

a) Revoke the license from the controller by entering this command:

license revoke *permission_ticket_url*

where *permission_ticket_url* is tftp://*server_ip*/*path*/*filename*.

b) Generate the rehost ticket by entering this command:

license revoke rehost *rehost_ticket_url*

where *rehost_ticket_url* is tftp://*server_ip*/*path*/*filename*.

c) If prompted, read and accept the terms of the End-User License Agreement (EULA).

Step 4 Use the rehost ticket generated in Step 3 to obtain a license installation file, which can then be installed on another controller as follows:

a) Go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet.
b) On the Product License Registration page, click **Upload Rehost Ticket** under Manage Licenses.
c) On the Upload Ticket page, enter the rehost ticket that you generated in Step 3 in the Enter Rehost Ticket text box and click **Continue**.
d) On the Validate Features page, verify that the license information for your controller is correct, enter the rehost quantity, and click **Continue**.
e) On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to use the license, read and accept the conditions of the End-User License Agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.
f) On the Review and Submit page, verify that all information is correct and click **Submit**.
g) When a message appears indicating that the registration is complete, click **Download License**. The rehost license key is e-mailed within 1 hour to the address that you specified.
h) After the e-mail arrives, copy the rehost license key to your TFTP server.
i) Follow the instructions in the Installing a License (GUI), on page 54 section to install this license on another controller.

Step 5 After revoking the license on original controller, correspondent evaluation licence appear with High pritority. Lower the priority of the evaluation license so that the parmanent license is in "In Use" status.

Transferring Licenses to a Replacement Controller after an RMA

Information About Transferring Licenses to a Replacement Controller after an RMA

If you return a Cisco WLC Cisco as part of the Return Material Authorization (RMA) process, you must transfer that controller's licenses within 60 days to a replacement controller that you receive from Cisco.

Because licenses are registered to the serial number of a controller, you can use the licensing portal on Cisco.com to request that the license from your returned controller be revoked and authorized for use on the replacement controller. After your request is approved, you can install the old license on the replacement controller. Any additional ap-count licenses if installed in the returned controller has to be rehosted on the replacement controller. Before you begin, you need the product ID and serial number of both the returned controller and the replacement controller. This information is included in your purchase records.

Note The evaluation licenses on the replacement controller are designed for temporary use and expire after 60 days. To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. If the evaluation licenses expire before you transfer the permanent licenses from your defective controller to your replacement controller, the replacement controller remains up and running using the permanent base license, but access points are no longer able to join the controller.

Transferring a License to a Replacement Controller after an RMA

Step 1 Browse to https://tools.cisco.com/SWIFT/LicensingUI/Quickstart.

Step 2 Log on to the site.

Step 3 In the **Manage** tab, click **Devices**.

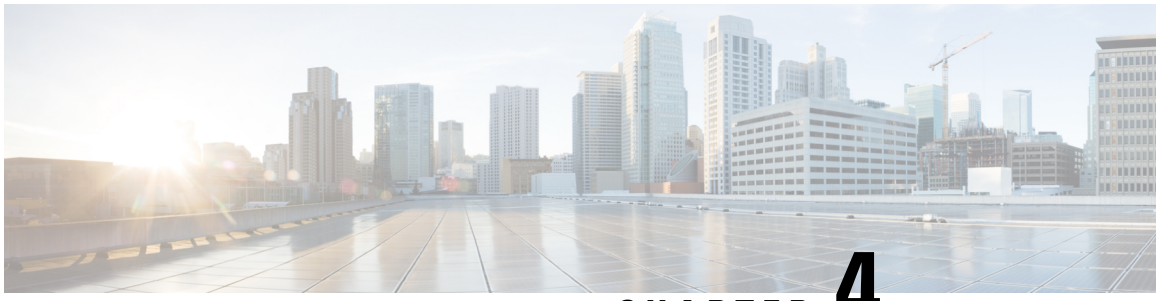
Step 4 Choose **Actions** > **Rehost/Transfer**.

Step 5 Follow the on-screen instructions to generate the license file.

The license is provided online or in an e-mail.

Step 6 Copy the license file to the TFTP server.

Step 7 Install the license by choosing **Management** > **Software Activation** > **Commands** > **Action** > **Install License**.



CHAPTER 4

Configuring 802.11 Bands

- Configuring 802.11 Bands, on page 69
- Configuring Band Selection, on page 72

Configuring 802.11 Bands

802.11 Bands

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

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

Note The Block Acks in a Cisco 2800, 3800, 1560 APs are sent at configured mandatory data rates in controller for 2.4 GHz radio.

This section contains the following subsections:

Configuring the 802.11 Bands (GUI)

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

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

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

Step 4 Specify the period at which the SSID is broadcast by the access point by entering a value between 20 and 1000 milliseconds (inclusive) in the Beacon Period text box. The default value is 100 milliseconds.

Note The beacon period in controllers is listed in terms of milliseconds. The beacon period can also be measured in time units, where one time unit equals 1024 microseconds or 102.4 milliseconds. If a beacon interval is listed as 100 milliseconds in a controller, it is only a rounded off value for 102.4 milliseconds. Due to hardware limitation in certain radios, even though the beacon interval is, say 100 time units, it is adjusted to 102 time units, which roughly equals 104.448 milliseconds. When the beacon period is to be represented in terms of time units, the value is adjusted to the nearest multiple of 17.

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

Step 6 Make access points advertise their channel and transmit power level in beacons and probe responses for CCX clients. Select the **DTPC Support** check box. Otherwise, unselect this check box. The default value is enabled.

Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Note DTPC and 801.11h power constraint cannot be enabled simultaneously.

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

Step 8 Use the Data Rates options to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

- **Mandatory**—Clients must support this data rate in order to associate to an access point on the controller.
- **Supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- **Disabled**—The clients specify the data rates used for communication.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Configuring the 802.11 Bands (CLI)

Step 1 Disable the 802.11a band by entering this command:

config 802.11a disable network

Note The 802.11a band must be disabled before you can configure the 802.11a network parameters in this section.

Step 2 Disable the 802.11b/g band by entering this command:

config 802.11b disable network

Note The 802.11b band must be disabled before you can configure the 802.11b network parameters in this section.

Step 3 Specify the rate at which the SSID is broadcast by the access point by entering this command:

config {**802.11a** | **802.11b**} **beaconperiod** *time_unit*

where *time_unit* is the beacon interval in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.

Step 4 Specify the size at which packets are fragmented by entering this command:

config {**802.11a** | **802.11b**} **fragmentation** *threshold*

where *threshold* is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 5 Make access points advertise their channel and transmit power level in beacons and probe responses by entering this command:

config {**802.11a** | **802.11b** } **dtpc** {**enable** | **disable**}

The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Step 6 Specify the maximum allowed clients that can be configured by entering this command:

config {**802.11a** | **802.11b**} **max-clients** *max_allow_clients*

The valid range is between 1 to 200.

Step 7 Specify the rates at which data can be transmitted between the controller and the client by entering this command:

config {**802.11a** | **802.11b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

where

- **disabled**—Clients specify the data rates used for communication.
- **mandatory**—Clients support this data rate in order to associate to an access point on the controller.
- **supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- *rate*—The rate at which data is transmitted:
  - 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (802.11a)
  - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps (802.11b/g)

Step 8 Enable the 802.11a band by entering this command:

config 802.11a enable network

The default value is enabled.

Step 9 Enable the 802.11b band by entering this command:

config 802.11b enable network

The default value is enabled.

Step 10 Enable or disable 802.11g network support by entering this command:

config 802.11b 11gSupport {**enable** | **disable**}

The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

Step 11 Enter the **save config** command to save your changes.

Step 12 View the configuration settings for the 802.11a or 802.11b/g band by entering this command:

show {**802.11a** | **802.11b**}

Information similar to the following appears:

```
802.11a Network.............................. Enabled
11nSupport................................... Enabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
802.11a Operational Rates
    802.11a 6M Rate.......................... Mandatory
    802.11a 9M Rate.......................... Supported
    802.11a 12M Rate......................... Mandatory
    802.11a 18M Rate......................... Supported
    802.11a 24M Rate......................... Mandatory
    802.11a 36M Rate......................... Supported
    802.11a 48M Rate......................... Supported
    802.11a 54M Rate......................... Supported
...
Beacon Interval.............................. 100
...
Default Channel.............................. 36
Default Tx Power Level....................... 1
DTPC Status.................................. Enabled
Fragmentation Threshold...................... 2346
Maximum Number of Clients per AP............. 200
```

Configuring Band Selection

Band Selection

Band selection enables client radios that are capable of dual-band (2.4 and 5-GHz) operations 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 3 nonoverlapping channels. To prevent

these sources of interference and improve overall network performance, configure band selection on the controller.

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

Note The WMM default configuration is not shown in the **show running-config** command output.

Band Selection Algorithm

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

- Scenario1: Client RSSI (as seen from the **show cont d0/d1** | **begin RSSI**command output) is greater than both Mid RSSI and Acceptable Client RSSI.
  - Dual-band clients: No 2.4-GHz probe responses are seen at any time; 5-GHz probe responses are seen for all 5-GHz probe requests.
  - Single-band (2.4-GHz) clients: 2.4-GHz probe responses are seen only after the probe suppression cycle.
  - After the client's probe count reaches the configured probe cycle count, the algorithm waits for the Age Out Suppression time and then marks the client probe's Active value as 0. Then, the algorithm is restarted.
- Scenario2: Client RSSI (as seen from **show cont d0/d1** | **begin RSSI**) lies between Mid-RSSI and Acceptable Client RSSI.
  - All 2.4-GHz and 5-GHz probe requests are responded to without any restrictions.
  - This scenario is similar to the band select disabled.

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

Restrictions for Band Selection

- Band selection-enabled WLANs do not support time-sensitive applications such as voice and video because of roaming delays.
- Band selection can be used only with Cisco Aironet 1140, 1250, 1260, 1550, 1600, 1800, 2600, 2800, 3500, 3600, 3800 Series APs.

- Mid-RSSI is unsupported on Cisco Aironet 1600 Series APs.
- Band selection is unsupported on Cisco Aironet 1040, OEAP 600 Series APs.
- Band selection is unsupported on Cisco Aironet 1040, OEAP 600 Series APs.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

Configuring Band Selection

Configuring Band Selection (GUI)

Step 1 Choose **Wireless** > **Advanced > Band Select** to open the **Band Select** page.

Step 2 In the **Probe Cycle Count** text box, enter a value between 1 and 10. This cycle count sets the number of 2.4 GHz probe suppression cycles. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 3 In the **Scan Cycle Period Threshold (milliseconds)** text box, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle (i.e. only if the time difference between the successive probe requests is greater than this configured value, then the count value in the band select table increases). The default cycle threshold is 200 milliseconds.

Step 4 In the **Age Out Suppression (seconds)** text box, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g/n clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 5 In the **Age Out Dual Band (seconds)** text box, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 In the **Acceptable Client RSSI (dBm)** text box, enter a value between –20 and –90 dBm. This parameter sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 7 In the **Acceptable Client Mid RSSI (dBm)** text box, enter a value between –20 and –90 dBm. This parameter sets the mid-RSSI, whose value can be used for toggling 2.4 GHz probe suppression based on the RSSI value. The default value is –60 dBm.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Step 10 To enable or disable band selection on specific WLANs, choose **WLANs** > **WLAN ID**. The **WLANs > Edit** page appears.

Step 11 Click the **Advanced** tab.

Step 12 In the **Load Balancing and Band Select** text area, if you want to enable band selection, select the **Client Band Select** check box. If you want to disable band selection, leave the check box unselected. The default value is disabled.

Step 13 Click **Save Configuration**.

Configuring Band Selection (CLI)

Step 1 Set the probe cycle count for band select by entering this command:

config band-select cycle-count *cycle_count*

You can enter a value between 1 and 10 for the *cycle_count* parameter.

Step 2 Set the time threshold for a new scanning cycle period by entering this command:

config band-select cycle-threshold *milliseconds*

You can enter a value for threshold between 1 and 1000 for the *milliseconds* parameter.

Step 3 Set the suppression expire to the band select by entering this command:

config band-select expire suppression *seconds*

You can enter a value for suppression between 10 to 200 for the *seconds* parameter.

Step 4 Set the dual band expire by entering this command:

config band-select expire dual-band *seconds*

You can enter a value for dual band between 10 and 300 for the *seconds* parameter.

Step 5 Set the client RSSI threshold by entering this command:

config band-select client-rssi *client_rssi*

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

Step 6 Set the client mid RSSI threshold by entering this command:

config band-select client-mid-rssi *client_mid_rssi*

You can enter a value for mid RSSI between -20 and -90 for the *client_mid_rssi* parameter.

Step 7 Enter the **save config** command to save your changes.

Step 8 Enable or disable band selection on specific WLANs by entering this command:

config wlan band-select allow {**enable** | **disable**} *wlan_ID*

You can enter a value between 1 and 512 for *wlan_ID* parameter.

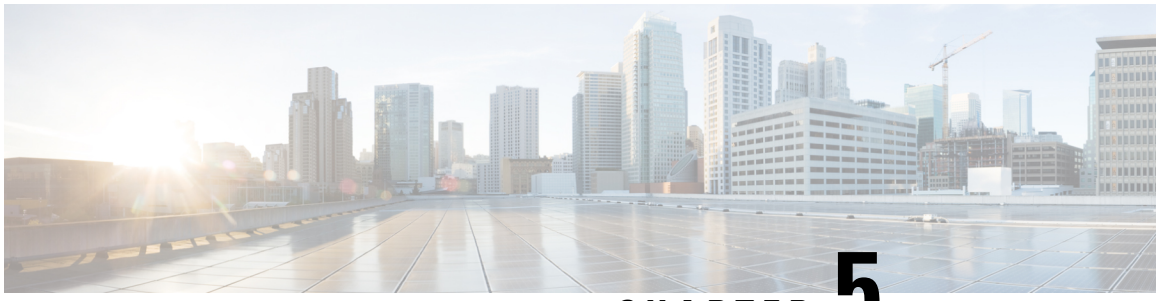
Step 9 Verify your settings by entering this command:

show band-select

Information similar to the following appears:

```
Band Select Probe Response..................... Enabled
   Cycle Count................................. 3 cycles
   Cycle Threshold............................. 300 milliseconds
   Age Out Suppression......................... 20 seconds
   Age Out Dual Band........................... 20 seconds
   Client RSSI................................. -30 dBm
   Client Mid RSSI............................. -80 dBm
```

Step 10 Enter the **save config** command to save your changes.



CHAPTER 5

Configuring 802.11 Parameters

- Configuring the 802.11n Parameters, on page 77
- Configuring 802.11h Parameters, on page 80
- Configuring the 802.11ac Parameters, on page 82

Configuring the 802.11n Parameters

802.11n Parameters

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

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

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

Configuring the 802.11n Parameters (GUI)

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

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

If you want to disable 802.11n mode when both 802.11n and 802.11ac modes are enabled, you must disable the 802.11ac mode first.

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

- 0 (7 Mbps)

- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps)
- 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
- 10 (43 Mbps)
- 11 (58 Mbps)
- 12 (87 Mbps)
- 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)

Any associated clients that support the selected rates may communicate with the access point using those rates. However, the clients are not required to be able to use this rate in order to associate. The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used.

Step 4 Click **Apply**.

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

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

If you choose **Allowed**, devices that cannot support WMM can join the WLAN but will not benefit from the 802.11n rates.

e) Click **Apply**.

Step 6 Click **Save Configuration**.

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

Configuring the 802.11n Parameters (CLI)

Procedure

- Enable 802.11n support on the network by entering this command:

  config {**802.11a** | **802.11b**} **11nsupport** {**enable** | **disable**}

- Specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client by entering this command:

  config {**802.11a** | **802.11b**} **11nsupport mcs tx** {**0-15**} {**enable** | **disable**}

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

  config wlan wmm {**allow** | **disable** | **require**} *wlan_id*

  The **require** parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

  If set to **allow**, devices that cannot support WMM can join the WLAN but do not benefit from 802.11n rates.

- Specify the aggregation method used for 802.11n packets as follows:
  a) Disable the network by entering this command:

     config {**802.11a** | **802.11b**} **disable network**

  b) Specify the aggregation method entering this command:

     config {**802.11a** | **802.11b**} **11nsupport** {**a-mpdu** | **a-msdu**} **tx priority** {**0-7** | **all**} {**enable** | **disable**}

     Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MSDU is performed in hardware and therefore is the default method.

Note For 802.11ac, all packets are A-MPDU. The A-MSDU option does not apply for 802.11ac.

You can specify the aggregation method for various types of traffic from the access point to the clients. This table defines the priority levels (0-7) assigned per traffic type.

Table 3: Traffic Type Priority Levels

User Priority	Traffic Type
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load

User Priority	Traffic Type
5	Video, less than 100-ms latency and jitter
6	Voice, less than 10-ms latency and jitter
7	Network control

You can configure each priority level independently, or you can use the **all** parameter to configure all of the priority levels at once. When you use the **enable** command, the traffic associated with that priority level uses A-MPDU transmission. When you use the **disable** command, the traffic associated with that priority level uses A-MSDU transmission. Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4 and 5 and the rest are disabled. By default, A-MSDU is enabled for all priorities except 6 and 7.

c) Reenable the network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

- Configure the 802.11n-5 GHz A-MPDU transmit aggregation scheduler by entering this command:

  config 802.11{**a** | **b**} **11nsupport a-mpdu tx scheduler** {**enable** | **disable** | **timeout rt** *timeout-value*}

  The timeout value is in milliseconds. The valid range is between 1 millisecond to 1000 milliseconds.
- Configure the guard interval for the network by entering this command:
  config 802.11{**a** | **b**} **11nsupport guard_interval** {**any** | **long**}
- Configure the Reduced Interframe Space (RIFS) for the network by entering this command:

  config 802.11{**a** | **b**} **11nsupport rifs rx** {**enable** | **disable**}
- Save your changes by entering this command:
  save config
- View the configuration settings for the 802.11 networks by entering this command:

  show {**802.11a** | **802.11b**}

Configuring 802.11h Parameters

802.11h Parameters

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

Configuring the 802.11h Parameters (GUI)

Step 1 Disable the 802.11 band as follows:

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

b) Unselect the **802.11a Network Status** check box.

c) Click **Apply**.

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

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

Step 4 In the Channel Switch Announcement area, select the **Channel Announcement** check box if you want the access point to announce when it is switching to a new channel and the new channel number, or unselect this check box to disable the channel announcement. The default value is disabled.

Step 5 If you enabled the channel announcement, the **Channel Quiet Mode** check box appears. Select this check box if you want the access point to stop transmitting on the current channel, or unselect this check box to disable quiet mode. The default value is disabled.

Step 6 Click **Apply**.

Step 7 Reenable the 802.11a band as follows:

a) Choose **Wireless > 802.11a/n/ac > Network** to open the **802.11a Global Parameters** page.
b) Select the **802.11a Network Status** check box.
c) Click **Apply**.

Step 8 Click **Save Configuration**.

Configuring the 802.11h Parameters (CLI)

Step 1 Disable the 802.11a network by entering this command:

config 802.11a disable network

Step 2 Enable or disable an access point to announce when it is switching to a new channel, and the new channel number by entering this command:

config 802.11h channelswitch {**enable** | **disable**} *switch_mode*

Enter either 0 or 1 for the *switch_mode* parameter to specify whether transmissions are restricted until the actual channel switch (0), or are not restricted (1). By default, this feature is in disabled state.

Step 3 Configure a new channel using the 802.11h channel announcement by entering this command:

config 802.11h setchannel channel *channel*

Step 4 Configure the 802.11h power constraint value by entering this command:

config 802.11h powerconstraint *value*

Use increments of 3 dB for the value so that the AP goes down one power level at a time.

Step 5 Reenable the 802.11a network by entering this command:

config 802.11a enable network

Step 6 View the status of the 802.11h parameters by entering this command:

show 802.11h

Information similar to the following appears:

```
Power Constraint.............................. 0
```

```
Channel Switch.................................. Disabled
Channel Switch Mode............................. 0
```

Configuring the 802.11ac Parameters

802.11ac Parameters

The 802.11ac radio module for the Cisco Aironet 3600 Series access point provides enterprise-class reliability and wired-network-like performance. It supports three spatial streams and up to 160 MHz-wide channels for a maximum data rate of 2.5 Gbps.

The 802.11ac radio in slot 2 is a subordinate radio for which you can configure specific parameters. Because the 802.11ac is a subordinate radio, it inherits many properties from the main 802.11a/n radio on slot 1. The parameters that you can configure for the 802.11ac radio are as follows:

- Admin status—Interface status of the radio that you can enable or disable. By default, the Admin status is in an enabled state. If you disable 802.11n, the 802.11ac radio is also disabled.
- Channel width—You can choose the RF channel width as 20 MHz, 40 MHz, 80 MHz, or 160 MHz. If you choose the channel width as 160 MHz, you must enable the 802.11ac mode on the **High Throughput** page.

Note The **11ac Supported** field is a nonconfigurable parameter that appears for the 802.11ac subordinate radio in slot 2.

Note When the Cisco Aironet 3600 Series access point with 802.11ac radio module is in unsupported mode such as Monitor and Sniffer, Admin Status and Channel Width will not be configured.

This section provides instructions to manage 802.11ac devices such as the Cisco Aironet 3600 Series Access Points on your network.

Note For the Cisco Aironet 3600 Series APs:

- With default AP group—Only WLAN IDs 1 to 8 are advertised on the 5-GHz radios; there is no limit on the 2.4-GHz radios.
- With user-defined AP group—Only the first 8 WLAN IDs are advertised on the 5-GHz radios regardless of the ID number; there is no limit on the 2.4-GHz radios.

Changing the 802.11n radio channel also changes the 802.11ac channels.

On the Cisco WLC GUI, the 802.11ac clients that are connected to the 802.11n radio are displayed 802.11an clients, and the 802.11ac clients that are connected to the 802.11ac radio are displayed as 802.11ac clients.

Ensure that your WLAN has WMM enabled and open or WPA2/AES for 802.11ac to be supported. Otherwise, the speed of 802.11ac is not available, even on 802.11ac clients.

For more information about the 802.11ac module on the Cisco Aironet 3600 Series access point, see http://www.cisco.com/c/en/us/products/wireless/aironet-3600-series/relevant-interfaces-and-modules.html.

Restrictions for 802.11ac Support

- The 802.11ac module is supported only on the following access points:
  - 1700
  - 1800
  - 2700
  - 2800
  - 3600
  - 3700
  - 3800
- The 802.11ac module is turned off if the built-in 5-GHz radio is turned off.
- You must ensure that the configuration of the channel, power values, and the mode of the 802.11ac module is the same as those of the built-in 5-GHz radio on the AP. Also, the 802.11ac module serves only 802.11ac clients.
- The 802.11ac module main channel cannot be changed individually.
- This 802.11ac support is applicable only to the following controller platforms:
  - Cisco 2504 WLC
  - Cisco 5508 WLC
  - Cisco 5520 WLC
  - Cisco Flex 7510 WLC
  - Cisco 8510 WLC
  - Cisco 8540 WLC
- Controllers do not support High availability for 802.11ac modules. The 802.11ac configuration (802.11ac Data Rates and 802.11ac Global mode) on the controller is not synchronized with the standby controller. This might result in client throughput fluctuations and reassociations when you explicitly disable those configurations on the active controller.

  In addition, the 802.11ac Global mode configuration controls whether the radio module is enabled. If 802.11ac Global mode is enabled on one controller but not on another, the 802.11ac module might be disabled if the access point associates with a controller on which 802.11ac Global mode is disabled.

- When changing AP from static to auto channel assignment, by default AP moves to best possible bandwidth supported by the radio and a valid channel. Channel number and width assignment may be suboptimal until next DCA cycle gets started.
- SSIDs with TKIP and SSIDs with TKIP+AES are not enabled on the 802.11ac radios. Therefore, all the 5-GHz clients are expected to associate with the 802.11n radios.

Configuring the 802.11ac High-Throughput Parameters (GUI)

Step 1 Choose **Wireless** > **802.11a/n/ac** > **High Throughput (802.11n/ac)**.

Step 2 Check the **11ac mode** check box to enable the 802.11ac support on the network.

Note You can modify the 802.11ac status only if the 802.11n mode is enabled.

Step 3 Check the check boxes of the desired rates to specify the Modulation and Coding Scheme (MCS) rates at which data can be transmitted between the access point and the client.

MCS index 8 and 9 are specific to 802.11ac. Enabling MCS data rate with index 9 automatically enables data rate with MCS index 8. You can enable or disable MCS index 8 only when MCS index 9 is disabled.

Step 4 Save the configuration.

Configuring the 802.11ac High-Throughput Parameters (CLI)

Procedure

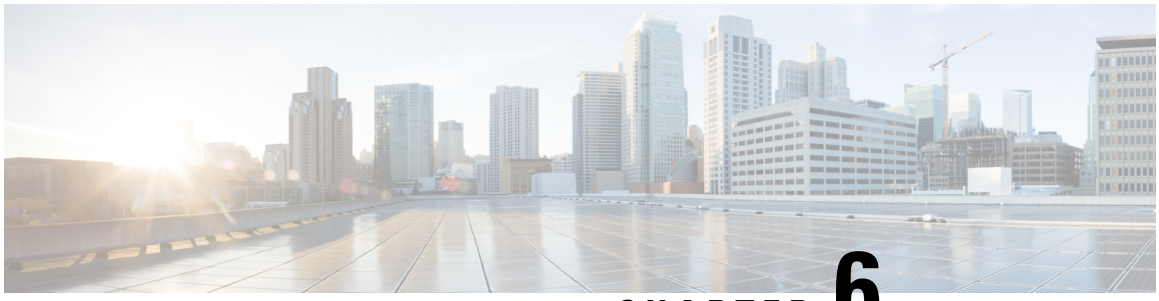
- Enable or disable 802.11ac support by entering this command:

  config 802.11a 11acSupport {**enable** | **disable**}

- Configure MCS transmit rates by entering this command:

  config 802.11a 11acSupport mcs tx {*rate-8* | *rate-9*} **ss** *spatial-stream-value* {**enable** | **disable**}

Note Enabling MCS data rate with MCS index 9 automatically enables data rate with MCS index 8.



CHAPTER 6

Configuring DHCP Proxy

- DHCP Proxy, on page 85
- Restrictions on Using DHCP Proxy, on page 85
- Configuring DHCP Proxy (GUI), on page 86
- Configuring DHCP Proxy (CLI), on page 86
- Configuring a DHCP Timeout (GUI), on page 87
- Configuring a DHCP Timeout (CLI), on page 87

DHCP Proxy

When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

When DHCP proxy is disabled on the controller, those DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the CAPWAP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP tunnel toward the client. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled. The ability to disable DHCP proxy allows organizations to use DHCP servers that do not support Cisco's native proxy mode of operation. It should be disabled only when required by the existing infrastructure.

Note DHCP proxy is enabled by default.

This section contains the following subsections:

Restrictions on Using DHCP Proxy

- DHCP proxy must be enabled in order for DHCP option 82 to operate correctly.
- All controllers that will communicate must have the same DHCP proxy setting.
- DHCP v6 Proxy is not supported.

Configuring DHCP Proxy (GUI)

Step 1 Choose **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page.

Step 2 Select the **Enable DHCP Proxy** check box to enable DHCP proxy on a global basis. Otherwise, unselect the check box. The default value is selected.

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

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

Configuring DHCP Proxy (GUI)

Step 1 Choose **Controller > Interfaces**.

Step 2 Select the interface you want to configure the DHCP proxy.

You can configure the DHCP proxy on the management, virtual, ap manager, or dynamic interfaces in the controller.

The **Interfaces > Edit** page is displayed with DHCP information on the primary and secondary DHCP servers configured in the controller. If the primary and secondary servers are not listed, you must enter values for the IP address of the DHCP servers in the text boxes displayed in this window.

Step 3 Select from the following option of the proxy mode drop-down to enable DHCP proxy on the selected management interface:Global—Uses the global DHCP proxy mode on the controller.Enabled—Enables the DHCP proxy mode on the interface. When you enable DHCP proxy on the controller; the controller unicasts the DHCP requests from the client to the configured servers. You must configure at least one DHCP server on either the interface associated with the WLAN or on the WLAN.Disabled—Disables the DHCP proxy mode on the interface. When you disable the DHCP proxy on the controller, the DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the CAPWAP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP tunnel toward the client. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled.

Step 4 Check the Enable DHCP option 82 checkbox to ensure additional security when DHCP is used to allocate network addresses, check the Enable DHCP option 82 checkbox.

Step 5 Click **Apply** to save the configuration.

Configuring DHCP Proxy (CLI)

Step 1 Enable or disable DHCP proxy by entering this command:

config dhcp proxy {**enable** | **disable**}

Step 2 View the DHCP proxy configuration by entering this command:

show dhcp proxy

Information similar to the following appears:

```
DHCP Proxy Behavior: enabled
```

Configuring DHCP Proxy (CLI)

Step 1 Configure the DHCP primary and secondary servers on the interface. To do this, enter the following commands:

- **config interface dhcp management primary** *primary-server*
- **config interface dhcp dynamic-interface** *interface-name* **primary primary-s**

Step 2 Configure DHCP proxy on the management or dynamic interface of the controller. To do this, enter the following command:

- **config interface dhcp management proxy-mode** enableglobaldisable
- **config interface dhcp dynamic-interface** *interface-name* **proxy-mode** enableglobaldisable.

Note To ensure additional security when DHCP is configured, use the **config interface dhcp***interface type***option-82 enable** command.

Step 3 Enter the **save config** command.

Step 4 To view the proxy settings of the controller interface enter the **show dhcp proxy** command.

Configuring a DHCP Timeout (GUI)

Step 1 Choose **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page.

Step 2 Select the **DHCP Timeout (5 - 120 seconds)** check box to enable a DHCP timeout on a global basis. Otherwise, unselect the check box. The valid range is 5 through 120 seconds.

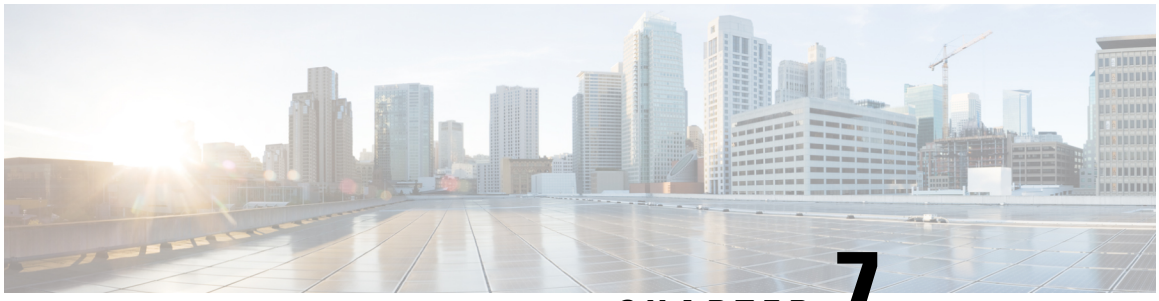
Step 3 Click **Apply** to commit your changes.

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

Configuring a DHCP Timeout (CLI)

Configure a DHCP timeout by entering this command:

config dhcp timeout *seconds*



CHAPTER 7

Configuring SNMP

- Configuring SNMP (CLI), on page 89
- SNMP Community Strings, on page 91
- Configuring Real Time Statistics (CLI), on page 93
- Configuring SNMP Trap Receiver (GUI), on page 94

Configuring SNMP (CLI)

Procedure

- Create an SNMP community name by entering this command:

  config snmp community create *name*
- Delete an SNMP community name by entering this command:

  config snmp community delete *name*
- Configure an SNMP community name with read-only privileges by entering this command:

  config snmp community accessmode ro *name*
- Configure an SNMP community name with read-write privileges by entering this command:

  config snmp community accessmode rw *name*
- For IPv4 configuration—Configure an IPv4 address and subnet mask for an SNMP community by entering this command:

  config snmp community ipaddr *ip-address ip-mask name*

Note This command behaves like an SNMP access list. It specifies the IP address from which the device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address. If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0.0.

Note The controller can use only one IP address range to manage an SNMP community.

- For IPv6 configuration—Configure an IPv6 address and prefix-length for an SNMP community by entering this command:

  config snmp community ipaddr *ipv6-address ip-mask name*
- Enable or disable a community name by entering this command:

  config snmp community mode {**enable** | **disable**}
- Enable or disable a community name by entering this command:

  config snmp community ipsec {**enable** | **disable**}
- Configure the IKE authentication methods by entering this command:

  config snmp community ipsec ike auth-mode {**certificate** | **pre-shared-key** *ascii/hex secret*}

  Authentication mode can be configured per trap receiver. By default, the authentication mode is set to certificate.
- Configure a destination for a trap by entering this command:

  config snmp trapreceiver create *name ip-address*
- Delete a trap by entering this command:

  config snmp trapreceiver delete *name*
- Change the destination for a trap by entering this command:

  config snmp trapreceiver ipaddr *old-ip-address name new-ip-address*
- Configure the trap receiver IPSec session entering this command:

  config snmp trapreceiver ipsec {**enable** | **disable**} *community-name*

  Trap receiver IPSec must be in the disabled state to change the authentication mode.
- Configure the IKE authentication methods by entering this command:

  config snmp trapreceiver ipsec ike auth-mode {**certificate** | **pre-shared-key** *ascii/hex secret community-name*}

  Authentication mode can be configured per trap receiver. By default, the authentication mode is set to certificate.
- Enable or disable the traps by entering this command:

  config snmp trapreceiver mode {**enable** | **disable**}
- Configure the name of the SNMP contact by entering this command:

  config snmp syscontact *syscontact-name*

  Enter up to 31 alphanumeric characters for the contact name.
- Configure the SNMP system location by entering this command:

  config snmp syslocation *syslocation-name*

  Enter up to 31 alphanumeric characters for the location.
- Verify that the SNMP traps and communities are correctly configured by entering these commands:

  show snmpcommunity

show snmptrap

Note Related issue: CSCvr33858.

Read-only community does not get snmpEngineID. As per RFC 2575, the recommendation is such that, some of the OIDs are to be restricted and one of them is SnmpEngineId(engineId). For more information, see https://tools.ietf.org/html/rfc2575.

- See the enabled and disabled trap flags by entering this command:

  show trapflags

  If necessary, use the **config trapflags** command to enable or disable trap flags.

- Configure when the warning message should be displayed after the number of clients or RFID tags associated with the controller hover around the threshold level by entering this command:

  config trapflags {**client** | **rfid**} max-warning-threshold {*threshold-between-80-to-100* | **enable** | **disable**}

  The warning message is displayed at an interval of 600 seconds (10 minutes).

- Configure the SNMP engine ID by entering this command:

  config snmp engineID *engine-id-string*

Note The engine ID string can be a maximum of 24 characters.

- View the engine ID by entering this command:

  show snmpengineID

- Configure the SNMP version by entering this command:

  config snmp version {**v1** | **v2c** | **v3**} {**enable** | **disable**}

SNMP Community Strings

The controller has commonly known default values of "public" and "private" for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. If you use the default community names, and since these are known, the community names could be used to communicate to the controller using SNMP. Therefore, we strongly advise that you change these values.

Changing the SNMP Community String Default Values (GUI)

Step 1 Choose **Management** and then **Communities** under SNMP. The SNMP v1 / v2c Community page appears.

Step 2 If “public” or “private” appears in the Community Name column, hover your cursor over the blue drop-down arrow for the desired community and choose **Remove** to delete this community.

Step 3 Click **New** to create a new community. The SNMP v1 / v2c Community > New page appears.

Step 4 In the Community Name text box, enter a unique name containing up to 16 alphanumeric characters. Do not enter "public" or "private."

Step 5 In the next two text boxes, enter the IPv4/IPv6 address and IP Mask/Prefix Length from which this device accepts SNMP packets with the associated community and the IP mask.

Step 6 Choose **Read Only** or **Read/Write** from the Access Mode drop-down list to specify the access level for this community.

Step 7 Choose **Enable** or **Disable** from the Status drop-down list to specify the status of this community.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your settings.

Step 10 Repeat this procedure if a "public" or "private" community still appears on the SNMP v1 / v2c Community page.

Changing the SNMP Community String Default Values (CLI)

Step 1 See the current list of SNMP communities for this controller by entering this command:

show snmp community

Step 2 If "public" or "private" appears in the SNMP Community Name column, enter this command to delete this community:

config snmp community delete *name*

The *name* parameter is the community name (in this case, "public" or "private").

Step 3 Create a new community by entering this command:

config snmp community create *name*

Enter up to 16 alphanumeric characters for the *name* parameter. Do not enter "public" or "private."

Step 4 For IPv4 specific configuration, enter the IPv4 address from which this device accepts SNMP packets with the associated community by entering this command:

config snmp community ipaddr *ip_address ip_mask name*

Step 5 For IPv6 specific configuration, enter the IPv6 address from which this device accepts SNMP packets with the associated community by entering this command:

config snmp community ipaddr *ip_address prefix_length name*

Step 6 Specify the access level for this community by entering this command, where **ro** is read-only mode and **rw** is read/write mode:

config snmp community accessmode {**ro** | **rw**} *name*

Step 7 Enable or disable this SNMP community by entering this command:

config snmp community mode {**enable** | **disable**} *name*

Step 8 Enable or disable SNMP IPSec sessions for all SNMP communities by entering this command:

config snmp community ipsec {**enable** | **disable**} *name*

By default SNMP IPSec session is disabled. SNMP IPSec session must be disabled state to change the authentication mode.

Step 9 Configure the IKE authentication methods by entering this command:

config snmp community ipsec ike auth-mode {**certificate** | **pre-shared-key** *ascii/hex secret*}

- If authentication mode is configured as pre-shared-key, then enter a secret value. The secret value can either be an ASCII or a hexadecimal value. If auth-mode configured is certificate, then WLC will use the ipsecCaCert and ipsecDevCerts for SNMP over IPSEC.
- If authentication mode is configured as certificate, then controller uses the IPSEC CA and IPSEC device certificates for SNMP sessions. You need to download these certificates to the controller using the **transfer download datatype** {**ipseccacert** | **ipsecdevcert**} command.

Step 10 Save your changes by entering this command:

save config

Step 11 Repeat this procedure if you still need to change the default values for a "public" or "private" community string.

Configuring Real Time Statistics (CLI)

SNMP traps are defined for CPU and memory utilization of AP and controller. The SNMP trap is sent out when the threshold is crossed. The sampling period and statistics update interval can be configured using SNMP and CLI.

Note To get the right value for the current memory usage, you should configure either sampling interval or statistics interval.

- Configure the sampling interval by entering this command:

  config service statistics sampling-interval *seconds*
- Configure the statistics interval by entering this command:

  config service statistics statistics-interval *seconds*
- See sampling and service interval statistics by entering this command:

  show service statistics interval

SNMP Trap Enhancements

This feature provides soaking of SNMP traps and resending of traps after a threshold that you can configure called the hold time. The hold time helps in suppressing false traps being generated. The traps that are supported are for CPU and memory utilization of AP and controller. The retransmission of the trap occurs until the trap is cleared.

Procedure

- Configure the hold time after which the SNMP traps are to be resent by entering this command:

  config service alarm hold-time *seconds*

- Configure the retransmission interval of the trap by entering this command:

  config service alarm trap retransmit-interval *seconds*

- Configure debugging of the traps by entering this command:

  debug service alarm {**enable** | **disable**}

Configuring SNMP Trap Receiver (GUI)

Step 1 Choose **Management** > **SNMP** > **Trap Receivers**.

Step 2 Click **New**.

The **SNMP Trap Receiver > New** page is displayed.

Step 3 In the **SNMP Trap Receiver Name** box, enter the SNMP trap receiver name.

Step 4 In the **IP Address (IPv4/IPv6)** box, enter the IP address of the trap receiver. Both IPv4 and IPv6 address formats are supported.

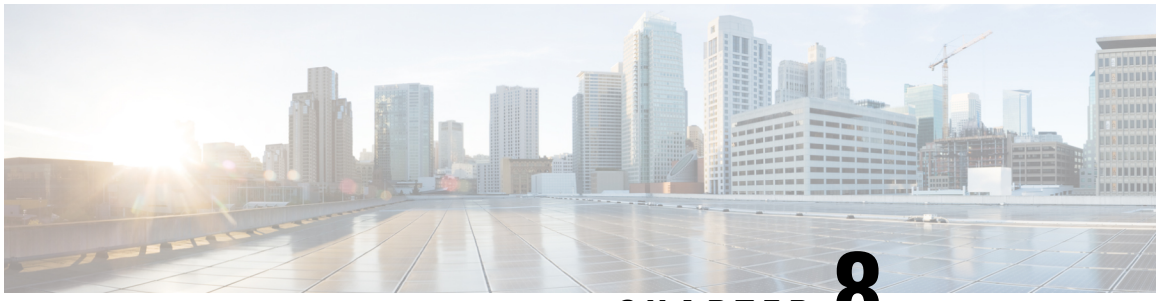
Step 5 From the **Status** drop-down list, choose to **Enable** or **Disable** the trap receiver.

Step 6 Check the **IPSec** check box if you want to enable IPSec parameters for the trap receiver.

Step 7 (Optional) If you enable the IPSec for the trap receiver, choose an **IPSec Profile Name** from the drop-down list.

Step 8 Save the configuration.

You can create a maximum of 6 such SNMP trap receivers.



CHAPTER 8

Configuring Aggressive Load Balancing

- Aggressive Load Balancing, on page 95
- Configuring Aggressive Load Balancing (GUI), on page 96
- Configuring Aggressive Load Balancing (CLI), on page 97

Aggressive Load Balancing

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

Note Clients are load balanced between access points on the same controller. Load balancing does not occur between access points on different controllers.

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

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

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

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

Passive scanning clients will be able to associate to an AP irrespective of whether load balancing is enabled or not.

Note Cisco 600 Series OfficeExtend Access Points do not support client load balancing.

With the 7.4 release, FlexConnect access points do support client load balancing.

You can configure the controller to analyze the WAN interface utilization of neighboring APs and then load balance the clients across the lightly loaded APs. You can configure this by defining a load balancing threshold. By defining the threshold, you can measure the WAN interface utilization percentage. For example, a threshold value of 50 triggers the load balancing upon detecting utilization of 50% or more on an AP-WAN interface.

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

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

This section contains the following subsections:

Configuring Aggressive Load Balancing (GUI)

Step 1 Choose **Wireless** > **Advanced** > **Load Balancing** to open the Load Balancing page.

Step 2 In the Client Window Size text box, enter a value between 1 and 20.

The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing window + client associations on AP with the lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 3 In the Maximum Denial Count text box, enter a value between 0 and 10.

The denial count sets the maximum number of association denials during load balancing.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 To enable or disable aggressive load balancing on specific WLANs, do the following:

a) Choose **WLANs** > **WLAN ID**. The WLANs > Edit page appears.
b) In the **Advanced** tab, select or unselect the **Client Load Balancing** check box.
c) Click **Apply**.

d) Click **Save Configuration**.

Configuring Aggressive Load Balancing (CLI)

Step 1 Set the client window for aggressive load balancing by entering this command:

config load-balancing window *client_count*

You can enter a value between 0 and 20 for the *client_count* parameter.

Step 2 Set the denial count for load balancing by entering this command:

config load-balancing denial *denial_count*

You can enter a value between 1 and 10 for the *denial_count* parameter.

Step 3 Save your changes by entering this command:

save config

Step 4 Enable or disable aggressive load balancing on specific WLANs by entering this command:

config wlan load-balance allow {**enable** | **disable**} *wlan_ID*

You can enter a value between 1 and 512 for *wlan_ID* parameter.

Step 5 Verify your settings by entering this command:

show load-balancing

Step 6 Save your changes by entering this command:

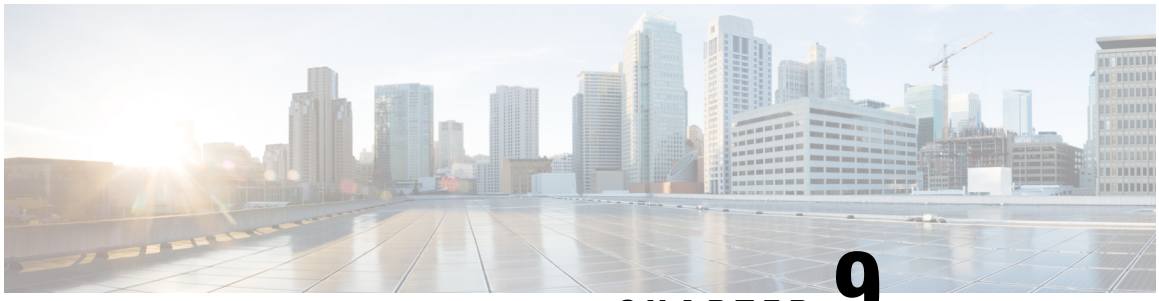
save config

Step 7 Configure the load balance mode on a WLAN by entering this command:

config wlan load-balance mode {*client-count* | *uplink-usage*} *wlan-id*

This feature requires the AP to upload its uplink usage statistics to the controller periodically. Check these statistics by entering this command:

show ap stats system *cisco-AP*



CHAPTER 9

Configuring Fast SSID Changing

- Fast SSID Changing, on page 99
- Configuring Fast SSID Changing (GUI), on page 99
- Configuring Fast SSID Changing (CLI), on page 99

Fast SSID Changing

When fast SSID changing is enabled, the controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced.

When fast SSID changing is disabled, the controller enforces a delay before clients are allowed to move to a new SSID. When fast SSID is disabled and the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID.

This section contains the following subsections:

Configuring Fast SSID Changing (GUI)

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

Step 2 From the Fast SSID Change drop-down list, choose **Enabled** to enable this feature or **Disabled** to disable it. The default value is disabled.

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

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

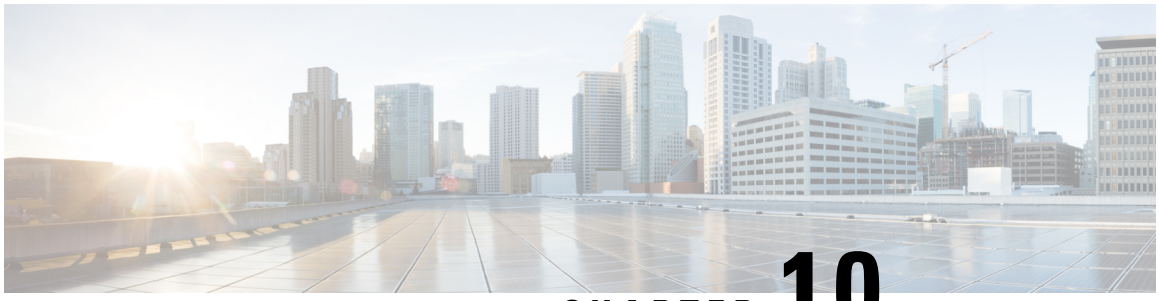
Configuring Fast SSID Changing (CLI)

Step 1 Enable or disable fast SSID changing by entering this command:

config network fast-ssid-change {**enable** | **disable**}

Step 2 Save your changes by entering this command:

save config



CHAPTER 10

Configuring 802.3 Bridging

- Configuring 802.3 Bridging, on page 101
- Enabling 802.3X Flow Control, on page 102

Configuring 802.3 Bridging

802.3 Bridging

The controller supports 802.3 frames and the applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

You can also configure 802.3 bridging using the Cisco Prime Network Control System. See the *Cisco Prime Network Control System Configuration Guide* for instructions.

This section contains the following subsections:

Restrictions on 802.3 Bridging

- Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP.

  The raw 802.3 frame contains destination MAC address, source MAC address, total packet length, and payload.

- By default, Cisco WLCs bridge all non-IPv4 packets (such as AppleTalk, IPv6, and so on). You can also use ACLs to block the bridging of these protocols.

Configuring 802.3 Bridging

Configuring 802.3 Bridging (GUI)

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

Step 2 From the 802.3 Bridging drop-down list, choose **Enabled** to enable 802.3 bridging on your controller or **Disabled** to disable this feature. The default value is Disabled.

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

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

Configuring 802.3 Bridging (CLI)

Step 1 See the current status of 802.3 bridging for all WLANs by entering this command:

show network

Step 2 Enable or disable 802.3 bridging globally on all WLANs by entering this command:

config network 802.3-bridging {**enable** | **disable**}

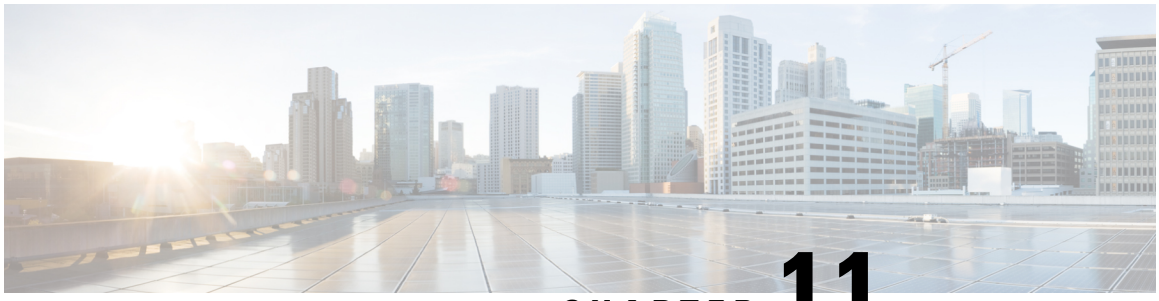
The default value is disabled.

Step 3 Save your changes by entering this command:

save config

Enabling 802.3X Flow Control

802.3X Flow Control is disabled by default. To enable it, enter the **config switchconfig flowcontrol enable** command.



CHAPTER 11

Configuring Multicast

- Configuring Multicast Mode, on page 103
- Configuring Multicast Domain Name System, on page 110
- Multicast Configuration for Cisco vWLC, Flex 7510, 5520, 8510, and 8540 WLCs, on page 120

Configuring Multicast Mode

Multicast/Broadcast Mode

If your network supports packet multicasting, you can configure the multicast method that the controller uses. The controller can perform multicasting in one of two modes:

- Unicast mode—In this mode, the controller unicasts every multicast packet to every access point associated to the controller. This mode is inefficient but might be required on networks that do not support multicasting.
- Multicast mode—In this mode, the controller sends multicast packets to a CAPWAP multicast group. This method reduces overhead on the controller processor and shifts the work of packet replication to your network, which is much more efficient than the unicast method.

Note We recommend that you use the unicast method only in networks where 50 or fewer APs are joined with the controller.

When you enable multicast mode and the controller receives a multicast packet from the wired LAN, the controller encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The controller always uses the management interface for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the interface on which clients receive multicast traffic. From the access point perspective, the multicast appears to be a broadcast to all SSIDs.

The controller supports Multicast Listener Discovery (MLD) v1 snooping for IPv6 multicast. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, you must enable Global Multicast Mode.

Note When you disable the Global Multicast Mode, the controller still forwards the IPv6 ICMP multicast messages, such as router announcements and DHCPv6 solicits, as these are required for IPv6 to work. As a result, enabling the Global Multicast Mode on the controller does not impact the ICMPv6 and the DHCPv6 messages. These messages will always be forwarded irrespective of whether or not the Global Multicast Mode is enabled.

Internet Group Management Protocol (IGMP) snooping is available to better direct multicast packets. When this feature is enabled, the controller gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) from the IGMP reports after selecting the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the infrastructure switch. The controller sends these reports with the source address as the interface address on which it received the reports from the clients. The controller then updates the access point MGID table on the access point with the client MAC address. When the controller receives multicast traffic for a particular multicast group, it forwards it to all the access points, but only those access points that have active clients listening or subscribed to that multicast group send multicast traffic on that particular WLAN. IP packets are forwarded with an MGID that is unique for an ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID that is unique for the ingress interface.

When IGMP snooping is disabled, the following is true:

- The controller always uses Layer 2 MGID when it sends multicast data to the access point. Every interface created is assigned one Layer 2 MGID. For example, the management interface has an MGID of 0, and the first dynamic interface created is assigned an MGID of 8, which increments as each dynamic interface is created.
- The IGMP packets from clients are forwarded to the router. As a result, the router IGMP table is updated with the IP address of the clients as the last reporter.

When IGMP snooping is enabled, the following is true:

- The controller always uses Layer 3 MGID for all Layer 3 multicast traffic sent to the access point. For all Layer 2 multicast traffic, it continues to use Layer 2 MGID.
- IGMP report packets from wireless clients are consumed or absorbed by the controller, which generates a query for the clients. After the router sends the IGMP query, the controller sends the IGMP reports with its interface IP address as the listener IP address for the multicast group. As a result, the router IGMP table is updated with the controller IP address as the multicast listener.
- When the client that is listening to the multicast groups roams from one controller to another, the first controller transmits all the multicast group information for the listening client to the second controller. As a result, the second controller can immediately create the multicast group information for the client. The second controller sends the IGMP reports to the network for all multicast groups to which the client was listening. This process aids in the seamless transfer of multicast data to the client.
- If the listening client roams to a controller in a different subnet, the multicast packets are tunneled to the anchor controller of the client to avoid the reverse path filtering (RPF) check. The anchor then forwards the multicast packets to the infrastructure switch.

Note The MGIDs are controller specific. The same multicast group packets coming from the same VLAN in two different controllers may be mapped to two different MGIDs.

Note If Layer 2 multicast is enabled, a single MGID is assigned to all the multicast addresses coming from an interface.

Note The maximum number of multicast groups supported per VLAN for a controller is 100.

This section contains the following subsections:

Restrictions on Configuring Multicast Mode

- The Cisco Wireless network solution uses some IP address ranges for specific purposes, and you should keep these ranges in mind when configuring a multicast group:
  - 224.0.0.0 through 224.0.0.255—Reserved link local addresses
  - 224.0.1.0 through 238.255.255.255—Globally scoped addresses
  - 239.0.0.0 through 239.255.x.y /16—Limited scope addresses
- When you enable multicast mode on the controller, you must also configure a CAPWAP multicast group address. APs subscribe to the CAPWAP multicast group using IGMP.
- Cisco 1100, 1130, 1200, 1230, and 1240 access points use IGMP versions 1, 2, and 3.
- APs in monitor mode, sniffer mode, or rogue detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the controllers should be different for different controllers.
- Lightweight APs transmit multicast packets at one of the configured mandatory data rates.

  Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell might fail to receive them successfully. If reliable reception is a goal, multicast frames should be transmitted at a low data rate, by disabling the higher mandatory data rates. If support for high data rate multicast frames is required, it might be useful to shrink the cell size and disable all lower data rates, or to use Media Stream.

  Depending on your requirements, you can take the following actions:
  - If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, that is low enough to reach the edges of the wireless cells.
  - If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, you can configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of nonmulticast clients.
  - Configure Media Stream.

- Multicast mode does not operate across intersubnet mobility events such as guest tunneling. It does, however, operate across Layer 3 roams.
- For CAPWAP, the controller drops multicast packets sent to UDP control and data ports 5246 and 5247, respectively. Therefore, you may want to consider not using these port numbers with the multicast applications on your network. We recommend that you do not use any Multicast UDP ports listed in https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113344-cuwn-ppm.html#anc8 as being UDP ports used by the controller.
- We recommend that any multicast applications on your network not use the multicast address configured as the CAPWAP multicast group address on the controller.
- For multicast to work on Cisco 2504 WLC, you have to configure the multicast IP address.
- Multicast mode is not supported on Cisco Flex 7500 Series WLCs.
- We recommend that you do not use Broadcast-Unicast or Multicast-Unicast mode on controller setup where there are more than 50 APs joined.
- While using Local and FlexConnect AP mode the controller's multicast support differs for different platforms.

  The parameters that affect Multicast forwarding are:

  - Controller platform.
  - Global AP multicast mode configuration at controller.
  - Mode of the AP—Local, FlexConnect central switching.
  - For Local switching, it does not send/receive the packet to/from controller, so it does not matter which Multicast mode is configured on the controller.

  Note FlexConnect APs will join the CAPWAP multicast group only if they have centrally switched WLANs. Flex APs with only locally switched WLANs do not join the CAPWAP multicast group.

- Effective with Release 8.2.100.0, it is not possible to download some of the older configurations from the controller because of the Multicast and IP address validations introduced in this release. The platform support for global multicast and multicast mode are listed in the following table.

Table 4: Platform Support for Global Multicast and Multicast Mode

Platform	Global Multicast	Multicast Mode	Supported
Cisco 5520 , 8510, and 8540 Controllers	Enabled	Unicast	No
	Enabled	Multicast	Yes
	Disabled	Unicast	No multicast support (config supported)
	Disabled	Multicast	No mulitcast support (config supported)

Platform	Global Multicast	Multicast Mode	Supported
Cisco Flex 7510 Controller	Global Multicast cannot be enabled. Only Unicast mode is supported. Also, AP-Multicast mode cannot be changed to Multicast-Multicast.		
Cisco 2504 Controller	Only Multicast mode is supported.		
Cisco vWLC	Multicast is not supported; only Unicast mode is supported.		
and Cisco 5508 Controller	Enabled	Unicast	Yes
	Enabled	Multicast	Yes
	Disabled	Unicast	Yes
	Disabled	Multicast	No

- For central switching downstream multicast, AP switching traffic is based on the MGID-to-WLAN mapping (bit map).

Enabling Multicast Mode (GUI)

Step 1 Choose **Controller** > **Multicast** to open the Multicast page.

Step 2 Select the **Enable Global Multicast Mode** check box to configure sending multicast packets. The default value is disabled.

Step 3 If you want to enable IGMP snooping, select the **Enable IGMP Snooping** check box. If you want to disable IGMP snooping, leave the check box unselected. The default value is disabled.

Step 4 To set the IGMP timeout, enter a value between 30 and 7200 seconds in the IGMP Timeout text box. The controller sends three queries in one timeout value at an interval of *timeout*/ 3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Step 5 Enter the IGMP Query Interval (seconds).

Step 6 Select the **Enable MLD Snooping** check box to support IPv6 forwarding decisions.

Note To enable MLD Snooping, you must enable Global Multicast Mode of the controller.

Step 7 In the **MLD Timeout** text box, enter a value between 30 and 7200 seconds to set the MLD timeout.

Step 8 Enter the MLD Query Interval (seconds). The valid range is between 15 and 2400 seconds.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Enabling Multicast Mode (CLI)

Step 1 Enable or disable multicasting on the controller by entering this command:

config network multicast global {**enable** | **disable**}

The default value is disabled.

Note The **config network broadcast** {**enable** | **disable**} command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode currently on the controller to operate.

Step 2 Perform either of the following:

a) Configure the controller to use the unicast method to send multicast and/or broadcast packets by entering this command:

config network multicast mode unicast

b) Configure the controller to use the multicast method to send multicast and/or broadcast packets to a CAPWAP multicast group by entering this command:

config network multicast mode multicast *multicast_group_ip_address*

Step 3 Enable or disable IGMP snooping by entering this command:

config network multicast igmp snooping {**enable** | **disable**}

The default value is disabled.

Step 4 Set the IGMP timeout value by entering this command:

config network multicast igmp timeout *timeout*

You can enter a *timeout* value between 30 and 7200 seconds. The controller sends three queries in one timeout value at an interval of *timeout*/3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Step 5 Enable or disable Layer 2 Multicast by entering this command:

config network multicast l2mcast {**enable** {**all** | *interface-name*} | **disable**}

Step 6 Enable or disable MLD snooping by entering this command:

config network multicast mld snooping {**enable** | **disable**}

The default value is disabled.

Note To enable MLD snooping, you must enable global multicast mode of the controller.

Step 7 Set the MLD timeout value by entering this command:

config network multicast mld timeout *timeout*

Enter the MLD timeout value in seconds. The valid range is between 30 and 7200 seconds.

Step 8 Set the MLD query interval by entering this command:

config network multicast mld query interval *interval*

Enter the MLD query interval value in seconds. The valid range is between 15 and 2400 seconds.

Step 9 Save your changes by entering this command:

save config

Viewing Multicast Groups (GUI)

Step 1 Choose **Monitor > Multicast**. The Multicast Groups page appears.

This page shows all the multicast groups and their corresponding MGIDs.

Step 2 Click the link for a specific MGID (such as MGID 550) to see a list of all the clients joined to the multicast group in that particular MGID.

Viewing Multicast Groups (CLI)

Step 1 See all the multicast groups and their corresponding MGIDs by entering this command:

show network multicast mgid summary

Information similar to the following appears:

```
Layer2 MGID Mapping:
--------------------
InterfaceName                    vlanId   MGID
-------------------------------- ------   ----
management                       0        0
test                             0        9
wired                            20       8

Layer3 MGID Mapping:
--------------------
Number of Layer3 MGIDs........................... 1

 Group address    Vlan  MGID
 ---------------  ----  ----
 239.255.255.250  0     550
```

Step 2 See all the clients joined to the multicast group in a specific MGID by entering this command:

show network multicast mgid detail *mgid_value*

where the *mgid_value* parameter is a number between 550 and 4095.

Information similar to the following appears:

```
Mgid..................................... 550
Multicast Group Address.................. 239.255.255.250
```

```
Vlan.................................... 0
Rx Packet Count......................... 807399588
No of clients........................... 1
Client List.............................
        Client MAC             Expire Time (mm:ss)
        00:13:02:23:82:ad      0:20
```

Viewing an Access Point's Multicast Client Table (CLI)

To help troubleshoot roaming events, you can view an access point's multicast client table from the controller by performing a remote debug of the access point.

Step 1 Initiate a remote debug of the access point by entering this command:

debug ap enable *Cisco_AP*

Step 2 See all of the MGIDs on the access point and the number of clients per WLAN by entering this command:

debug ap command "show capwap mcast mgid all" *Cisco_AP*

Step 3 See all of the clients per MGID on the access point and the number of clients per WLAN by entering this command:

debug ap command "show capwap mcast mgid id *mgid_value***"** *Cisco_AP*

Configuring Multicast Domain Name System

Multicast Domain Name System

Multicast Domain Name System (mDNS) is a protocol used for service discovery by Apple products (called Bonjour) and by Google products (called Chromecast). The mDNS service discovery enables wireless clients to access Apple services such as Apple Printer and Apple TV advertised in a different Layer 3 network. mDNS performs DNS queries over IP multicast. mDNS supports zero-configuration IP networking. As a standard, mDNS uses multicast IP address 224.0.0.251 as the destination address and 5353 as the UDP destination port.

Location Specific Services

The processing of mDNS service advertisements and mDNS query packets support Location-Specific Services (LSS). All the valid mDNS service advertisements that are received by the controller are tagged with the MAC address of the AP that is associated with the service advertisement from the service provider while inserting the new entry into the service provider database. The response formulation to the client query filters the wireless entries in the SP-DB using the MAC address of the AP associated with the querying client. The wireless service provider database entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service. If LSS is disabled for any service, the wireless service provider database entries are not filtered when they respond to any query from a wireless client for the service.

LSS applies only to wireless service provider database entries. There is no location awareness for wired service provider devices.

The status of LSS cannot be enabled for services with ORIGIN set to wired and vice-versa.

mDNS AP

The mDNS AP feature allows the controller to have visibility of wired service providers that are on VLANs that are not visible to the controller. You can configure any AP as an mDNS AP and enable the AP to forward mDNS packets to the controller. VLAN visibility on the controller is achieved by APs that forward the mDNS advertisements to the controller. The mDNS packets between the AP and the controller are forwarded in Control and Provisioning of Wireless Access Points (CAPWAP) data tunnel that is similar to the mDNS packets from a wireless client. Only CAPWAPv4 tunnels are supported. APs can be in either the access port or the trunk port to learn the mDNS packets from the wired side and forward them to the controller.

You can use the configurable knob that is provided on the controller to start or stop mDNS packet forwarding from a specific AP. You can also use this configuration to specify the VLANs from which the AP should snoop the mDNS advertisements from the wired side. The maximum number of VLANs that an AP can snoop is 10.

If the AP is in the access port, you should not configure any VLANs on the AP to snoop. The AP sends untagged packets when a query is to be sent. When an mDNS advertisement is received by the mDNS AP, the VLAN information is not passed on to the controller. The service provider's VLAN that is learned through the mDNS AP's access VLAN is maintained as 0 in the controller.

By default, the mDNS AP snoops in native VLAN. When an mDNS AP is enabled, native VLAN snooping is enabled by default and the VLAN information is passed as 0 for advertisements received on the native VLAN.

The mDNS AP feature is supported only on local mode and monitor mode APs.

The mDNS AP configuration is retained on those mDNS APs even if global mDNs snooping is disabled.

Note There is no check to ensure that no two mDNS APs are duplicating the same traffic for the same service. But, for the same VLAN, there is such a check.

If an mDNS AP is reset or associated with the same controller or another controller, one of the following occurs:

- If the global snooping is disabled on the controller, a payload is sent to the AP to disable mDNS snooping.
- If the global snooping is enabled on the controller, the configuration of the AP before the reset or the association procedure is retained.

The process flow for the mDNS AP feature is as follows:

- Uplink (Wired infrastructure to AP to Controller):
  1. Receives the 802.3 mDNS packet on configured VLANs.
  2. Forwards the received mDNS packet over CAPWAP.
  3. Populates multicast group ID (MGID) based on the received VLAN.
- Downlink (Controller to AP to Wired Infrastructure):
  1. Receives an mDNS query over CAPWAP from the controller.
  2. Forwards the query as 802.3 packet to wired infrastructure.

3. The VLAN is identified from dedicated MGIDs.

Per-Service SP Count Limit

The following list shows the global service provider limit per controller model:

- Cisco 8510 WLC—16000
- Cisco Flex 7510 WLC—16000
- Cisco 5508 WLC—6400
- Cisco 2504 WLC—6400

If the total number of service providers for all services is within the specified limit, any service is free to learn or discover as many other services. There is no per service reservation or restriction, which allows flexibility to accommodate more service providers for any service with respect to other services.

Priority MAC Support

You can configure up to 50 MAC addresses per service; these MAC addresses are the service provider MAC addresses that require priority. This guarantees that any service advertisements originating from these MAC addresses for the configured services are learned even if the service provider database is full by deleting the last nonpriority service provider from the service that has the highest number of service providers. When you configure the priority MAC address for a service, there is an optional parameter called ap-group, which is applicable only to wired service providers to associate a sense of location to the wired service provider devices. When a client mDNS query originates from this ap-group, the wired entries with priority MAC and ap-group are looked up and the wired entries are listed first in the aggregated response.

Origin-Based Service Discovery

You can configure a service to filter inbound traffic that is based on its origin, that is either wired or wireless. All the services that are learned from an mDNS AP are treated as wired. When the learn origin is wired, the LSS cannot be enabled for the service because LSS applies only to wireless services.

A service that has its origin set to wireless cannot be changed to wired if the LSS status is enabled for the service because LSS is applicable only to wireless service provider database. If you change the origin between wired and wireless, the service provider database entries with the prior origin type is cleared.

Related Documentation

- *Cisco Wireless LAN Controller Bonjour Phase IV Deployment Guide*: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/WLAN-Bonjour-DG/WLAN-Bonjour-DG.html
- *mDNS Gateway with Chromecast Support Feature Deployment Guide*: https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_mDNS_gateway_chromecast_support_feature_deployment_guide.html

This section contains the following subsections:

Restrictions for Configuring Multicast DNS

- mDNS over IPv6 is not supported.

- mDNS snooping is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points. For locally switched WLANs, all multicast traffic including mDNS is simply bridged between the local VLAN and the SSID.
- mDNS is not supported on remote LANs.
- mDNS is not supported on Cisco AP1240 and Cisco AP1130.
- Third-party mDNS servers or applications are not supported on the controller using the mDNS feature. Devices that are advertised by the third-party servers or applications are not populated on the mDNS service or device table correctly on the controller.
- The controller prevents addition or modification of the mDNS-profile when any interface is in use by an active WLAN in an AP group. When attempting to make changes to the mDNS profile which is already linked to an active WLAN, the following error message is displayed—**Interface is mapped to an AP Group**.
- mDNS snooping is not necessary in order to forward mDNS multicasts, if the network is configured to forward multicast traffic. However, Apple mDNS (Bonjour) traffic is sent with time to live of 1, so without mDNS snooping, Bonjour will work within a Layer 2 broadcast domain.
- In a large campus network, if multicast forwarding is enabled, it is recommended to enable mDNS snooping, and then disable mDNS on all WLANs, except anywhere mDNS is required. This is in order to prevent Bonjour multicast traffic from overwhelming the network.
- mDNS APs cannot duplicate the same traffic for the same service or VLAN.
- LSS filtering is restricted to only wireless services.
- The LSS, mDNS AP, Priority MAC address, and origin-based discovery features can be configured only using the controller CLI and cannot be configured using the controller GUI.

Configuring Multicast DNS (GUI)

Step 1 Configure the global mDNS parameters and the Master Services Database by following these steps:

a) Choose **Controller** > **mDNS** > **General**.
b) Select or unselect the **mDNS Global Snooping** check box to enable or disable snooping of mDNS packets, respectively.
c) Enter the mDNS query interval in minutes. The query interval is the frequency at which the controller queries for a service.
d) Choose a service from the **Select Service** drop-down list.

Note To add a new mDNS-supported service to the list, choose **Other**. Specify the service name and the service string. The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services Database. The controller can snoop and learn a maximum of 64 services.

e) Select or unselect the **Query Status** check box to enable or disable an mDNS query for a service, respectively.
f) Click **Add**.
g) Click **Apply**.
h) To view the details of an mDNS service, hover your cursor over the blue drop-down arrow of a service, and choose **Details**.

Step 2 Configure an mDNS profile by following these steps:

a) Choose **Controller** > **mDNS** > **Profiles**.

The controller has a default mDNS profile, which is default-mdns-profile. It is not possible to delete the default profile.

b) To create a new profile, click **New**, enter a profile name, and click **Apply**.
c) To edit a profile, click a profile name on the **mDNS Profiles** page; from the **Service Name** drop-down list, choose a service to be associated with the profile, and click **Apply**.

You can add multiple services to a profile.

Step 3 Click **Save Configuration**.

What to do next

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The highest priority is given to the profiles associated with interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

- Map an mDNS profile to an interface group by following these steps:
  1. Choose **Controller** > **Interface Groups**.
  2. Click the corresponding interface group name.

     The **Interface Groups > Edit** page is displayed.
  3. From the **mDNS Profile** drop-down list, choose a profile.

- Map an mDNS profile to an interface by following these steps:
  1. Choose **Controller** > **Interfaces**.
  2. Click the corresponding interface name.

     The **Interfaces > Edit** page is displayed.
  3. From the **mDNS Profile** drop-down list, choose a profile.

- Map an mDNS profile to a WLAN by following these steps:
  1. Choose **WLANs**. click the WLAN ID to open the WLANs > Edit page.
  2. Click the corresponding WLAN ID.

     The **WLANs > Edit** page is displayed.
  3. Click the **Advanced** tab.
  4. Select the **mDNS Snooping** check box.
  5. From the **mDNS Profile** drop-down list, choose a profile.

Note The wireless controller advertises the services from the wired devices (such as Apple TVs) learnt over VLANs, when:

- mDNS snooping is enabled in the WLAN Advanced options.
- mDNS profile is enabled either at interface group (if available), interface, or WLAN.

Configuring Multicast DNS (CLI)

- Configure mDNS snooping by entering this command:

  config mdns snooping {**enable** | **disable**}

- Configure mDNS services by entering this command:

  config mdns service {{**create** *service-name service-string* **origin** {**wireless** | **wired** | **all**} **lss** {**enable** | **disable**} [**query**] [**enable** | **disable**]} | **delete** *service-name*}

- Configure a query for an mDNS service by entering this command:

  config mdns service query {**enable** | **disable**} *service-name*

- Configure a query interval for mDNS services by entering this command:

  config mdns query interval *value-in-minutes*

- Configure an mDNS profile by entering this command:

  config mdns profile {**create** | **delete**} *profile-name*

  Note If you try to delete an mDNS profile that is already associated with an interface group, an interface, or a WLAN, an error message is displayed.

- Configure mDNS services to a profile by entering this command:

  config mdns profile service {**add** | **delete**} *profile-name service-name*

- Map an mDNS profile to an interface group by entering this command:

  config interface group mdns-profile {*interface-group-name* | **all**} {*mdns-profile-name* | **none**}

  Note If the mDNS profile name is **none**, no profiles are attached to the interface group. Any existing profile that is attached is removed.

- View information about an mDNS profile that is associated with an interface group by entering this command:

  show interface group detailed *interface-group-name*

- Map an mDNS profile to an interface by entering this command:

config interface mdns-profile {**management** | {*interface-name* | **all**}} {*mdns-profile-name* | **none**}

- View information about the mDNS profile that is associated with an interface by entering this command:

  show interface detailed *interface-name*

- Configure mDNS for a WLAN by entering this command:

  config wlan mdns {**enable** | **disable**} {*wlan-id* | **all**}

- Map an mDNS profile to a WLAN by entering this command:

  config wlan mdns profile {*wlan-id* | **all**} {*mdns-profile-name* | **none**}

- View information about an mDNS profile that is associated with a WLAN by entering this command:

  show wlan *wlan-id*

- View information about all mDNS profiles or a particular mDNS profile by entering this command:

  show mdns profile {**summary** | **detailed** *mdns-profile-name*}

- View information about all mDNS services or a particular mDNS service by entering this command:

  show mdns service {**summary** | **detailed** *mdns-service-name*}

- View information about the mDNS domain names that are learned by entering this command:

  show mdns domain-name-ip summary

- View the mDNS profile for a client by entering this command:

  show client detail *client-mac-address*

- View the mDNS details for a network by entering this command:

  show network summary

- Clear the mDNS service database by entering this command:

  clear mdns service-database {**all** | *service-name*}

- View events related to mDNS by entering this command:

  debug mdns message {**enable** | **disable**}

- View mDNS details of the events by entering this command:

  debug mdns detail {**enable** | **disable**}

- View errors related to mDNS processing by entering this command:

  debug mdns error {**enable** | **disable**}

- Configure debugging of all mDNS details by entering this command:

  debug mdns all {**enable** | **disable**}

Procedure

- Location Specific Service-related commands:
  - Enable or disable location specific service on a specific mDNS service or all mDNS services by entering this command:

config mdns service lss {**enable** | **disable**} {*service-name* | **all**}

Note By default, LSS is in disabled state.

- View the status of LSS by entering these commands:

  Summary—**show mdns service summary**

  Detailed—**show mdns service detailed** *service-name*

- Configure troubleshooting HA-related mDNS by entering this command:

  debug mdns ha {**enable** | **disable**}

- Origin-based service discovery-related commands:
  - Configure learning of services from wired, wireless, or both by entering this command:

    config mdns service origin {**Wireless** | **Wired** | **All**} {*service-name* | **all**}

    It is not possible to configure wired services if LSS is enabled and vice versa. It is not possible to enable LSS for wired-only service learn origin.

  - View the status of origin-based service discovery by entering this command:

    Summary—**show mdns service summary**

    Detailed—**show mdns service detailed** *service-name*

  - View all the service advertisements that are present in the controller, but not discovered because of restrictions on learning those services, by entering this command:

    show mdns service not-learnt

    Service advertisements across all VLANs and origin types that are not learned are displayed.

- Priority MAC address-related commands:
  - Configure per-service MAC addresses of service-providing devices to ensure that they are snooped and discovered even if the service provider database is full, by entering this command:

    config mdns service priority-mac {**add** | **delete**} *priority-mac-addr service-name* **ap-group** *ap-group-name*

    The optional AP group is applicable only to wired service provider devices to give them a sense of location; these service providers are placed higher in the order than the other wired devices.

  - View the status of Priority MAC address by entering this command:

    Detailed—**show mdns service detailed** *service-name*

- mDNS AP-related commands:
  - Enable or disable mDNS forwarding on an AP that is associated with the controller by entering this command:

    config mdns ap {**enable** | **disable**} {*ap-name* | **all**} **vlan** *vlan-id*

    There is no default mDNS AP. VLAN ID is an optional node.

- Configure the VLAN on which the AP should snoop, and forward the mDNS packets by entering this command:

  config mdns ap vlan {**add** | **delete**} *vlan-id ap-name*

- View all the APs for which mDNS forwarding is enabled by entering this command:

  show mdns ap summary

Bonjour Gateway Based on Access Policy

From 7.4 release WLC supports Bonjour gateway functionality on WLC itself for which you need not even enable multicast on the controller. The WLC explores all Bonjour discovery packets and does not forward them on AIR or Infra network.

Bonjour is Apple's version of Zeroconf - it is Multicast Domain Name System (mDNS) with DNS-SD (Domain Name System-Service Discovery). Apple devices will advertise their services via IPv4 and IPv6 simultaneously (IPv6 link local and Globally Unique). To address this issue controller acts as a Bonjour Gateway. The WLC listens for Bonjour services and by caching those Bonjour advertisements (AirPlay, AirPrint etc) from the source/host e.g. AppleTV and responds to Bonjour clients when they ask/request for a service.

Bonjour gateway has inadequate capabilities to filter cached wired or wireless service instances based on the credentials of the querying client and its location.

Currently the limitations are:

- Location-Specific Services (LSS) filters the wireless service instances only while responding to a query from wireless clients. The filtering is based on the radio neighborhood of the querying client.
- LSS cannot filter wired service instance because of no sense of location.
- LSS filtering is per service type and not per client. It means that all clients receive the location based filtered response if LSS is enabled for the service type and clients cannot override the behavior.
- There is no other filtering mechanism based on client role or user-id.

The requirement is to have configuration per service instance.

Following are the three criteria of the service instance sharing:

- User-id
- Client-role
- Client location

The configuration can be applied to wired and wireless service instances. The response to any query is on the policy configured for each service instance. The response enables the selective sharing of service instances based on the location, user-id or role.

As the most service publishing devices are wired, the configuration allows filtering of wired services at par with the wireless service instances.

There are two levels of filtering client queries:

1. At the service type level by using the mDNS profile
2. At the service instance level using the access policy associated with the service.

Restrictions on Bonjour Gateway Based on Access Policy

- The total number of policies that can be created is same as the number of service instances that are supported on the platform. Hundred policies can be supported; 99 policies and one default policy.
- The number of rules per policy is limited to one.
- Policy and rules can be created irrespective of the service instances. The policy is applied only when it is complete and discovers the target service instances.
- A service instance can be associated with a maximum of five policies.
- Five service groups can be assigned for a MAC address.

Creating Bonjour Access Policy through Prime Infrastructure

The admin user can create the Bonjour access policy using the GUI of the Prime Infrastructure (PI).

Step 1 Log in to the Cisco Prime Infrastructure using the Admin credentials.

Step 2 Choose **Administration** > **AAA** > **Users** > **Add User**.

Step 3 Choose **mDNS Policy Admin**.

Step 4 Add or remove the devices in the mDNS Device Filter. Click **Save**.

Step 5 Add the users for a device in the Users list dialog box. Click **Save**.

Note See Cisco Prime Infrastructure Administrator Guide for the release 2.2 for more details.

Configuring mDNS Service Groups (GUI)

Step 1 Choose **Controller** > **mDNS** > **mDNS Policies**.

Step 2 Select service group from the list of Group Names.

Step 3 Under Service Instance List perform the following steps:

a) Enter the service provider MAC address in MAC address.

b) Enter the name of service provider in **Name**. Click **Add**.

c) From the **Location Type** drop-down list, choose the type of location.

Note If the location is selected as 'Any', the policy checks on the location attribute are not performed.

In the case of mDNS policy filtered by AP groups, the design is for substring match. The policy is applied on the first substring match.

Note The list of current service instances associated with the service group is shown in a table.

Step 4 Under **Policy / Rule** enter the role names and the user names as the criteria of enforcing the policy.

Configuring mDNS Service Groups (CLI)

Step 1 Enable or disable the mDNS policy by entering this command: **config mdns policy enable | disable**

Step 2 Create or delete a mDNS policy service group by entering this command: **config mdns policy service-group create | delete** <*service-group-name*>

Step 3 Configure the parameters of a service group by entering this command: **config mdns policy service-group device-mac add** <*service-group-name*> <*mac-addr*> <*device name*> **location-type** *[<AP_LOCATION | AP_NAME | AP_GROUP>]* **device-location** *[<location string | any | same>]*

Step 4 Configure the user role for a service-group by entering this command: **config mdns policy service-group user-role add | delete** <*service-group-name*> <*user-role-name*>

Step 5 Configure the user name for a service-group by entering this command: **config mdns policy service-group user-name add | delete** <*service-group-name*> <*user-name*>

Multicast Configuration for Cisco vWLC, Flex 7510, 5520, 8510, and 8540 WLCs

Switching from Multicast-Unicast Mode to Multicast-Multicast Mode

Step 1 Assign both IPv4 and IPv6 (required only if IPv6 is enabled) multicast addresses by entering this command:

a) **config network multicast mode multicast** *IPv4-multicast-address*

b) **config ipv6 multicast mode multicast** *IPv6-multicast-address*

Step 2 Enable global multicast by entering this command:

config network multicast global enable

Switching from Multicast-Multicast Mode to Multicast-Unicast Mode

Step 1 Disable global multicast by entering this command:

config network multicast global disable

Step 2 Configure the Multicast-Unicast mode by entering this command (IPv6 configuration is required only when IPv6 is enabled):

a) **config network multicast mode unicast**

b) **config ipv6 multicast mode unicast**

Restrictions

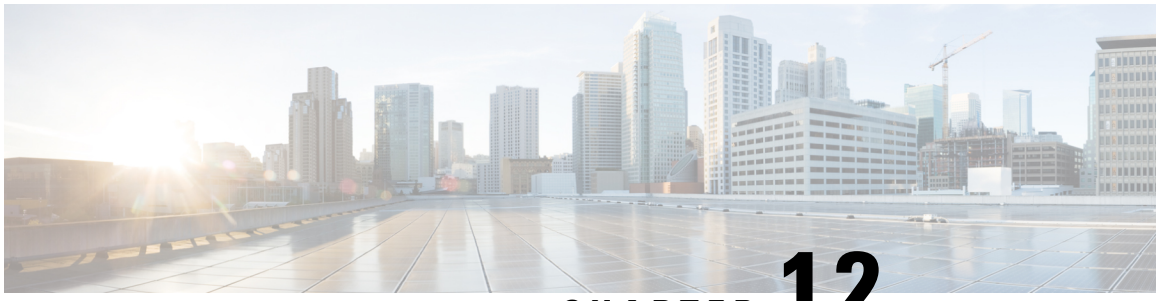
- We recommend that you do not switch from Multicast-Multicast mode to Multicast-Unicast mode on a loaded network because it can burden the network. We recommend that you use Multicast-Multicast mode on these platforms because of the scale factor.
- IGMP and MLD snooping cannot be enabled unless global multicast is enabled, and multicast mode is Multicast-Multicast.
- Global multicast can be enabled only when Multicast-Multicast mode is configured.
- Switching from Multicast-Multicast mode to Multicast-Unicast mode is not allowed if the global multicast is enabled. You must disable global multicast before switching the mode in this case.
- FlexConnect APs:
  - Can join in Multicast-Multicast mode from Release 8.0 onwards.
  - Multicast-Unicast mode has to be enabled if IPv6 support is required on FlexConnect APs by the central-switching clients. Therefore, IGMP or MLD snooping is not supported.
  - VideoStream is not supported because it requires IGMP or MLD snooping.

Troubleshooting

Unable to switch to Multicast-Multicast mode as Global Multicast is not getting enabled

Possible issue—IPv6 is configured but not in use. Check if IPv6 is still in Multicast-Unicast mode.

Solution—Disable IPv6 if it is not being used or switch Multicast-Unicast to Multicast-Multicast mode for IPv6.



CHAPTER 12

Configuring Client Roaming

- Information About Client Roaming, on page 123
- Restrictions for Client Roaming, on page 125
- Configuring CCX Client Roaming Parameters (GUI), on page 125
- Configuring CCX Client Roaming Parameters (CLI), on page 126
- Obtaining CCX Client Roaming Information (CLI), on page 126
- Debugging CCX Client Roaming Issues (CLI), on page 127

Information About Client Roaming

The Cisco UWN solution supports seamless client roaming across lightweight access points managed by the same controller, between controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on different subnets. Also, in controller software release 4.1 or later releases, client roaming with multicast packets is supported.

You can adjust the default RF settings (RSSI, hysteresis, scan threshold, and transition time) to fine-tune the operation of client roaming using the controller GUI or CLI.

Inter-Controller Roaming

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

Intra-Controller Roaming

Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address. The controller provides DHCP functionality with a relay function. Same-controller roaming is supported in single-controller deployments and in multiple-controller deployments.

Inter-Subnet Roaming

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

Voice-over-IP Telephone Roaming

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

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

CCX Layer 2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements:

- Access point assisted roaming—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.
- Enhanced neighbor list—This feature focuses on improving a CCXv4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.
- Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.

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

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

This section contains the following subsections:

Restrictions for Client Roaming

- CCX versions 1 through 5 are supported. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) in order to utilize these roaming enhancements.

  The roaming enhancements mentioned above are enabled automatically, with the appropriate CCX support.
- FlexConnect access points in standalone mode do not support CCX Layer 2 roaming.
- Client roaming between Cisco 600 Series OEAPs is not supported.
- Seamless L2 and L3 roaming is not supported between a Cisco and a third-party wireless infrastructure, which also includes a Cisco IOS access point.

Configuring CCX Client Roaming Parameters (GUI)

Step 1 Choose **Wireless** > **802.11a/n/ac or 802.11b/g/n** > **Client Roaming**. The 802.11a (802.11b) > Client Roaming page appears.

Step 2 If you want to fine-tune the RF parameters that affect client roaming, choose **Custom** from the **Mode** drop-down list and go to *Step 3*. If you want to leave the RF parameters at their default values, choose **Default** and go to *Step 8*.

Step 3 In the **Minimum RSSI** text box, enter a value for the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

The range is –90 to –50 dBm.

The default is –85 dBm.

Step 4 In the **Hysteresis** text box, enter a value to indicate how much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.

The range is 3 to 20 dB.

The default is 3 dB.

Step 5 In the **Scan Threshold** text box, enter the minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold.

The range is –90 to –50 dBm.

The default is –72 dBm.

Step 6 In the **Transition Time** text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

The range is 1 to 5 seconds.

The default is 5 seconds.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Step 9 Repeat this procedure if you want to configure client roaming for another radio band.

Configuring CCX Client Roaming Parameters (CLI)

Configure CCX Layer 2 client roaming parameters by entering this command:

config {**802.11a** | **802.11b**} **l2roam rf-params** {**default** | **custom** *min_rssi roam_hyst scan_thresh trans_time*}

Obtaining CCX Client Roaming Information (CLI)

Step 1 View the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network by entering this command:

show {**802.11a** | **802.11b**} **l2roam rf-param**

Step 2 View the CCX Layer 2 client roaming statistics for a particular access point by entering this command:

show {**802.11a** | **802.11b**} **l2roam statistics** *ap_mac*

This command provides the following information:

- The number of roam reason reports received
- The number of neighbor list requests received
- The number of neighbor list reports sent
- The number of broadcast neighbor updates sent

Step 3 View the roaming history for a particular client by entering this command:

show client roam-history *client_mac*

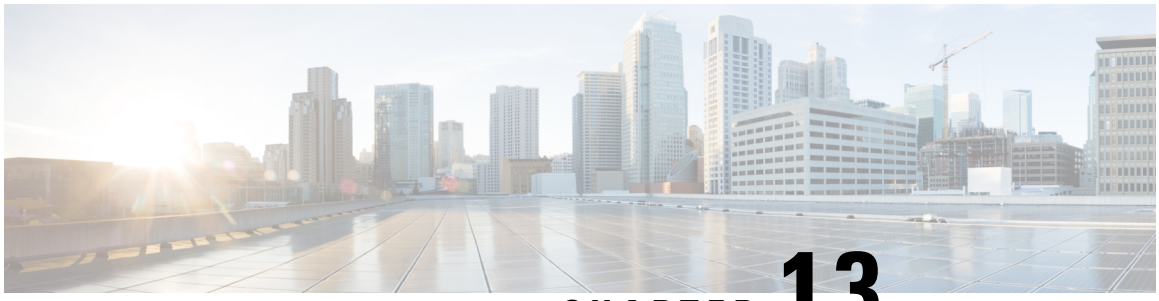
This command provides the following information:

- The time when the report was received
- The MAC address of the access point to which the client is currently associated
- The MAC address of the access point to which the client was previously associated
- The channel of the access point to which the client was previously associated
- The SSID of the access point to which the client was previously associated
- The time when the client disassociated from the previous access point
- The reason for the client roam

Debugging CCX Client Roaming Issues (CLI)

If you experience any problems with CCX Layer 2 client roaming, enter this command:

debug l2roam [**detail** | **error** | **packet** | **all**] {**enable** | **disable**}



CHAPTER 13

Configuring IP-MAC Address Binding

- IP-MAC Address Binding, on page 129
- Configuring IP-MAC Address Binding (CLI), on page 129

IP-MAC Address Binding

The controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. The controller checks only the MAC address of the client and ignores the IP address. Disable IP-MAC Address Binding if you have a wireless client that has multiple IP addresses mapped to the same MAC address. Examples include a PC running a VM software in Bridge mode, or a third-party WGB.

You must disable IP-MAC address binding to use an access point in sniffer mode if the access point is associated with a Cisco 2504 Wireless Controller, a Cisco 5508 Wireless Controller, or a controller network module. To disable IP-MAC address binding, enter the **config network ip-mac-binding disable**.

WLAN must be enabled to use an access point in sniffer mode if the access point is associated with a Cisco 2504 Wireless Controller, a Cisco 5508 Wireless Controller, or a controller network module. If WLAN is disabled, the access point cannot send packets.

Note If the IP address or MAC address of the packet has been spoofed, the check does not pass, and the controller discards the packet. Spoofed packets can pass through the controller only if both the IP and MAC addresses are spoofed together and changed to that of another valid client on the same controller.

This section contains the following subsection:

Configuring IP-MAC Address Binding (CLI)

Step 1 Enable or disable IP-MAC address binding by entering this command:

config network ip-mac-binding {**enable** | **disable**}

The default value is enabled.

Note You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

Note You must disable this binding check in order to use an access point in sniffer mode if the access point is joined to a Cisco 5508 WLC.

Step 2 Save your changes by entering this command:

save config

Step 3 View the status of IP-MAC address binding by entering this command:

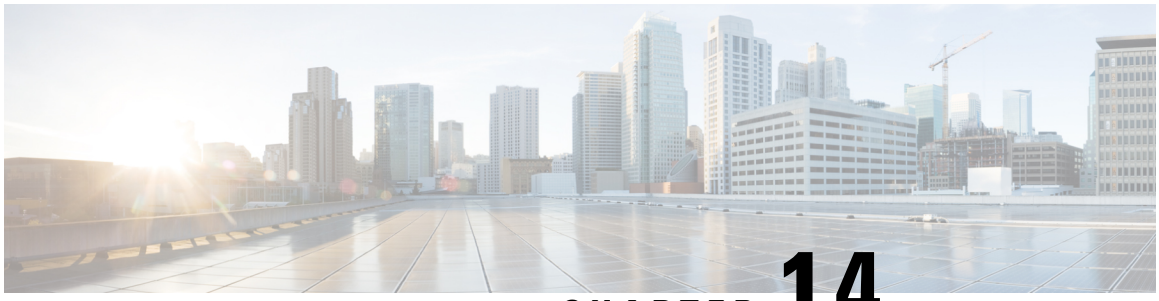
show network summary

Information similar to the following appears:

```
RF-Network Name............................. ctrl4404
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
...
```

IP/MAC Addr Binding Check ..... Enabled

```
...<?Line-Break?><?HardReturn?>
```



CHAPTER 14

Configuring Quality of Service

- Configuring Quality of Service, on page 131
- Configuring Quality of Service Roles, on page 135

Configuring Quality of Service

Quality of Service

Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.

The controller supports four QoS levels:

- Platinum/Voice—Ensures a high quality of service for voice over wireless.
- Gold/Video—Supports high-quality video applications.
- Silver/Best Effort—Supports normal bandwidth for clients. This is the default setting.
- Bronze/Background—Provides the lowest bandwidth for guest services.

Note VoIP clients should be set to Platinum.

You can configure the bandwidth of each QoS level using QoS profiles and then apply the profiles to WLANs. The profile settings are pushed to the clients associated to that WLAN. In addition, you can create QoS roles to specify different bandwidth levels for regular and guest users. Follow the instructions in this section to configure QoS profiles and QoS roles. You can also define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN.

The wireless rate limits can be defined on both upstream and downstream traffic. Rate limits can be defined per SSID and/or specified as a maximum rate limit for all clients. These rate limits can be individually configured.

This section contains the following subsections:

Configuring Quality of Service Profiles

You can configure the Platinum, Gold, Silver, and Bronze QoS profiles.

Configuring QoS Profiles (GUI)

Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles.

To disable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 2 Choose **Wireless > QoS > Profiles** to open the **QoS Profiles** page.

Step 3 Click the name of the profile that you want to configure to open the Edit QoS Profile page.

Step 4 Change the description of the profile by modifying the contents of the Description text box.

Step 5 Define the data rates on a per-user basis as follows:

a) Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Ensure that you configure the average data rate before you configure the burst data rate.

c) Define the average real-time rate for UDP traffic per user by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

d) Define the peak real-time rate for UDP traffic per user by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 6 Define the data rates on a per-SSID basis as follows:

a) Define the average data rate TCP traffic per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic in the WLANs.

c) Define the average real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

d) Define the peak real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic in the WLANs.

Step 7 Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN.

a) From the Maximum Priority drop-down list, choose the maximum QoS priority for any data frames transmitted by the AP to any station in the WLAN.

For example, a QoS profile named 'gold' targeted for video applications has the maximum priority set to video by default.

b) From the Unicast Default Priority drop-down list, choose the QoS priority for unicast data frames transmitted by the AP to non-WMM stations in the WLAN

c) From the Multicast Default Priority drop-down list, choose the QoS priority for multicast data frames transmitted by the AP to stations in the WLAN,

Note The default unicast priority cannot be used for non-WMM clients in a mixed WLAN.

Step 8 Choose **802.1p** from the Protocol Type drop-down list and enter the maximum priority value in the 802.1p Tag text box to define the maximum value (0–7) for the priority tag associated with packets that fall within the profile.

The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Note If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Step 11 Reenable the 802.11 networks.

To enable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 12 Choose **WLANs** and select a WLAN ID to apply the new QoS profile to it.

Step 13 In the **WLAN > Edit** page, go to the **QoS** tab and select the QoS Profile type from the Quality of Service drop-down list. The QoS profile will add the rate limit values configured on the controller on per WLAN, per radio and per AP basis.

For example, if upstream rate limit of 5Mbps is configured for a QoS profile of type silver, then every WLAN that has silver profile will limit traffic to 5Mbps (5Mbps for each wlan) on each radio and on each AP where the WLAN is applicable.

Step 14 Click **Apply**.

Step 15 Click **Save Configuration**.

Configuring QoS Profiles (CLI)

Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:

config 802.11{a | b} disable network

Step 2 Change the profile description by entering this command:

config qos description {**bronze** | **silver** | **gold** | **platinum** }*description*

Step 3 Define the average data rate for TCP traffic per user or per SSID by entering this command:

config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Note For the *rate* parameter, you can enter a value between 0 and 512,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Step 4 Define the peak data rate for TCP traffic per user or per SSID by entering this command:

config qos burst-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 5 Define the average real-time data rate for UDP traffic per user or per SSID by entering this command:

config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 6 Define the peak real-time data rate for UDP traffic per user or per SSID by entering this command:

config qos burst-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 7 Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN by entering this command:

config qos priority {**bronze** | **gold** | **platinum** | **silver**} {*maximum priority*} {*default unicast priority*} {*default multicast priority*}

You choose from the following options for the *maximum priority*, *default unicast priority*, and *default multicast priority* parameters:

- besteffort
- background
- video
- voice

Step 8 Define the maximum value (0–7) for the priority tag associated with packets that fall within the profile, by entering these commands:

config qos protocol-type {**bronze** | **silver** | **gold** | **platinum**} **dot1p**

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *tag*

The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Note The 802.1p tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for a QoS profile.

Note If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 9 Reenable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:

config 802.11{a | b} enable network

Step 10 Apply the new QoS profile to a WLAN, by entering these commands:
config wlan qos <WLAN ID> {bronze | silver | gold | platinum}

Configuring Quality of Service Roles

Quality of Service Roles

After you configure a QoS profile and apply it to a WLAN, it limits the bandwidth level of clients associated to that WLAN. Multiple WLANs can be mapped to the same QoS profile, which can result in bandwidth contention between regular users (such as employees) and guest users. In order to prevent guest users from using the same level of bandwidth as regular users, you can create QoS roles with different (and presumably lower) bandwidth contracts and assign them to guest users.

You can configure up to ten QoS roles for guest users.

Note If you choose to create an entry on the RADIUS server for a guest user and enable RADIUS authentication for the WLAN on which web authentication is performed rather than adding a guest user to the local user database from the controller, you need to assign the QoS role on the RADIUS server itself. To do so, a "guest-role" Airespace attribute called the *Airespace-Guest-Role-Name* with the attribute identifier value of 11 and the datatype of string, which should match the name of the "guest-role" configured on the controller, needs to be added on the RADIUS server. This attribute is sent to the controller when authentication occurs. If a role with the name returned from the RADIUS server is found configured on the controller, the bandwidth associated with that role is enforced for the guest user after authentication completes successfully.

Ensure that the Layer 3 security of *Web Policy* is configured on the WLAN before the AAA parameter is processed by the controller. If the WLAN does not have a Layer 3 Security of *Web Policy*, the AAA parameter is ignored.

This section contains the following subsections:

Configuring QoS Roles

Configuring QoS Roles (GUI)

Step 1 Choose **Wireless** > **QoS** > **Roles** to open the QoS Roles for the Guest Users page.

This page shows any existing QoS roles for guest users.

Note If you want to delete a QoS role, hover your cursor over the blue drop-down arrow for that role and choose **Remove**.

Step 2 Click **New** to create a new QoS role. The **QoS Role Name > New** page appears.

Step 3 In the **Role Name** text box, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on).

Step 4 Click **Apply**.

Step 5 Click the name of the QoS role to edit the bandwidth of a QoS role. The **Edit QoS Role Data Rates** page appears.

Note The values that you configure for the per-user bandwidth contracts affect only the amount of bandwidth going downstream (from the access point to the wireless client). They do not affect the bandwidth for upstream traffic (from the client to the access point).

Note The Access Points that support per-user bandwidth contracts for upstream (from the client to the access point) are - AP1140, AP1040, AP3500, AP3600, AP1250, and AP1260.

Step 6 Define the average data rate for TCP traffic on a per-user basis by entering the rate in Kbps in the **Average Data Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 7 Define the peak data rate for TCP traffic on a per-user basis by entering the rate in Kbps in the Burst Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Ensure that you configure the average data rate before you configure the burst data rate.

Step 8 Define the average real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the **Average Real-Time Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 9 Define the peak real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the **Burst Real-Time Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Step 12 Apply a QoS role to a guest user by following the instructions in the Configuring Local Network Users for the Controller (GUI) section.

Configuring QoS Roles (CLI)

Step 1 Create a QoS role for a guest user by entering this command:

config netuser guest-role create *role_name*

Note If you want to delete a QoS role, enter the **config netuser guest-role delete** *role_name* command.

Step 2 Configure the bandwidth contracts for a QoS role by entering these commands:

- **config netuser guest-role qos data-rate average-data-rate** *role_name rate*—Configures the average data rate for TCP traffic on a per-user basis.
- **config netuser guest-role qos data-rate burst-data-rate** *role_name rate*—Configures the peak data rate for TCP traffic on a per-user basis.

  Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

- **config netuser guest-role qos data-rate average-realtime-rate** *role_name rate*—Configures the average real-time rate for UDP traffic on a per-user basis.
- **config netuser guest-role qos data-rate burst-realtime-rate** *role_name rate*—Configures the peak real-time rate for UDP traffic on a per-user basis.

  Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

  Note For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 3 Apply a QoS role to a guest user by entering this command:

config netuser guest-role apply *username role_name*

For example, the role of *Contractor* could be applied to guest user *jsmith*.

Note If you do not assign a QoS role to a guest user, the Role text box in the User Details shows the role as "default." The bandwidth contracts for this user are defined in the QoS profile for the WLAN.

Note If you want to unassign a QoS role from a guest user, enter the **config netuser guest-role apply** *username* **default command**. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

Step 4 Save your changes by entering this command:

save config

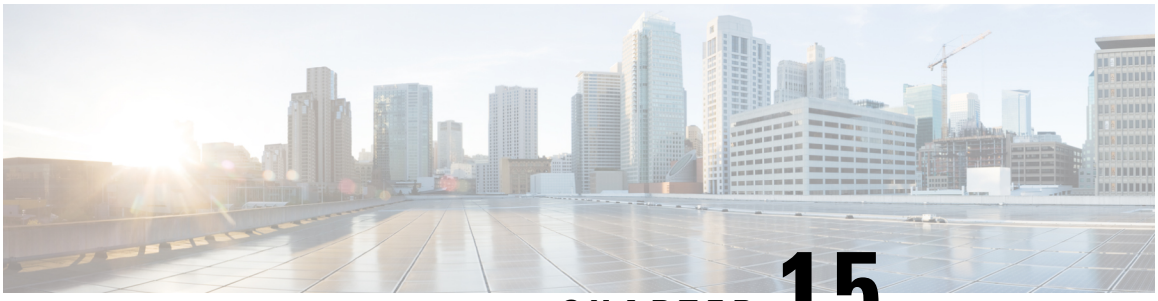
Step 5 See a list of the current QoS roles and their bandwidth parameters by entering this command:

show netuser guest-roles

Information similar to the following appears:

```
Role Name..................................... Contractor
     Average Data Rate........................ 10
     Burst Data Rate.......................... 10
     Average Realtime Rate.................... 100
     Burst Realtime Rate...................... 100

Role Name..................................... Vendor
     Average Data Rate........................ unconfigured
     Burst Data Rate.......................... unconfigured
```

```
Average Realtime Rate..................... unconfigured
Burst Realtime Rate..................... unconfigured
```



CHAPTER 15

Configuring Application Visibility and Control

- Application Visibility and Control, on page 139
- Restrictions for Application Visibility and Control, on page 140
- Configuring Application Visibility and Control (GUI), on page 141
- Configuring Application Visibility and Control (CLI), on page 142
- Configuring NetFlow, on page 143

Application Visibility and Control

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

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

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

AVC DSCP marks only the DSCP of the original packet in the controller in both directions (upstream and downstream). It does not affect the outer CAPWAP DCSP. AVC DSCP is applicable only when the application is classified. For example, based on the AVC profile configuration, if an application is classified as ftp or http, the corresponding DSCP marking is applied irrespective of the WLAN QoS. For downstream, the DSCP value of outer CAPWAP header and inner packet's DSCP are taken from AVC DSCP. WLAN QoS is only applicable for all traffic from WLC to AP through CAPWAP. It does not change the DSCP of the original packet.

Using AVC rule, you can limit the bandwidth of a particular application for all the clients joined on the WLAN. These bandwidth contracts coexist with per-client downstream rate limiting with per client downstream rate limits that takes precedence over the per-application rate limits.

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

AVC is supported in central switching mode on the following controller platforms: Cisco 2504 WLCs, Cisco 5508 WLCs, Cisco Flex 7510 WLCs, Cisco 8510 WLCs, and Cisco Wireless Services Module 2 (WiSM2).

The number of concurrent flows supported for AVC classification on different controller platforms are noted in the following table.

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

Application Visibility and Control Protocol Packs

Protocol packs are a means to distribute protocol updates outside the controller software release trains, and can be loaded on the controller without replacing the controller software.

The Application Visibility and Control Protocol Pack (AVC Protocol Pack) is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. A set of required protocols can be loaded, which helps AVC to recognize additional protocols for classification on your network. The manifest file gives information about the protocol pack, such as the protocol pack name, version, and some information about the available PDLs in the protocol pack.

The AVC Protocol Packs are released to specific AVC engine versions. You can load a protocol pack if the engine version on the controller platform is the same or higher than the version required by the protocol pack.

This section contains the following subsections:

Restrictions for Application Visibility and Control

- IPv6 packet classification is not supported.
- Layer 2 roaming is not supported across controllers.
- Multicast traffic is not supported.
- Controller GUI support is not present for the AVC Protocol Pack feature.
- Downloading the AVC Protocol Pack is not supported on the Cisco 2500 Series Wireless LAN Controllers.
- The number of applications that you can apply rate limit is 3.
- Only one rule can be configured per application. An application cannot have both a rate limit as well as a Mark rule.
- AVC rate limiting is not supported on Cisco 2504 WLC.

Configuring Application Visibility and Control (GUI)

Step 1 Create and configure an AVC profile by following these steps:

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles**.
b) Click **New**.
c) Enter the AVC profile name.
d) Click **Apply**.
e) On the **AVC Profile Name** page, click the corresponding AVC profile name.

The **AVC Profile > Edit** page is displayed.

f) Click **Add New Rule**.
g) Choose the application group and the application name from the respective drop-down lists.

View the list of default AVC applications available by choosing **Wireless** > **Application Visibility and Control** > **AVC Applications**.

h) From the **Action** drop-down list, choose either of the following:

- **Drop**—Drops the upstream and downstream packets that correspond to the chosen application.
- **Mark**—Marks the upstream and downstream packets that correspond to the chosen application with the Differentiated Services Code Point (DSCP) value that you specify in the **DSCP (0 to 63)** drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.

Note The default action is to give permission to all applications.

i) If you choose **Mark** from the **Action** drop-down list, choose a DSCP value from the **DSCP (0 to 63)** drop-down list.

The DSCP value is a packet header code that is used to define QoS across the Internet. The DSCP values are mapped to the following QoS levels:

- **Platinum (Voice)**—Assures a high QoS for Voice over Wireless.
- **Gold (Video)**—Supports high-quality video applications.
- **Silver (Best Effort)**—Supports normal bandwidth for clients.
- **Bronze (Background)**—Provides the lowest bandwidth for guest services.

You can also choose **Custom** and specify the DSCP value. The valid range is from 0 to 63.

j) Click **Apply**.
k) Click **Save Configuration**.

Step 2 Associate an AVC profile to a WLAN by following these steps:

a) Choose **WLANs** and click the corresponding WLAN ID.

The **WLANs > Edit** page is displayed.

b) Click the **QoS** tab.
c) Choose the AVC profile from the **AVC Profile** drop-down list.
d) Click **Apply**.

e) Click **Save Configuration**.

Configuring Application Visibility and Control (CLI)

- Create or delete an AVC profile by entering this command:

  config avc profile *avc-profile-name* {**create** | **delete**}
- Add a rule for an AVC profile by entering this command:

  config avc profile *avc-profile-name* **rule add application** *application-name* {**drop** | **mark** *dscp-value* | **ratelimit** *Average Ratelimit value Burst Ratelimit value*}
- Remove a rule for an AVC profile by entering this command:

  config avc profile *avc-profile-name* **rule remove application** *application-name*
- Configure an AVC profile to a WLAN by entering this command:

  config wlan avc *wlan-id* **profile** *avc-profile-name* {**enable** | **disable**}
- Configure application visibility for a WLAN by entering this command:

  config wlan avc *wlan-id* **visibility** {**enable** | **disable**}

  Note Application visibility is the subset of an AVC profile. Therefore, visibility is automatically enabled when you configure an AVC profile on the WLAN.
- Download an AVC Protocol Pack to the controller by entering these commands:
  1. **transfer download datatype avc-protocol-pack**
  2. **transfer download start**
- View information about all AVC profile or a particular AVC profile by entering this command:

  show avc profile {**summary** | **detailed** *avc-profile-name*}
- View information about AVC applications by entering these commands:
  - **show avc applications** [*application-group*]—Displays all the supported AVC applications for the application group.
  - **show avc statistics application** *application_name* **top-users** [**downstream wlan** | **upstream wlan** | **wlan**] [*wlan_id*]} —Displays AVC statistics for the top users of an application.
  - **show avc statistics top-apps** [**upstream** | **downstream**]—Displays the AVC statistics for the most used application.
  - **show avc statistics wlan** *wlan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}—Displays the AVC statistics of a WLAN per application or top applications or top application groups.
  - **show avc statistics client** *client_MAC* {**application** *application_name* | **top-apps** [**upstream** | **downstream**]}—Displays the client AVC statistics per application or top applications.

Note You can view list of 30 applications using the **show avc applications** and **show avc statistics** commands.

- View the protocol pack that is used on the controller by entering this command:

  show avc protocol-pack version
- View the AVC engine version information by entering this command:

  show avc engine version
- Configure troubleshooting for AVC events by entering this command:

  debug avc events {**enable** | **disable**}
- Configure troubleshooting for AVC errors by entering this command:

  debug avc error {**enable** | **disable**}

Configuring NetFlow

NetFlow

NetFlow is an embedded instrumentation within the controller software to characterize wireless network flows. NetFlow monitors each IP flow and exports the aggregated flow data to the external NetFlow collectors.

The NetFlow architecture consists of the following components:

- Collector—Entity that collects all the IP traffic information from various NetFlow exporters.
- Exporter—Network entity that exports the template with the IP traffic information. The controller acts as an exporter.

Note Controller does not support IPv6 address format when acting as an exporter for NetFlow.

Configuring NetFlow (GUI)

Step 1 Configure the Exporter by performing these steps:

a) Choose **Wireless** > **Netflow** > **Exporter.**
b) Click **New**.
c) Enter the Exporter name, IP address, and the port number.

   The valid range for the port number is from 1 to 65535.

d) Click **Apply**.
e) Click **Save Configuration**.

Step 2 Configure the NetFlow Monitor by performing these steps:

a) Choose **Wireless** > **Netflow** > **Monitor.**
b) Click **New** and enter a Monitor name.
c) On the Monitor List window, click the Monitor name to open the **Netflow Monitor** > **Edit** window.
d) Choose the exporter name and the record name from the respective drop-down lists.

- Client App Record—Better Performance

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

Step 3 Associate a NetFlow Monitor to a WLAN by performing these steps:

a) Choose **WLANs** and click a WLAN ID to open the **WLANs** > **Edit page.**
b) In the QoS tab, choose a NetFlow monitor from the **Netflow Monitor** drop-down list.
c) Click **Apply**.
d) Click **Save Configuration**.

Configuring NetFlow (CLI)

- Create an Exporter by entering this command:

  config flow create exporter *exporter-name ip-addr port-number*
- Create a NetFlow Monitor by entering this command:

  config flow create monitor *monitor-name*
- Associate or dissociate a NetFlow monitor with an exporter by entering this command:

  config flow {**add** | **delete**} **monitor** *monitor-name* **exporter** *exporter-name*
- Associate or dissociate a NetFlow monitor with a record by entering this command:

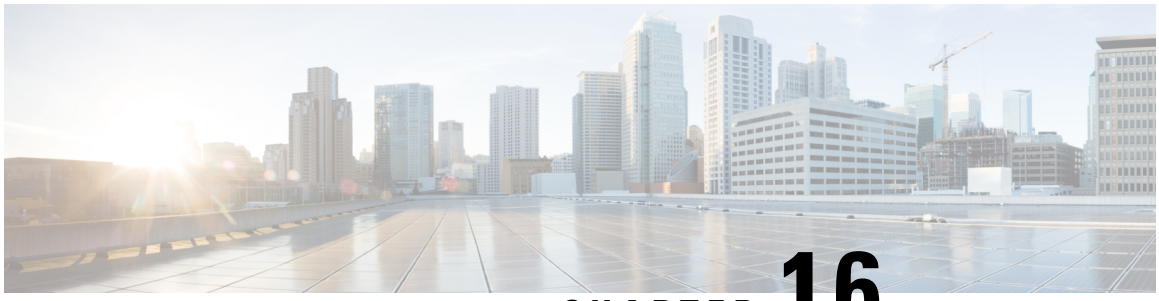
  config flow {**add** | **delete**} **monitor** *monitor-name* **record ipv4_client_app_flow_record**
- Associate or dissociate a NetFlow monitor with a WLAN by entering this command:

  config wlan flow *wlan-id* **monitor** *monitor-name* {**enable** | **disable**}
- View a summary of NetFlow monitors by entering this command:

  show flow monitor summary
- View information about the Exporter by entering this command:

  show flow exporter {**summary** | **statistics**}
- Configure NetFlow debug by entering this command:

  debug flow {**detail** | **error** | **info**} {**enable** | **disable**}



CHAPTER 16

Configuring Media and EDCA Parameters

- Configuring Voice and Video Parameters, on page 145
- Configuring SIP-Based CAC, on page 157
- Configuring Media Parameters, on page 158
- Configuring Voice Prioritization Using Preferred Call Numbers, on page 159
- Configuring EDCA Parameters, on page 160

Configuring Voice and Video Parameters

Voice and Video Parameters

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

- Call admission control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

Each of these parameters is supported in Cisco Compatible Extensions (CCX) v4 and v5.

This section contains the following subsections:

Call Admission Control

Call admission control (CAC) enables an AP to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi Multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, in order to maintain QoS under differing network loads, CAC in CCXv4 is required. Two types of CAC are available: static CAC and load-based CAC.

The following restrictions apply:

- CAC is not supported in FlexConnect local authentication, resulting in voice traffic not getting properly tagged.
- CAC supports the following PHY rates: 6,11,12,24 megabits per second. If CAC is enabled, then at least one of these rates should be enabled on the AP.

Static CAC

Static CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

The QoS setting for a WLAN determines the level of static CAC support. To use static CAC with voice applications, the WLAN must be configured for Platinum QoS. To use static CAC with video applications, the WLAN must be configured for Gold QoS. Also, make sure that WMM is enabled for the WLAN. See the 802.3 Bridging, on page 101 section for QoS and WMM configuration instructions.

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, static CAC does not operate properly.

Load-Based CAC

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

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

Expedited Bandwidth Requests

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

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

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

Table 5: TSPEC Request Handling Examples

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

[1] For static CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.

[2] Static CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Note Admission control for TSPEC g711-40ms codec type is supported.

Note When video ACM is enabled, the controller rejects a video TSPEC if the non-MSDU size in the TSPEC is greater than 149 or the mean data rate is greater than 1 Kbps.

U-APSD

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

Traffic Stream Metrics

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

The metrics consist of a collection of uplink (client side) and downlink (access point side) statistics between an access point and a client device that supports CCX v4 or later releases. If the client is not CCX v4 or CCXv5 compliant, only downlink statistics are captured. The client and access point measure these metrics. The access point also collects the measurements every 5 seconds, prepares 90-second reports, and then sends the reports to the controller. The controller organizes the uplink measurements on a client basis and the downlink measurements on an access point basis and maintains an hour's worth of historical data. To store this data, the controller requires 32 MB of additional memory for uplink metrics and 4.8 MB for downlink metrics.

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

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

Note Access points support TSM entries in both local and FlexConnect modes.

Table 6: TSM Entries in Cisco 5508 and Flex 7510 WLCs

TSM Entries	5508	Flex 7510
MAX AP TSM entries	100	100
MAX Client TSM entries	250	250
MAX TSM entries	100*250=25000	100*250=25000

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

Configuring Voice Parameters

Configuring Voice Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Platinum QoS level.

Step 2 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, unselect the 802.11a (or 802.11b/g) Network Status check box, and click **Apply** to disable the radio network.

Step 3 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media page appears. The Voice tab is displayed by default.

Step 4 (Optional) Select the **Admission Control (ACM)** check box to enable static CAC for this radio band. The default value is disabled.

Step 5 (Optional) Select the **Admission Control (ACM)** you want to use by choosing from the following choices:

- **Load-based**—To enable channel-based CAC. This is the default option.
- **Static**—To enable radio-based CAC.

Step 6 In the **Max RF Bandwidth** text box, enter the percentage of the maximum bandwidth allocated to clients for voice applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band.

The range is 5% to 85%. The sum of maximum bandwidth percentage of voice and video should not exceed 85%.

The default is 75%.

Step 7 In the **Reserved Roaming Bandwidth** text box, enter the percentage of maximum allocated bandwidth that is reserved for roaming voice clients. The controller reserves this bandwidth from the maximum allocated bandwidth for roaming voice clients.

The range is 0% to 25%.

The default is 6%.

Step 8 To enable expedited bandwidth requests, select the **Expedited Bandwidth** check box. By default, this text box is disabled.

Step 9 To enable SIP CAC support, select the **SIP CAC Support** check box. By default, SIP CAC support is disabled.

Step 10 From the **SIP Codec** drop-down list, choose one of the following options to set the codec name. The default value is G.711. The options are as follows:

- User Defined
- G.711
- G.729

Step 11 In the **SIP Bandwidth (kbps)** text box, enter the bandwidth in kilobits per second.

The possible range is 8 to 64.

The default value is 64.

Note The **SIP Bandwidth (kbps)** text box is highlighted only when you select the SIP codec as User-Defined. If you choose the SIP codec as G.711, the **SIP Bandwidth (kbps)** text box is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (kbps) text box is set to 8.

Step 12 In the **SIP Voice Sample Interval (msecs)** text box, enter the value for the sample interval.

Step 13 In the **Maximum Calls** text box, enter the maximum number of calls that can be made to this radio. The maximum call limit includes both direct and roaming-in calls. If the maximum call limit is reached, the new or roaming-in calls result in failure.

The possible range is 0 to 25.

The default value is 0, which indicates that there is no check for maximum call limit.

Note If SIP CAC is supported and the CAC method is static, the Maximum Possible Voice Calls and Maximum Possible Roaming Reserved Calls fields appear.

Step 14 Select the **Metrics Collection** check box to collect traffic stream metrics. By default, this box is unselected. That is, the traffic stream metrics is not collected by default.

Step 15 Click **Apply**.

Step 16 Choose **Network** under 802.11a/n/ac or 802.11b/g/n, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to reenable the radio network.

Step 17 Click **Save Configuration**.

Step 18 Repeat this procedure if you want to configure voice parameters for another radio band.

Configuring Voice Parameters (CLI)

Before you begin

Ensure that you have configured SIP-based CAC.

Step 1 See all of the WLANs configured on the controller by entering this command:

show wlan summary

Step 2 Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Platinum by entering this command:

show wlan *wlan_id*

Step 3 Disable the radio network by entering this command:

config {**802.11a** | **802.11b**} **disable network**

Step 4 Save your settings by entering this command:

save config

Step 5 Enable or disable static voice CAC for the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **cac voice acm** {**enable** | **disable**}

Step 6 Set the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **cac voice max-bandwidth** *bandwidth*

The *bandwidth* range is 5 to 85%, and the default value is 75%. Once the client reaches the value specified, the access point rejects new calls on this network.

Step 7 Set the percentage of maximum allocated bandwidth reserved for roaming voice clients by entering this command:

config {**802.11a** | **802.11b**} **cac voice roam-bandwidth** *bandwidth*

The *bandwidth* range is 0 to 25%, and the default value is 6%. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.

Step 8 Configure the codec name and sample interval as parameters and to calculate the required bandwidth per call by entering this command:

config {**802.11a** | **802.11b**} **cac voice sip codec** {**g711** | **g729**} **sample-interval** *number_msecs*

Step 9 Configure the bandwidth that is required per call by entering this command:

config {**802.11a** | **802.11b**} **cac voice sip bandwidth** *bandwidth_kbps* **sample-interval** *number_msecs*

Step 10 Reenable the radio network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Step 11 View the TSM voice metrics by entering this command:

show [802.11a | 802.11b] cu-metrics *AP_Name*

The command also displays the channel utilization metrics.

Step 12 Enter the **save config** command to save your settings.

Configuring Video Parameters

Configuring Video Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Platinum or Gold QoS level.

Step 2 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 3 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media page appears.

Step 4 In the **Video** tab, check the **Admission Control (ACM)** check box to enable video CAC for this radio band. The default value is disabled.

Step 5 From the **CAC Method** drop-down list, choose between **Static** and **Load Based** methods.

The static CAC method is based on the radio and the load-based CAC method is based on the channel.

Note For TSpec and SIP based CAC for video calls, only Static method is supported.

Step 6 In the **Max RF Bandwidth** text box, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. When the client reaches the value specified, the access point rejects new requests on this radio band.

The range is 5% to 85%. The sum of maximum bandwidth percentage of voice and video should not exceed 85%. The default is 0%.

Step 7 In the Reserved Roaming Bandwidth text box, enter the percentage of the maximum RF bandwidth that is reserved for roaming clients for video.

Step 8 Configure the SIP CAC Support by checking or unchecking the **SIP CAC Support** check box.

SIP CAC is supported only if SIP Snooping is enabled.

Note You cannot enable SIP CAC if you have selected the Load Based CAC method.

Step 9 Click **Apply**.

Step 10 Choose **Network** under 802.11a/n/ac or 802.11b/g/n, check the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to reenable the radio network.

Step 11 Click **Save Configuration**.

Step 12 Repeat this procedure if you want to configure video parameters for another radio band.

Configuring Video Parameters (CLI)

Before you begin

Ensure that you have configured SIP-based CAC.

Step 1 See all of the WLANs configured on the controller by entering this command:

show wlan summary

Step 2 Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Gold by entering this command:

show wlan *wlan_id*

Step 3 Disable the radio network by entering this command:

config {**802.11a** | **802.11b**} **disable network**

Step 4 Save your settings by entering this command:

save config

Step 5 Enable or disable video CAC for the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **cac video acm** {**enable** | **disable**}

Step 6 To configure the CAC method as either static or load-based, enter this command:

config {**802.11a** | **802.11b**} **cac video cac-method** {**static** | **load-based**}

Step 7 Set the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **cac video max-bandwidth** *bandwidth*

The *bandwidth* range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.

Note If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

Step 8 To configure the percentage of the maximum RF bandwidth that is reserved for roaming clients for video, enter this command:

config {**802.11a** | **802.11b**} **cac video roam-bandwidth** *bandwidth*

Step 9 To configure the CAC parameters for SIP-based video calls, enter this command:

config {**802.11a** | **802.11b**} **cac video sip** {**enable** | **disable**}

Step 10 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command:

config {**802.11a** | **802.11b**} **cac video tspec-inactivity-timeout** {**enable** | **ignore**}

Step 11 Reenable the radio network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Step 12 Enter the **save config** command to save your settings.

Viewing Voice and Video Settings

Viewing Voice and Video Settings (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client to open the Clients > Detail page.

This page shows the U-APSD status (if enabled) for this client under Quality of Service Properties.

Step 3 Click **Back** to return to the Clients page.

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated as follows:

a) Hover your cursor over the blue drop-down arrow for the desired client and choose **802.11aTSM** or **802.11b/g TSM**. The Clients > AP page appears.

b) Click the **Detail** link for the desired access point to open the Clients > AP > Traffic Stream Metrics page.

This page shows the TSM statistics for this client and the access point to which it is associated. The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Step 5 See the TSM statistics for a particular access point and a particular client associated to this access point, as follows:

a) Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n/ac** or **802.11b/g/n**. The 802.11a/n/ac Radios or 802.11b/g/n Radios page appears.

b) Hover your cursor over the blue drop-down arrow for the desired access point and choose **802.11aTSM** or **802.11b/g TSM**. The AP > Clients page appears.

c) Click the **Detail** link for the desired client to open the AP > Clients > Traffic Stream Metrics page.

This page shows the TSM statistics for this access point and a client associated to it. The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Viewing Voice and Video Settings (CLI)

Step 1 See the CAC configuration for the 802.11 network by entering this command:

show ap stats {**802.11a** | **802.11b**}

Step 2 See the CAC statistics for a particular access point by entering this command:

show ap stats {802.11a | 802.11b} *ap_name*

Information similar to the following appears:

```
Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)..... 0
Total channel MT free..................... 0
Total voice MT free....................... 0
Na Direct................................. 0
Na Roam................................... 0
  Video Bandwidth in use(% of config bw)..... 0
  Total num of voice calls in progress...... 0
  Num of roaming voice calls in progress..... 0
  Total Num of voice calls since AP joined..... 0
  Total Num of roaming calls since AP joined..... 0
 Total Num of exp bw requests received.......... 5
  Total Num of exp bw requests admitted.......... 2

Num of voice calls rejected since AP joined...... 0
  Num of roam calls rejected since AP joined..... 0
  Num of calls rejected due to insufficient bw....0
  Num of calls rejected due to invalid params.... 0
  Num of calls rejected due to PHY rate.......... 0
  Num of calls rejected due to QoS policy..... 0
```

In the example above, "MT" is medium time, "Na" is the number of additional calls, and "exp bw" is expedited bandwidth.

Note Suppose an AP has to be rebooted when a voice client associated with the AP is on an active call. After the AP is rebooted, the client continues to maintain the call, and during the time the AP is down, the database is not refreshed by the controller. Therefore, we recommend that all active calls are ended before the AP is taken down.

Step 3 See the U-APSD status for a particular client by entering this command:

show client detail *client_mac*

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated by entering this command:

show client tsm {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**}

The optional **all** command shows all access points to which this client has associated. Information similar to the following appears:

```
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds

  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec).............................10
      Maximum Lost Packet count(5sec)............................5
      Average Lost Packet count(5secs)...........................2
    DownLink Stats
```

```
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec)..............................10
      Maximum Lost Packet count(5sec).............................5
      Average Lost Packet count(5secs)............................2
```

Note The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Note Clear the TSM statistics for a particular access point or all the access points to which this client is associated by entering this **clear client tsm** {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**} command.

Step 5 See the TSM statistics for a particular access point and a particular client associated to this access point by entering this command:

show ap stats {**802.11a** | **802.11b**} *ap_name* **tsm** {*client_mac* | **all**}

The optional **all** command shows all clients associated to this access point. Information similar to the following appears:

```
AP Interface Mac:                   00:0b:85:01:02:03
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds

  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec)..............................10
      Maximum Lost Packet count(5sec).............................5
      Average Lost Packet count(5secs)............................2
    DownLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec)..............................10
      Maximum Lost Packet count(5sec).............................5
      Average Lost Packet count(5secs)............................2
```

Note The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Step 6 Enable or disable debugging for call admission control (CAC) messages, events, or packets by entering this command:

debug cac {**all** | **event** | **packet**}{**enable** | **disable**}

where **all** configures debugging for all CAC messages, **event** configures debugging for all CAC events, and **packet** configures debugging for all CAC packets.

Step 7 Use the following command to perform voice diagnostics and to view the debug messages between a maximum of two 802.11 clients:

debug voice-diag {**enable** | **disable**} *mac-id mac-id2* [**verbose**]

The verbose mode is an optional argument. When the verbose option is used, all debug messages are displayed in the console. You can use this command to monitor a maximum of two 802.11 clients. If one of the clients is a non-WiFi client, only the 802.11 client is monitored for debug messages.

Note It is implicitly assumed that the clients being monitored are on call.

Note The debug command automatically stops after 60 minutes.

Step 8 Use the following commands to view various voice-related parameters:

- **show client voice-diag status**

  Displays information about whether voice diagnostics is enabled or disabled. If enabled, will also displays information about the clients in the watch list and the time remaining for the diagnostics of the voice call.

  If voice diagnostics is disabled when the following commands are entered, a message indicating that voice diagnostics is disabled appears.

- **show client voice-diag tspec**

  Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.

- **show client voice-diag qos-map**

  Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.

- **show client voice-diag avrg_rssi**

  Display the client's RSSI values in the last 5 seconds when voice diagnostics is enabled.

- **show client voice-diag roam-history**

  Displays information about the last three roaming calls. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, the reason for the roaming-failure.

- **show client calls {active | rejected} {802.11a | 802.11bg | all}**

  This command lists the details of active TSPEC and SIP calls on the controller.

Step 9 Use the following commands to troubleshoot video debug messages and statistics:

- **debug ap show stats {802.11b | 802.11a}** *ap-name* **multicast**—Displays the access point's supported multicast rates.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **load**—Displays the access point's QBSS and other statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **tx-queue**—Displays the access point's transmit queue traffic statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **client** {**all** | **video** | *client-mac*}—Displays the access point's client metrics.

- **debug ap show stats {802.11b | 802.11a}** *ap-name packet*—Displays the access point's packet statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **video metrics**—Displays the access point's video metrics.
- **debug ap show stats video** *ap-name* **multicast mgid** *number* —Displays an access point's Layer 2 MGID database number.
- **debug ap show stats video** *ap-name* **admission**—Displays an access point's admission control statistics.
- **debug ap show stats video** *ap-name* **bandwidth**—Displays an access point's video bandwidth.

Configuring SIP-Based CAC

Restrictions for SIP-Based CAC

- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

Configuring SIP-Based CAC (GUI)

Before you begin

- Ensure that you have set the voice to the platinum QoS level.
- Ensure that you have enabled call snooping for the WLAN.
- Ensure that you have enabled the Admission Control (ACM) for this radio.

Step 1 Choose **Wireless** > **Advanced** > **SIP Snooping** to open the SIP Snooping page.

Step 2 Specify the call-snooping ports by entering the starting port and the ending port.

Step 3 Click **Apply** and then click **Save Configuration**.

Configuring SIP-Based CAC (CLI)

Step 1 Set the voice to the platinum QoS level by entering this command:

config wlan qos *wlan-id* **Platinum**

Step 2 Enable the call-snooping feature for a particular WLAN by entering this command:

config wlan call-snoop enable *wlan-id*

Step 3 Enable the ACM to this radio by entering this command:

config {**802.11a** | **802.11b**} **cac** {**voice** | **video**} **acm enable**

Step 4 To configure the call snooping ports, enter this command:

config advanced sip-snooping-ports *starting-port ending-port*

Step 5 To troubleshoot SIP-based CAC events, enter this command:

debug sip event {**enable** | **disable**}

Configuring Media Parameters

Configuring Media Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Gold QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 4 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media > Parameters page appears.

Step 5 Choose the **Media** tab to open the Media page.

Step 6 Select the **Unicast Video Redirect** check box to enable Unicast Video Redirect. The default value is disabled.

Step 7 In the **Maximum Media Bandwidth (0-85%)** text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches the specified value, the access point rejects new calls on this radio band.

The default value is 85%; valid values are from 0 to 85%.

Step 8 In the **Client Phy Rate** text box, enter the value for the rate in kilobits per second at which the client operates.

Step 9 In the **Maximum Retry Percent (0-100%)** text box, enter the percentage of the maximum retry. The default value is 80.

Step 10 Select the **Multicast Direct Enable** check box to enable the **Multicast Direct Enable** text box. The default value is enabled.

Step 11 From the **Max Streams per Radio** drop-down list, choose the maximum number of allowed multicast direct streams per radio. Choose a value between 1 to 20 or No Limit. The default value is set to No Limit.

Step 12 From the **Max Streams per Client** drop-down list, choose the maximum number of allowed clients per radio. Choose a value between 1 to 20 or No Limit. The default value is set to No Limit.

Step 13 If you want to enable the best radio queue for this radio, select the **Best Effort QoS Admission** check box. The default value is disabled.

Configuring Voice Prioritization Using Preferred Call Numbers

Voice Prioritization Using Preferred Call Numbers

You can configure a controller to support calls from clients that do not support TSPEC-based calls. This feature is known as voice prioritization. These calls are given priority over other clients utilizing the voice pool. Voice prioritization is available only for SIP-based calls and not for TSPEC-based calls. If the bandwidth is available, it takes the normal flow and allocates the bandwidth to those calls.

You can configure up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the controller does not check on the maximum call limit. It invokes the CAC to allocate bandwidth for the preferred call. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

This section contains the following subsections:

Prerequisites for Configuring Voice Prioritization Using Preferred Call Numbers

You must configure the following before configuring voice prioritization:

- Set WLAN QoS to platinum.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

Configuring a Preferred Call Number (GUI)

Step 1 Set the WLAN QoS profile to Platinum.

Step 2 Enable ACM for the WLAN radio.

Step 3 Enable SIP call snooping for the WLAN.

Step 4 Choose **Wireless** > **Advanced** > **Preferred Call** to open the **Preferred Call** page.

All calls configured on the controller appear.

Note To remove a preferred call, hover your cursor over the blue drop-down arrow and choose **Remove**.

Step 5 Click **Add Number** to add a new preferred call.

Step 6 In the Call Index text box, enter the index that you want to assign to the call. Valid values are from 1 through 6.

Step 7 In the Call Number text box, enter the number.

Step 8 Click **Apply** to add the new number.

Configuring a Preferred Call Number (CLI)

Step 1 Set the voice to the platinum QoS level by entering this command:

config wlan qos wlan-id Platinum

Step 2 Enable the ACM to this radio by entering this command:

config {802.11a | 802.11b} cac {voice | video} acm enable

Step 3 Enable the call-snooping feature for a particular WLAN by entering this command:

config wlan call-snoop enable *wlan-id*

Step 4 Add a new preferred call by entering this command:

config advanced sip-preferred-call-no *call_index* {*call_number* | **none**}

Step 5 Remove a preferred call by entering this command:

config advanced sip-preferred-call-no *call_index* **none**

Step 6 View the preferred call statistics by entering the following command:

show ap stats {802.11{a | b} | wlan} *ap_name*

Step 7 Enter the following command to list the preferred call numbers:

show advanced sip-preferred-call-no

Configuring EDCA Parameters

Enhanced Distributed Channel Access Parameters

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

This section contains the following subsections:

Configuring EDCA Parameters (GUI)

Step 1 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 2 Click **EDCA Parameters**under 802.11a/n/ac or 802.11b/g/n.

Step 3 The **802.11a (or 802.11b/g) > EDCA Parameters** window is displayed.

Step 4 Choose one of the following options from the **EDCA Profile** drop-down list:

- **WMM**—Enables the Wi-Fi Multimedia (WMM) default parameters. We recommend this setting for use in SpectraLink phones. Use this setting unless a specific client application recommends a different setting.
- **Spectralink Voice Priority**—This setting is not recommended.
- **Voice Optimized**—Enables Enhanced Distributed Channel Access (EDCA) voice-optimized profile parameters. Choose this option when 8821 phones are deployed in your network, and video services are not in use.
- **Voice & Video Optimized**—Enables EDCA voice-optimized and video-optimized profile parameters. Choose this option when 8821 phones are deployed in your network, and video services are not in use.
- **Custom Voice**—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

Note If you deploy video services, admission control must be disabled.

Step 5 To enable MAC optimization for voice, check the **Enable Low Latency MAC** check box. By default, this check box is not checked. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point.

Note We recommend against you enabling low latency MAC. You should enable low-latency MAC only if the WLAN allows WMM clients. If WMM is enabled, then low-latency MAC can be used with any of the EDCA profiles.

Step 6 Click **Apply** to commit your changes.

Step 7 To re-enable the radio network, click **Network** under 802.11a/n/ac or 802.11b/g/n, check the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 8 Click **Save Configuration**.

Configuring EDCA Parameters (CLI)

Step 1 Disable the radio network by entering this command:

config {**802.11a** | **802.11b**} **disable network**

Step 2 Save your settings by entering this command:

save config

Step 3 Enable a specific EDCA profile by entering this command:

config advanced {802.11a | 802.11b} edca-parameters {**wmm-default | svp-voice | optimized-voice | optimzed-voice-video | custom-voice** }

- **wmm-default**—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option if voice or video services are not deployed on your network.
- **svp-voice**—Enables SpectraLink voice-priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
- **optimized-voice**—Enables EDCA voice-optimized profile parameters. Choose this option if voice services other than SpectraLink are deployed on your network.

- **optimized-video-voice**—Enables EDCA voice-optimized and video-optimized profile parameters. Choose this option if both voice and video services are deployed on your network.
- **custom-voice**—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

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

Step 4 View the current status of MAC optimization for voice by entering this command:

show {**802.11a** | **802.11b**}

Information that is similar to the following example is displayed:

```
Voice-mac-optimization.................Disabled
```

Step 5 Enable or disable MAC optimization for voice by entering this command:

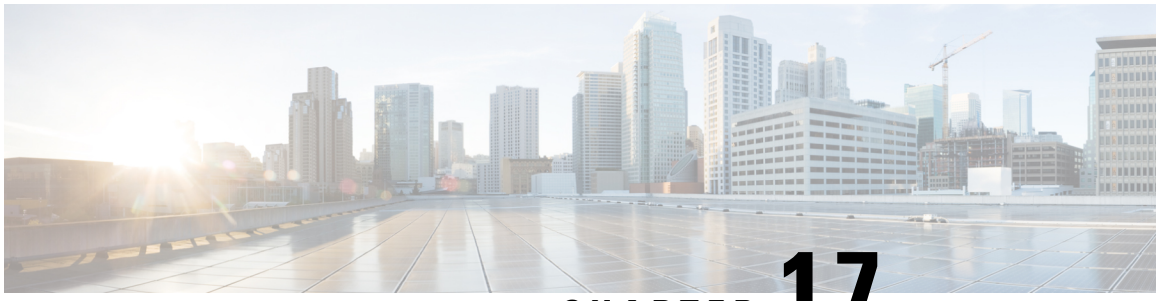
config advanced {**802.11a** | **802.11b**} **voice-mac-optimization** {**enable** | **disable**}

Note This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight APs. This, in tun improves the number of voice calls serviced per AP. The default value is disabled.

Step 6 Re-enable the radio network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Step 7 Save your settings by entering this command: **save config**.



CHAPTER 17

Configuring the Cisco Discovery Protocol

- Cisco Discovery Protocol, on page 163
- Restrictions for Cisco Discovery Protocol, on page 163
- Configuring the Cisco Discovery Protocol, on page 165
- Viewing Cisco Discovery Protocol Information, on page 167
- Getting CDP Debug Information, on page 170

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices.

The default value for the frequency of periodic transmissions is 60 seconds, and the default advertised time-to-live value is 180 seconds. The second and latest version of the protocol, CDPv2, introduces new time-length-values (TLVs) and provides a reporting mechanism that allows for more rapid error tracking, which reduces downtime.

Note Cisco recommends that you disable Cisco Discovery Protocol on the controller and access point when connected to non-Cisco switches as CDP is unsupported on non-Cisco switches and network elements.

Restrictions for Cisco Discovery Protocol

- CDPv1 and CDPv2 are supported on the following devices:
  - Cisco 2504 Wireless Controller
  - Cisco 5508 Wireless Controller
  - Cisco 5520 Wireless Controller
  - Cisco 8510 Wireless Controller
  - Cisco 8540 Wireless Controller
  - CAPWAP-enabled access points

- An access point connected directly to a Cisco 2504 Wireless Controller

Note To use the Intelligent Power Management feature, ensure that CDPv2 is enabled on the Cisco 2504 Wireless Controller. CDP v2 is enabled by default.

- The Cisco 600 Series OEAPs do not support CDP.
- The support of CDPv1 and CDPv2 enables network management applications to discover Cisco devices.
- The following TLVs are supported by both the controller and the access point:
  - Device-ID TLV: 0x0001—The hostname of the controller, the access point, or the CDP neighbor.
  - Address TLV: 0x0002—The IP address of the controller, the access point, or the CDP neighbor.
  - Port-ID TLV: 0x0003—The name of the interface on which CDP packets are sent out.
  - Capabilities TLV: 0x0004—The capabilities of the device. The controller sends out this TLV with a value of Host: 0x10, and the access point sends out this TLV with a value of Transparent Bridge: 0x02.
  - Version TLV: 0x0005—The software version of the controller, the access point, or the CDP neighbor.
  - Platform TLV: 0x0006—The hardware platform of the controller, the access point, or the CDP neighbor.
  - Power Available TLV: 0x001a— The amount of power available to be transmitted by power sourcing equipment to permit a device to negotiate and select an appropriate power setting.
  - Full/Half Duplex TLV: 0x000b—The full- or half-duplex mode of the Ethernet link on which CDP packets are sent out.
- These TLVs are supported only by the access point:
  - Power Consumption TLV: 0x0010—The maximum amount of power consumed by the access point.
  - Power Request TLV:0x0019—The amount of power to be transmitted by a powerable device in order to negotiate a suitable power level with the supplier of the network power.
- If the switch has provided power through CDP, it continues to provide only with CDP, and vice-versa with LLDP. (CSCvg86156)
- Changing the CDP configuration on the controller does not change the CDP configuration on the access points that are connected to the controller. You must enable and disable CDP separately for each access point.
- You can enable or disable the CDP state on all or specific interfaces and radios. This configuration can be applied to all access points or a specific access point.
- The following is the behavior assumed for various interfaces and access points:
  - CDP is disabled on radio interfaces on indoor (nonindoor mesh) access points.
  - Nonmesh access points have CDPs disabled on radio interfaces when they join the controller. The persistent CDP configuration is used for the APs that had CDP support in its previous image.

- CDP is enabled on radio interfaces on indoor-mesh and mesh access points.
- Mesh access points will have CDP enabled on their radio interfaces when they join the controller. The persistent CDP configuration is used for the access points that had CDP support in a previous image. The CDP configuration for radio interfaces is applicable only for mesh APs.

- CDP over radio backhaul link is not supported in Wave 2 (COS) APs.
- CDP is not supported in radio interfaces of Wave 2 (COS) APs. The GUI configuration of this has no effect.

Configuring the Cisco Discovery Protocol

Configuring the Cisco Discovery Protocol (GUI)

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

Step 2 Select the **CDP Protocol Status** check box to enable CDP on the controller or unselect it to disable this feature. The default value is selected.

Note Enabling or disabling this feature is applicable to all controller ports.

Step 3 From the CDP Advertisement Version drop-down list, choose **v1** or **v2** to specify the highest CDP version supported on the controller. The default value is v1.

Step 4 In the Refresh-time Interval text box, enter the interval at which CDP messages are to be generated. The range is 5 to 254 seconds, and the default value is 60 seconds.

Step 5 In the Holdtime text box, enter the amount of time to be advertised as the time-to-live value in generated CDP packets. The range is 10 to 255 seconds, and the default value is 180 seconds.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Step 8 Perform one of the following:

- To enable or disable CDP on a specific access point, follow these steps:

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

  Click the link for the desired access point.

  Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

  Select the **Cisco Discovery Protocol** check box to enable CDP on this access point or unselect it to disable this feature. The default value is enabled.

  Note If CDP is disabled in Step 2, a message indicating that the Controller CDP is disabled appears.

- Enable CDP for a specific Ethernet interface, radio, or slot as follows:

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

  Click the link for the desired access point.

Choose the **Interfaces** tab and select the corresponding check boxes for the radios or slots from the CDP Configuration section.

Note Configuration for radios is only applicable for mesh access points.

Click **Apply** to commit your changes.

- To enable or disable CDP on all access points currently associated to the controller, follow these steps:

  Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

  Select the **CDP State** check box to enable CDP on all access points associated to the controller or unselect it to disable CDP on all access points. The default value is selected. You can enable CDP on a specific Ethernet interface, radio, or slot by selecting the corresponding check box. This configuration will be applied to all access points associated with the controller.

  Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Configuring the Cisco Discovery Protocol (CLI)

Step 1 Enable or disable CDP on the controller by entering this command:

config cdp {**enable** | **disable**}

CDP is enabled by default.

Step 2 Specify the interval at which CDP messages are to be generated by entering this command:

config cdp timer *seconds*

The range is 5 to 254 seconds, and the default value is 60 seconds.

Step 3 Specify the amount of time to be advertised as the time-to-live value in generated CDP packets by entering this command:

config cdp holdtime *seconds*

The range is 10 to 255 seconds, and the default value is 180 seconds.

Step 4 Specify the highest CDP version supported on the controller by entering this command:

config cdp advertise {**v1** | **v2**}

The default value is v1.

Step 5 Enable or disable CDP on all access points that are joined to the controller by entering the **config ap cdp** {**enable** | **disable**} **all** command.

The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **config ap cdp enable all** command.

Note After you enable CDP on all access points joined to the controller, you may disable and then reenable CDP on individual access points using the command in Step 6. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

Step 6 Enable or disable CDP on a specific access point by entering this command:

config ap cdp {**enable** | **disable**} *Cisco_AP*

Step 7 Configure CDP on a specific or all access points for a specific interface by entering this command:

config ap cdp {ethernet | radio} *interface_number slot_id* **{enable** | **disable} {all** | *Cisco_AP***}**

Note When you use the config ap cdp command to configure CDP on radio interfaces, a warning message appears indicating that the configuration is applicable only for mesh access points.

Step 8 Save your changes by entering this command:

save config

Viewing Cisco Discovery Protocol Information

Viewing Cisco Discovery Protocol Information (GUI)

Step 1 Choose **Monitor** > **CDP** > **Interface Neighbors** to open the CDP > Interface Neighbors page appears.

This page shows the following information:

- The controller port on which the CDP packets were received
- The name of each CDP neighbor
- The IP address of each CDP neighbor
- The port used by each CDP neighbor for transmitting CDP packets
- The time left (in seconds) before each CDP neighbor entry expires
- The functional capability of each CDP neighbor, defined as follows: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device
- The hardware platform of each CDP neighbor device

Step 2 Click the name of the desired interface neighbor to see more detailed information about each interface's CDP neighbor. The CDP > Interface Neighbors > Detail page appears.

This page shows the following information:

- The controller port on which the CDP packets were received
- The name of the CDP neighbor
- The IP address of the CDP neighbor
- The port used by the CDP neighbor for transmitting CDP packets
- The CDP version being advertised (v1 or v2)

- The time left (in seconds) before the CDP neighbor entry expires
- The functional capability of the CDP neighbor, defined as follows: Router, Trans Bridge,?Source Route Bridge, Switch, Host, IGMP, Repeater, or Remotely Managed Device
- The hardware platform of the CDP neighbor device
- The software running on the CDP neighbor

Step 3 Choose **AP Neighbors** to see a list of CDP neighbors for all access points connected to the controller. The CDP AP Neighbors page appears.

Step 4 Click the **CDP Neighbors** link for the desired access point to see a list of CDP neighbors for a specific access point. The CDP > AP Neighbors page appears.

This page shows the following information:

- The name of each access point
- The IP address of each access point
- The name of each CDP neighbor
- The IP address of each CDP neighbor
- The port used by each CDP neighbor
- The CDP version being advertised (v1 or v2)

Step 5 Click the name of the desired access point to see detailed information about an access point's CDP neighbors. The CDP > AP Neighbors > Detail page appears.

This page shows the following information:

- The name of the access point
- The MAC address of the access point's radio
- The IP address of the access point
- The interface on which the CDP packets were received
- The name of the CDP neighbor
- The IP address of the CDP neighbor
- The port used by the CDP neighbor
- The CDP version being advertised (v1 or v2)
- The time left (in seconds) before the CDP neighbor entry expires
- The functional capability of the CDP neighbor, defined as follows: R - Router, T - Trans Bridge,?B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device
- The hardware platform of the CDP neighbor device
- The software running on the CDP neighbor

Step 6 Choose **Traffic Metrics** to see CDP traffic information. The CDP > Traffic Metrics page appears.

This page shows the following information:

- The number of CDP packets received by the controller
- The number of CDP packets sent from the controller
- The number of packets that experienced a checksum error
- The number of packets dropped due to insufficient memory
- The number of invalid packets

Viewing Cisco Discovery Protocol Information (CLI)

Step 1 See the status of CDP and to view CDP protocol information by entering this command:

show cdp

Step 2 See a list of all CDP neighbors on all interfaces by entering this command:

show cdp neighbors [detail]

The optional detail command provides detailed information for the controller's CDP neighbors.

Note This command shows only the CDP neighbors of the controller. It does not show the CDP neighbors of the controller's associated access points. Additional commands are provided below to show the list of CDP neighbors per access point.

Step 3 See all CDP entries in the database by entering this command:

show cdp entry all

Step 4 See CDP traffic information on a given port (for example, packets sent and received, CRC errors, and so on) by entering this command:

show cdp traffic

Step 5 See the CDP status for a specific access point by entering this command:

show ap cdp ap-name *Cisco_AP*

Step 6 See the CDP status for all access points that are connected to the controller by entering this command:

show ap cdp all

Step 7 See a list of all CDP neighbors for a specific access point by entering these commands:

- **show ap cdp neighbors ap-name** *Cisco_AP*
- **show ap cdp neighbors detail** *Cisco_AP*

Note The access point sends CDP neighbor information to the controller only when the information changes.

Step 8 See a list of all CDP neighbors for all access points connected to the controller by entering these commands:

- **show ap cdp neighbors all**
- **show ap cdp neighbors detail all**

Note The access point sends CDP neighbor information to the controller only when the information changes.

Getting CDP Debug Information

- Get debug information related to CDP packets by entering by entering this command:

  debug cdp packets
- Get debug information related to CDP events by entering this command:

  debug cdp events

CHAPTER 18

Configuring Authentication for the Controller and NTP/SNTP Server

- Authentication for the Controller and NTP/SNTP Server, on page 171
- Configuring the NTP/SNTP Server to Obtain the Date and Time (GUI), on page 171
- Configuring the NTP/SNTP Server for Authentication (CLI), on page 172

Authentication for the Controller and NTP/SNTP Server

We highly recommend that controllers synchronize their time with an external NTP/SNTP server. We also recommend that you authenticate this connection to the NTP/SNTP server, as a best practice. By default, an MD5 checksum is used in this scenario.

Each NTP/SNTP server IP address is added to the controller database. The respective controller then attempts to poll an NTP/SNTP server from this database in the index order. The controller then obtains and synchronizes the current time at each user-defined polling interval, as well as following a reboot event. By default, the NTP polling interval is 600 seconds.

Guidelines and Restrictions on NTP

- When the time difference between the NTP server and the controller exceeds 1000s, the **ntpd** process exits and adds a panic message to the system log. In this situation, set the time on the controller manually.
- NTPv4 protocol is not supported in Cisco 2504 and 5508 Wireless Controllers.

Configuring the NTP/SNTP Server to Obtain the Date and Time (GUI)

Step 1 Choose **Controller** > **NTP** > **Server** to open the **NTP Severs** page.

Step 2 Click **New** to add a new NTP/SNTP Server.

Step 3 (Optional) In the **Server Index (Priority)** field, enter the NTP/SNTP server index.

The controller tries Index 1 first, then Index 2 through 3, in a descending order. Set this to 1 if your network is using only one NTP/SNTP server.

Step 4 Enter the server IP address.

You can enter an IPv4 or an IPv6 address or a fully qualified domain name (FQDN), which should meet the following criteria:

- Contains only a-z , A-Z, and 0-9 characters.
- Does not start with a dot (.) or a hyphen (-).
- Does not end with a dot (.).
- Does not have 2 consecutive dots (..).

Step 5 Enable or disable the NTP/SNTP Authentication.

Step 6 If you enable the NTP/SNTP Authentication, enter the Key Index.

Step 7 Click **Apply**.

Step 8 Delete an exisitng NTP server IP address or DNS server by hovering the cursor over the blue drop-down arrow for that server index and choose **Remove**.

Step 9 Confirm the deletion by clicking on **OK** in the dialog box.

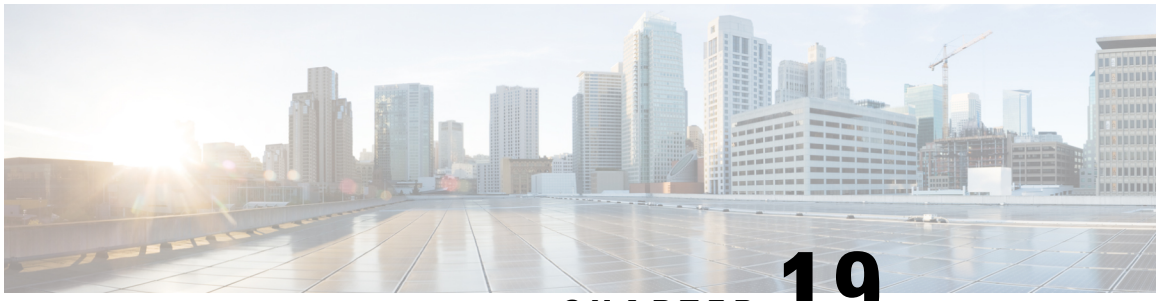
Configuring the NTP/SNTP Server for Authentication (CLI)

Procedure

- **config time ntp auth enable** *server-index key-index*—Enables NTP/SNTP authentication on a given NTP/SNTP server.
- **config time ntp key-auth add** *key-index key-typekey-format key*—Adds an authentication key. By default MD5 is used. The key format can be "ascii" or "hex".
- Configure the NTP interval by entering this command:

  config time ntp interval *interval_seconds*

- **config time ntp key-auth delete** *key-index*—Deletes authentication keys.
- **config time ntp auth disable** *server-index*—Disables NTP/SNTP authentication.
- **show ntp-keys**—Displays the NTP/SNTP authentication related parameter.



CHAPTER 19

Configuring RFID Tag Tracking

- Information About Configuring RFID Tag Tracking, on page 173
- Configuring RFID Tag Tracking (CLI), on page 174
- Viewing RFID Tag Tracking Information (CLI), on page 175
- Debugging RFID Tag Tracking Issues (CLI), on page 175

Information About Configuring RFID Tag Tracking

The controller enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the mobility services engine.

To know more about the tags supported by controller, see http://www.cisco.com/c/en/us/products/wireless/compatible-extensions.html. The mobility services engine receives telemetry and chokepoint information from tags that are compliant with this CCX specification.

Table 7: Cisco Compatible Extensions for RFID Tags Summary

Partners	**AeroScout**		**WhereNet**	**Pango (InnerWireless)**
Product Name	T2	T3	Wheretag IV	V3
Telemetry				
Temperature	X	X	—	X
Pressure	—	—	—	—
Humidity	—	—	—	—
Status	—	—	—	—
Fuel	—	—	—	—
Quantity	—	—	—	—
Distance	—	—	—	—

Partners	AeroScout		WhereNet	Pango (InnerWireless)
Motion Detection	X	X	—	X
Number of Panic Buttons	1	2	0	1
Tampering		X	X	X
Battery Information	X	X	X	X
Multiple-Frequency Tags	X	X	X	

[3] For chokepoint systems, note that the tag can work only with chokepoints coming from the same vendor.

Note The Network Mobility Services Protocol (NMSP) runs on the mobility services engine. For NMSP to function, the TCP port (16113) over which the controller and the mobility services engine communicate must be open (not blocked) on any firewall that exists between these two devices.

The Cisco-approved tags support these capabilities:

- **Information notifications**—Enables you to view vendor-specific and emergency information.
- **Information polling**—Enables you to monitor battery status and telemetry data. Many telemetry data types provide support for sensory networks and a large range of applications for RFID tags.
- **Measurement notifications**—Enables you to deploy chokepoints at strategic points within your buildings or campuses. Whenever an RFID tag moves to within a defined proximity of a chokepoint, the tag begins transmitting packets that advertise its location in relation to the chokepoint.

You can configure and view RFID tag tracking information through the controller CLI.

Configuring RFID Tag Tracking (CLI)

Step 1 Enable or disable RFID tag tracking by entering this command:

config rfid status {**enable** | **disable**}

The default value is enabled.

Step 2 Specify a static timeout value (between 60 and 7200 seconds) by entering this command:

config rfid timeout *seconds*

The static timeout value is the amount of time that the controller maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.

Step 3 Enable or disable RFID tag mobility for specific tags by entering these commands:

- **config rfid mobility** *vendor_name* **enable**—Enables client mobility for a specific vendor's tags. When you enter this command, tags are unable to obtain a DHCP address for client mode when attempting to select and/or download a configuration.
- **config rfid mobility** *vendor_name* **disable**—Disables client mobility for a specific vendor's tags. When you enter this command, tags can obtain a DHCP address. If a tag roams from one subnet to another, it obtains a new address rather than retaining the anchor state.

Note These commands can be used only for Pango tags. Therefore, the only valid entry for *vendor_name* is "pango" in all lowercase letters.

Viewing RFID Tag Tracking Information (CLI)

Step 1 See the current configuration for RFID tag tracking by entering this command:

show rfid config

Step 2 See detailed information for a specific RFID tag by entering this command:

show rfid detail *mac_address*

where *mac_address* is the tag's MAC address.

Step 3 See a list of all RFID tags currently connected to the controller by entering this command:

show rfid summary

Step 4 See a list of RFID tags that are associated to the controller as clients by entering this command:

show rfid client

Debugging RFID Tag Tracking Issues (CLI)

If you experience any problems with RFID tag tracking, use these debug commands.

- Configure MAC address debugging by entering this command:

  debug mac addr *mac_address*

Note We recommend that you perform the debugging on a per-tag basis. If you enable debugging for all of the tags, the console or Telnet screen is inundated with messages.

- Enable or disable debugging for the 802.11 RFID tag module by entering this command:

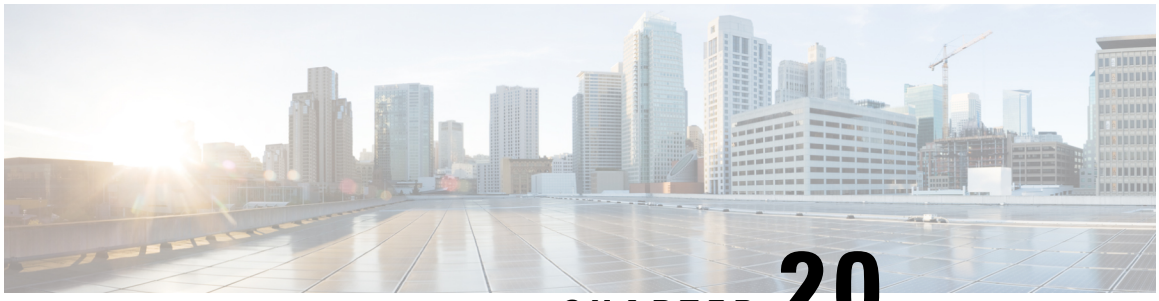
debug dot11 rfid {**enable** | **disable**}

- Enable or disable RFID debug options by entering this command:

  debug rfid {**all** | **detail** | **error** | **nmsp** | **receive**} {**enable** | **disable**}

  where

  - **all** configures debugging of all RFID messages.
  - **detail** configures debugging of RFID detailed messages.
  - **error** configures debugging of RFID error messages.
  - **nmsp** configures debugging of RFID NMSP messages.
  - **receive** configures debugging of incoming RFID tag messages.



CHAPTER 20

Resetting the Controller to Default Settings

- Resetting the Controller to Default Settings, on page 177
- Resetting the Controller to Default Settings (GUI), on page 177
- Resetting the Controller to Default Settings (CLI), on page 177

Resetting the Controller to Default Settings

You can return the controller to its original configuration by resetting the controller to factory-default settings.

This section contains the following subsections:

Resetting the Controller to Default Settings (GUI)

Step 1 Start your Internet browser.

Step 2 Enter the controller IP address in the browser address line and press **Enter**. An Enter Network Password dialog box appears.

Step 3 Enter your username in the User Name text box. The default username is *admin*.

Step 4 Enter the wireless device password in the Password text box and press **Enter**. The default password is *admin*.

Step 5 Choose **Commands** > **Reset to Factory Default**.

Step 6 Click **Reset**.

Step 7 When prompted, confirm the reset.

Step 8 Reboot the controller without saving the configuration.

Step 9 Use the configuration wizard to enter configuration settings.

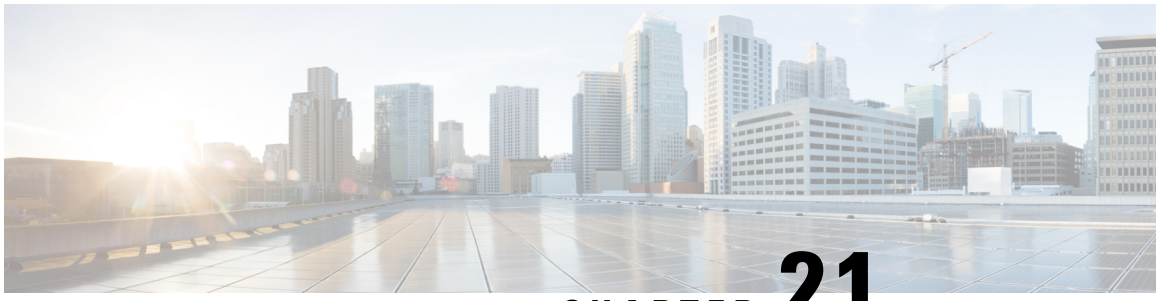
Resetting the Controller to Default Settings (CLI)

Step 1 Enter the **reset system** command. At the prompt that asks whether you need to save changes to the configuration, enter **N**. The unit reboots.

Step 2 When you are prompted for a username, enter the **recover-config** command to restore the factory-default configuration. The controller reboots and displays this message:

```
Welcome to the Cisco WLAN Solution Wizard Configuration Tool
```

Step 3 Use the configuration wizard to enter configuration settings.



CHAPTER 21

Managing Controller Software and Configurations

- Upgrading the Controller Software, on page 179
- Transferring Files to and from a Controller, on page 190
- Saving Configurations, on page 204
- Editing Configuration Files, on page 204
- Clearing the Controller Configuration, on page 205
- Erasing the Controller Configuration, on page 206
- Resetting the Controller, on page 206

Upgrading the Controller Software

When you upgrade the controller software, the software on the access points associated with the controller is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.

⚠

Caution Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image. Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported in the controller software release, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Considerations for Upgrading Controller Software

The following are some of the general restrictions that are applicable when upgrading the controller software. For any release-specific restrictions, see the relevant release notes.

For correct interoperability among Cisco Wireless infrastructure, including but not limited to mobility among controllers, AP compatibility, we recommend that you consult the *Cisco Wireless Solutions Software Compatibility Matrix* at:

https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

- For every software upgrade, we recommend that you consult the corresponding release notes for any caveats, considerations, or possible interim upgrades required to upgrade your controller(s) to the desired release of software.
- We recommend that you have a backup of your configuration in an external repository prior to any software upgrade activity.
- The upgrade of the controller software, with a fast connection to your TFTP, SFTP, or FTP file server, can take approximately 15 to 25 minutes or less from the start of the software transfer to reboot of controller (might take longer if the upgrade also includes a Field Upgrade Software installation during the same maintenance window). The time required for the upgrade of the associated APs might vary from one network to another, due to a variety of deployment-specific factors, such as number of APs associated with controller, speed of network connectivity between a given AP and the controller, and so on.
- We recommend that, during the upgrade process, you do not power off controller or any AP associated with the controller.
- Controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Download Software area in Cisco.com.
- The objects under the SNMP table bsnAPIfDot11CountersEntry like bsnAPIfDot11RetryCount, bsnAPIfDot11TransmittedFrameCount, and so on, per SNMP MIB description, are defined to use the index as 802.3 (Ethernet) MAC address of the AP. However, the controller sends the AP radio MAC address in snmpget, getnext, and getbulk. This is because the snmpwalk returns index using base radio MAC address instead of the AP Ethernet MAC address.
- You can reduce the network downtime using the following options:
  - You can predownload the AP image.

    For more information about predownloading the AP image, see the "Predownloading an Image to an Access Point" section.
  - For FlexConnect access points, use the FlexConnect Efficient AP upgrade feature to reduce traffic between the controller and the AP (main site and the branch).

    For more information about configuring FlexConnect AP upgrades, see the "Configuring FlexConnect AP Upgrades for FlexConnect APs" chapter.

Upgrading Controller Software (GUI)

Before you begin

Before upgrading the controller software, we recommend that you consult relevant release notes for any release-specific restrictions.

Step 1 Upload your controller configuration files to a server to back them up.

Note We highly recommend that you back up your configuration files of the controller prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Get the controller software image by following these steps:

a) Browse to http://www.cisco.com/cisco/software/navigator.html.
b) Choose **Wireless** > **Wireless LAN Controller**.

   The following options are available: **Integrated Controllers and Controller Modules**, **Mobility Express**, and **Standalone Controllers**.

c) Depending on your controller platform, click one of the above options.
d) Click the controller model number or name. The Download Software page is displayed.
e) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:

   Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

   Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

   Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

f) Choose a software release number.
g) Click the filename (*filename*.aes).
h) Click **Download**.
i) Read Cisco's End User Software License Agreement and then click **Agree**.
j) Save the file to your hard drive.
k) Repeat steps *a* through *k* to download the remaining file.

Step 3 Copy the controller software image (*filename*.aes) to the default directory on your TFTP or FTP server.

Note In Release 8.1 and later releases, transfer over HTTP is also supported.

Note In 8.3, 8.4, and 8.5 releases, for Cisco 2504 WLC, 5508 WLC, and WiSM2, the Cisco WLC software image is split into two images: Base Install Image and Supplementary AP Bundle Image. Therefore, to upgrade to 8.3, 8.4, or 8.5 release, you must repeat Step 2 through Step 14 to complete the installation of both Base Install Image and Supplementary AP Bundle Image.

Download the Supplementary AP Bundle Image only if you are using any of these APs: AP80x, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, and/or Cisco Aironet 1600 APs.

Step 4 (Optional) Disable the 802.11 networks.

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 5 Choose **Commands > Download File** to open the **Download File to Controller** page.

Step 6 From the **File Type** drop-down list, choose **Code**.

Step 7 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)
- **HTTP** (available in 8.1 and later releases)

Step 8 In the **IP Address** text box, enter the IP address of the server.

Step 9 (Optional) If you are using a TFTP server, the default values of 10 retries for the Maximum Retries text field, and 6 seconds for the Timeout text field should work correctly without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the **Maximum Retries** text box and the amount of time (in seconds) that the TFTP server attempts to download the software in the **Timeout** text box.

Step 10 In the **File Path** text box, enter the directory path of the software.

Step 11 In the **File Name** text box, enter the name of the controller software file (*filename*.aes).

Step 12 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** text box, enter the username to log into the FTP server.
b) In the **Server Login Password** text box, enter the password to log into the FTP server.
c) In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 13 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Note In 8.3, 8.4, and 8.5 releases, for Cisco 2504 WLC, 5508 WLC, and WiSM2, the Cisco WLC software image is split into two images: Base Install Image and Supplementary AP Bundle Image. Therefore, to upgrade to 8.3, 8.4, or 8.5 release, you must repeat Step 2 through Step 14 to complete the installation of both Base Install Image and Supplementary AP Bundle Image.

Download the Supplementary AP Bundle Image only if you are using any of these APs: AP80x, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, and/or Cisco Aironet 1600 APs.

Step 14 (Optional) After the download is complete, you can choose to predownload the image to your access points. For more information, see the "Predownloading an Image to an Access Point" section.

Step 15 Click **Reboot** to reboot the controller.

Step 16 If prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm.

Step 18 After the controller reboots, repeat step 6 to step 16 to install the remaining file.

Step 19 For Cisco WiSM2, reenable the controller port channel on the Catalyst switch.

Step 20 If you have disabled the 802.11 networks, reenable them.

Step 21 To verify the controller software version, choose **Monitor** on the controller GUI and see **Software Version** in the Controller Summary area.

Upgrading Controller Software (CLI)

Before you begin

Before upgrading the controller software, we recommend that you consult relevant release notes for any release-specific restrictions.

Step 1 Upload your controller configuration files to a server to back them up.

Note We highly recommend that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Get the controller software image by following these steps:

a) Browse to http://www.cisco.com/cisco/software/navigator.html.

b) Choose **Wireless** > **Wireless LAN Controller**.

The following options are available: **Integrated Controllers and Controller Modules**, **Mobility Express**, and **Standalone Controllers**.

c) Depending on your controller platform, click one of the above options.

d) Click the controller model number or name. The Download Software page is displayed.

e) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:

Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

f) Choose a software release number.

g) Click the filename (*filename*.aes).

h) Click **Download**.

i) Read Cisco's End User Software License Agreement and then click **Agree**.

j) Save the file to your hard drive.

k) Repeat steps *a* through *k* to download the remaining file.

Step 3 Copy the controller software image (*filename*.aes) to the default directory on your TFTP or FTP server.

Note In Release 8.3, for Cisco 2504 WLC, 5508 WLC, and WiSM2, the Cisco WLC software image is split into two images: Base Install Image and Supplementary AP Bundle Image. Therefore, to upgrade to Release 8.3 or later supported releases, you must repeat Step 2 through Step 11 to complete the installation of both Base Install Image and Supplementary AP Bundle Image.

Download the Supplementary AP Bundle Image only if you are using any of these APs: AP80x, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, and/or Cisco Aironet 1600 Series APs.

Step 4 Log onto the controller CLI.

Step 5 On the controller CLI over Telnet or SSH, enter the **ping server-ip-address** command to verify that the controller can contact the TFTP or FTP server.

Step 6 (Optional) Disable the 802.11 networks by entering this command:

config 802.11{a | b} disable network

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 7 View current download settings by entering the **transfer download start** command. Press **n** at the prompt to view the current download settings.

Step 8 Change the download settings, if necessary by entering these commands:

- **transfer download mode {tftp | ftp | sftp}**
- **transfer download datatype code**

- **transfer download serverip** *server-ip-address*
- **transfer download filename** *filename*
- **transfer download path** *server-path-to-file*

Note Pathnames on a TFTP or FTP server are relative to the server's default or root directory. For example, in the case of the Solaris TFTP server, the path is "/".

(Optional) If you are using a TFTP server, also enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

If you are using an FTP server, also enter these commands:

- **transfer download username** *username*
- **transfer download password** *password*
- (Optional) **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 9 View the current updated settings by entering the **transfer download start** command. Press **y** at the prompt to confirm the current download settings and start the software download.

Step 10 (Optional) After the download is complete, you can choose to predownload the image to your access points. For more information, see the "Predownloading an Image to an Access Point" section.

Step 11 Save the code update to nonvolatile NVRAM and reboot the controller by entering this command:

reset system

The controller completes the bootup process.

Step 12 After the controller reboots, repeat Steps 7 through 11 to install the remaining file.

Step 13 For Cisco WiSM2, re-enable the controller port channel on the Catalyst switch.

Step 14 If you have disabled the 802.11 networks in Step 6, renable them by entering this command:

config 802.11{a | b} enable network

Step 15 To verify the controller software that is installed, enter the **show sysinfo** command and see Product Version.

Step 16 (Optional) To verify the Cisco Unified Wireless Network Controller Boot Software file that is installed on the controller, enter the **show sysinfo** command on the controller CLI and see Recovery Image Version or Emergency Image Version.

Note If a Cisco Unified Wireless Network Controller Boot Software ER.aes file is not installed, Recovery Image Version or Emergency Image Version show 'N/A.'

Predownloading an Image to an Access Point

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

You can now download the upgrade image to the controller and then download the image to the access point while the network is still operational. You can also schedule a reboot of the controller and access points, either after a specified amount of time or at a specific date and time. When both devices are up, the access point discovers and rejoins the controller.

Concurrent Controller to AP Image Upgrade

This table lists the controllers and their maximum concurrent AP image download support.

Controller	Maximum Number of Concurrent AP Image Download Supported
Cisco 2504 WLC	75
Cisco 5508 WLC	500
Cisco 5520 WLC	1000
Cisco Flex 7510 WLC	1000
Cisco 8510 WLC	1000
Cisco 8540 WLC	1000
Cisco WiSM2	500
Cisco vWLC	1000

Flash Memory Requirements on Access Points

This table lists the Cisco AP models and the minimum amount of free flash memory required for the predownload process to work:

Cisco AP	Minimum Free Flash Memory Required
3700(I/E)	16 MB
3600(I/E)	14 MB
3502(I/E)	14 MB
2700(I/E)	16 MB
2602(I/E)	14 MB
1700(I/E)	16 MB

Cisco AP	Minimum Free Flash Memory Required
1602(I/E)	12 MB
1262	14 MB
1142	12 MB

Note

- The required flash memory can vary based on the radio type and the number of antennas used.
- This predownload feature is not supported on 1242 and 1131 Cisco AP models.
- Cisco AP1142 has 32 MB of total flash memory and can support the predownload feature.
- During the predownloading of image to APs, some APs do not have enough memory to keep the current radio firmware available. After the image has been predownloaded, these APs have the image only on flash memory and no other memory is available to host the current image or version radio firmware. The APs that have this limitation are as follows: Cisco Aironet 700, 1140, 1260, 1520, 1530, 1550, 1600, 3500, and 3600 Series APs.

  For more information about this limitation, see CSCvg41698.
- As part of the fix for CSCvb75682, if the flash memory of Cisco Aironet 1700, 2700, and 3700 Series APs is less than 10 Mb and a recovery image is present, the backup images in these APs are deleted.

Access Point Predownload Process

The access point predownload feature works as follows:

- The controller image is downloaded.
  - (Optional) The primary image becomes the backup image of the controller and the downloaded image becomes the new primary image. Change the current boot image as the backup image by using the **config boot backup** command to ensure that if a system failure occurs, the controller boots with the last working image of the controller.
  - Start the AP image predownload procedure for all joined APs or a specific AP, by entering the **config ap image predownload primary** {**all** | *ap-name*} command.
  - The upgrade image is downloaded as the backup image on the APs. You can verify this by using the **show ap image all** command.
  - Change the boot image to primary image manually using the **config boot primary** command and reboot the controller for the upgrade image to be activated.

    or
  - You issue a scheduled reboot with the **swap** keyword. The **swap** keyword has the following importance: The swapping occurs to the primary and backup images on the access point and the currently active image on controller with the backup image.
  - When the controller reboots, the access points are disassociated and eventually come up with an upgraded image. Once the controller responds to the discovery request sent by an access point with its discovery response packet, the access point sends a join request.

- The actual upgrade of the images occur. The following sequence of actions occur:
  - During boot time, the access point sends a join request.
  - The controller responds with the join response with the image version that the controller is running.
  - The access point compares its running image with the running image on the controller. If the versions match, the access point joins the controller.
  - If the versions do not match, the access point compares the version of the backup image and if they match, the access point swaps the primary and backup images and reloads and subsequently joins the controller.
  - If the primary image of the access point is the same as the controller image, the access point reloads and joins the controller.
  - If none of the above conditions are true, the access point sends an image data request to the controller, downloads the latest image, reloads, and joins the controller.

Note Normally, when upgrading the image of an AP, you can use the preimage download feature to reduce the amount of time the AP is unavailable to serve clients. However, it also increases the downtime because the AP cannot serve clients during an upgrade. The preimage download feature can be used to reduce this downtime. However, in the case of a branch office set up, the upgrade images are still downloaded to each AP over the WAN link, which has a higher latency.

A more efficient way is to use the FlexConnect AP Image Upgrade feature. When this feature is enabled, one AP of each model in the local network first downloads the upgrade image over the WAN link. For more information about FlexConnect AP upgrades, see the "FlexConnect AP Image Upgrades" chapter.

Guidelines and Restrictions for Predownloading an Image to an Access Point

- The 2600, 3500, and 3600 AP models can store only a single image in the flash. When you reboot the AP (without rebooting the controller after a pre-download), it will download the current image from the controller as the current image will be overwritten by the pre-downloaded image in the flash.
- The maximum number of concurrent predownloads is limited to half the number of concurrent normal image downloads. This limitation allows new access points to join the controller during image downloading.
- If you reach the predownload limit, then the access points that cannot get an image sleep for a time between 180 to 600 seconds and then reattempt the predownload.
- Before you predownload, you should change the active controller boot image to the backup image to ensure that if the controller reboots for some reason, it comes back up with the earlier running image, not the partially downloaded upgrade image.
- This predownload feature is not supported on 1242 and 1131 Cisco AP models.
- When the system time is changed by using the **config time** command, the time set for a scheduled reset is not valid and the scheduled system reset is canceled. You are given an option either to cancel the scheduled reset before configuring the time or retain the scheduled reset and not configure the time.

- All the primary, secondary, and tertiary controllers should run the same images as the primary and backup images. That is, the primary image of all three controllers should be X and the secondary image of all three controllers should be Y or the feature is not effective.

  Having different versions of the controller software running on primary, secondary, and tertiary controllers adds unnecessary and protracted delays to APs failing over and joining the other available controllers in an N+1 setup. This is due to the APs being forced to download different image versions when failing over to a secondary or tertiary controller, and joining back to their primary controller when it is available.

- At the time of the reset, if any AP is downloading the controller image, the scheduled reset is canceled. The following message appears with the reason why the scheduled reset was canceled:

  ```
  %OSAPI-3-RESETSYSTEM_FAILED: osapi_task.c:4458 System will not reset as software is
  being upgraded.
  ```

- Predownloading a 7.2 or later version of image on a Cisco Aironet 1240 access point is not supported when upgrading from a previous controller release. If predownloading is attempted to the Cisco Aironet 1240 access point, the AP gets disconnected.

- There are two images for the1550 Mesh AP - 1550 with 64 MB memory and 1550 with 128 MB memory. During the controller upgrade to 7.6 and higher versions, the AP images are downloaded and there are two reboots.

- If you upgrade from a release that is prior to Release 7.5 directly to Release 7.6.X or a later release, the predownload process on Cisco AP2600 and AP3600 fails. After the controller is upgraded to Release 7.6.X or a later release, the new image is loaded on Cisco AP2600 and AP3600. After the upgrade to a Release 7.6.X image, the predownload functionality works as expected. The predownload failure is only a one-time failure.

- If you upgrade from 8.2 to 8.4 release, the predownload process on Cisco AP1700, AP2700, or AP3700 fails with the following error message:

  ```
  Not enough free space to download.
  ```

  After the controller is reloaded with 8.4, the backup image version still shows up as 3.0.

- If an AP is in the process of downloading a software image, the status of the download is not shown on the controller CLI. During the image download process, any configuration performed on the AP via the controller CLI is not applied. Therefore, we recommend that you do not perform any configuration on the AP via the controller CLI if an image download on the AP is in progress.

Predownloading an Image to Access Points—Global Configuration (GUI)

To predownload an image to the APs, you must perform the following steps after upgrading your controller software image and before you reboot the controller for the new image to take effect.

Step 1 To configure the predownloading of access point images globally, choose **Wireless > Access Points > Global Configuration** to open the **Global Configuration** page.

Step 2 In the **AP Image Pre-download** section, perform one of the following:

- To instruct all the access points to predownload a primary image from the controller, click **Download Primary** under the AP Image Pre-download.
- To instruct all the access points to swap their primary and backup images, click **Interchange Image**.

- To download an image from the controller and store it as a backup image, click **Download Backup**.
- To terminate the predownload operation, click **Abort Predownload**.

Step 3 Click **OK**.

Step 4 Click **Apply**.

Predownloading an Image to Access Points (CLI)

To predownload an image to the APs, you must perform the following steps after upgrading your controller software image and before you reboot the controller for the new image to take effect.

Step 1 Specify APs that will receive the predownload image by entering one of these commands:

- Specify APs for predownload by entering this command:

  config ap image predownload {**primary** | **backup**} {*ap_name* | **all**}

  The primary image is the new image; the backup image is the existing image. APs always boot with the primary image.

- Swap an AP's primary and backup images by entering this command:

  config ap image swap {*ap_name* | **all**}

- Display detailed information on APs specified for predownload by entering this command:

  show ap image {**all** | *ap-name*}

The output lists APs that are specified for predownloading and provides for each AP, primary and secondary image versions, the version of the predownload image, the predownload retry time (if necessary), and the number of predownload attempts. The output also includes the predownload status for each device. The status of the APs is as follows:

- None—The AP is not scheduled for predownload.
- Predownloading—The AP is predownloading the image.
- Not supported—The AP (1120, 1230, and 1310) does not support predownloading.
- Initiated—The AP is waiting to get the predownload image because the concurrent download limit has been reached.
- Failed—The AP has failed 64 predownload attempts.
- Complete—The AP has completed predownloading.

Step 2 Set a reboot time for the controller and the APs.

Use one of these commands to schedule a reboot of the controller and APs:

- Specify the amount of time delay before the devices reboot by entering this command:

  reset system in *HH*:*MM*:*SS* **image** {**swap** | **no-swap**} **reset-aps** [**save-config**]

  Note The **swap** operand in the **reset** command will result in the swapping of the primary and backup images on both the controller and the AP and sets the default flag on the next controller reboot.

  The controller sends a reset message to all joined APs, and then the controller resets.

- Specify a date and time for the devices to reboot by entering this command:

  reset system at *YYYY-MM-DD HH*:*MM*:*SS* **image** {**swap** | **no-swap**} **reset-aps** [**save-config**]

  The controller sends a reset message to all joined APs, and then the controller resets.

  Note The **swap** operand in the **reset** command will result in the swapping of the primary and backup images on both the controller and the AP.

- (Optional) Set up an SNMP trap message that announces the upcoming reset by entering this command:

  reset system notify-time *minutes*

  The controller sends the announcement trap *the configured number of minutes* before the reset.

- Cancel the scheduled reboot by entering this command:

  reset system cancel

  Note If you configure reset times and then use the **config time** command to change the system time on the controller, the controller notifies you that any scheduled reset times will be canceled and must be reconfigured after you set the system time.

Use the **show reset** command to display scheduled resets.

Information similar to the following appears:

```
System reset is scheduled for Apr 08 01:01:01 2010.
Current local time and date is Apr 07 02:57:44 2010.
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

Transferring Files to and from a Controller

Controllers have built-in utilities for uploading and downloading various files. Follow the instructions in these sections to import files using either the controller GUI or CLI:

Downloading a Login Banner File

You can download a login banner file using either the GUI or the CLI. The login banner is the text that appears on the page before user authentication when you access the controller GUI or CLI using Telnet, SSH, or a console port connection.

You save the login banner information as a text (*.txt) file. The text file cannot be larger than 1296 characters and cannot have more than 16 lines of text.

Note The ASCII character set consists of printable and nonprintable characters. The login banner supports only printable characters.

Here is an example of a login banner:

```
Welcome to the Cisco Wireless Controller!
Unauthorized access prohibited.
Contact sysadmin@corp.com for access.
```

Follow the instructions in this section to download a login banner to the controller through the GUI or CLI. However, before you begin, make sure that you have a TFTP or FTP server available for the file download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.

Downloading a Login Banner File (GUI)

Step 1 Copy the login banner file to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the **Download File to Controller** page.

Step 3 From the **File Type** drop-down list, choose **Login Banner**.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 5 In the **IP Address** field, enter the IP address of the server type you chose in Step 4.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fieldes should work correctly without any adjustment. However, you can change these values.

Step 6 (Optional) Enter the maximum number of times that the TFTP server attempts to download the certificate in the **Maximum Retries** field and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the **Timeout** field.

Step 7 In the **File Path** field, enter the directory path of the login banner file.

Step 8 In the **File Name** field, enter the name of the login banner text (*.txt) file.

Step 9 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.
b) In the **Server Login Password** field, enter the password to log into the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the login banner file to the controller. A message appears indicating the status of the download.

Downloading a Login Banner File (CLI)

Step 1 Log onto the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Download the controller login banner by entering this command:

transfer download datatype login-banner

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer download serverip server-ip-address

Step 5 Specify the name of the config file to be downloaded by entering this command:

transfer download path server-path-to-file

Step 6 Specify the directory path of the config file by entering this command:

transfer download filename *filename.txt*

Step 7 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands:

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 9 View the download settings by entering the **transfer download start** command. Enter **y** when prompted to confirm the current settings and start the download process.

Clearing the Login Banner (GUI)

Step 1 Choose **Commands** > **Login Banner** to open the Login Banner page.

Step 2 Click **Clear**.

Step 3 When prompted, click **OK** to clear the banner.

To clear the login banner from the controller using the controller CLI, enter the **clear login-banner** command.

Downloading Device Certificates

Each wireless device (controller, access point, and client) has its own device certificate. For example, the controller is shipped with a Cisco-installed MIC device certificate.

Note For more information about configuring local EAP, see the "Configuring Local EAP" section.

Follow the instructions in this section to download a vendor-specific device certificate to the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the certificate download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Note All certificates downloaded to the controller must be in PEM format.

Note Clients using Microsoft Windows 10 with default (zero-touch config) supplicant fail to connect to controller when there is no CA certificate to validate the server certificate. This is because the supplicant does not pop up a window to accept the server certificate and silently rejects the 802.1X authentication. Therefore, we recommend that you do either of the following:

- Manually install a third-party CA certificate on the AAA server, which the clients using Microsoft Windows 10 can trust.
- Use any other supplicant, such as Cisco AnyConnect, which pops up a window to trust or not trust the server certificate. If you accept the trust certificate, then the client is authenticated.

Downloading Device Certificates (GUI)

Step 1 Copy the device certificate to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the File Type drop-down list, choose **Vendor Device Certificate**.

Step 4 In the Certificate Password text box, enter the password that was used to protect the certificate.

Step 5 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 6 In the IP Address text box, enter the IP address of the server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 7 Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

Step 8 In the File Path text box, enter the directory path of the certificate.

Step 9 In the File Name text box, enter the name of the certificate.

Step 10 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.
b) In the Server Login Password text box, enter the password to log into the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 11 Click **Download** to download the device certificate to the controller. A message appears indicating the status of the download.

Step 12 After the download is complete, choose **Commands** > **Reboot** > **Reboot**.

Step 13 If prompted to save your changes, click **Save and Reboot**.

Step 14 Click **OK** to confirm your decision to reboot the controller.

Downloading Device Certificates (CLI)

Step 1 Log onto the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the type of the file to be downloaded by entering this command:

transfer download datatype eapdevcert

Step 4 Specify the certificate's private key by entering this command:

transfer download certpassword *password*

Step 5 Specify the IP address of the TFTP or FTP server by entering this command:

transfer download serverip *server-ip-address*

Step 6 Specify the name of the config file to be downloaded by entering this command:

transfer download path *server-path-to-file*

Step 7 Specify the directory path of the config file by entering this command:

transfer download filename *filename.pem*

Step 8 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 9 If you are using an FTP server, enter these commands (skip this step if you are not using FTP server):

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 10 View the updated settings by entering the **transfer download start** command. Answer **y** when prompted to confirm the current settings and start the download process.

Step 11 Reboot the controller by entering this command:

reset system

Downloading CA Certificates

Controllers and access points have a Certificate Authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate may be used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, it must be downloaded to the controller.

Note For more information about configuring local EAP, see the "Configuring Local EAP" section.

Follow the instructions in this section to download CA certificates to the controller through the GUI or CLI. However, before you begin, make sure that you have a TFTP or FTP server available for the certificate download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.

- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Note All certificates downloaded to the controller must be in PEM format.

Download CA Certificates (GUI)

Step 1 Copy the CA certificate to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the File Type drop-down list, choose **Vendor CA Certificate**.

Step 4 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 5 In the IP Address text box, enter the IP address of the server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

Step 7 In the File Path text box, enter the directory path of the certificate.

Step 8 In the File Name text box, enter the name of the certificate.

Step 9 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log on to the FTP server.
b) In the Server Login Password text box, enter the password to log on to the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the CA certificate to the controller. A message appears indicating the status of the download.

Step 11 After the download is complete, choose **Commands** > **Reboot** > **Reboot**.

Step 12 If prompted to save your changes, click **Save and Reboot**.

Step 13 Click **OK** to confirm your decision to reboot the controller.

Downloading CA Certificates (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the type of the file to be downloaded by entering this command:
transfer download datatype eapdevcert

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip *server-ip-address*

Step 5 Specify the directory path of the config file by entering this command:
transfer download path *server-path-to-file*

Step 6 Specify the name of the config file to be downloaded by entering this command:
transfer download filename *filename*

Step 7 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands (skip this step if you are not using FTP server):

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering the **transfer download start** command. Answer y when prompted to confirm the current settings and start the download process.

Step 10 Reboot the controller by entering the **reset system** command.

Uploading PACs

Protected access credentials (PACs) are credentials that are either automatically or manually provisioned and used to perform mutual authentication with a local EAP authentication server during EAP-FAST authentication. When manual PAC provisioning is enabled, the PAC file is manually generated on the controller.

Follow the instructions in this section to generate and load PACs from the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the PAC upload. Follow these guidelines when setting up a TFTP or FTP server:

- If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.

- If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.

This section contains the following subsections:

Uploading PACs (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **PAC (Protected Access Credential)**.

Step 3 In the **User** text box, enter the name of the user who will use the PAC.

Step 4 In the **Validity** text box, enter the number of days for the PAC to remain valid. The default setting is zero (0).

Step 5 In the **Password** and **Confirm Password** text boxes, enter a password to protect the PAC.

Step 6 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 7 In the **IP Address (IPv4/IPv6)** text box, enter the IPv4/IPv6 address of the server.

Step 8 In the **File Path** text box, enter the directory path of the PAC.

Step 9 In the **File Name** text box, enter the name of the PAC file. PAC files have a .pac extension.

Step 10 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** text box, enter the username to log into the FTP server.
b) In the **Server Login Password** text box, enter the password to log into the FTP server.
c) In the **Server Port Number** text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 11 Click **Upload** to upload the PAC from the controller. A message appears indicating the status of the upload.

Step 12 Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.

Uploading PACs (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to upload the config file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 3 Upload a Protected Access Credential (PAC) by entering this command:

transfer upload datatype pac

Step 4 Specify the identification of the user by entering this command:

transfer upload pac *username validity password*

Step 5 Specify the IP address of the TFTP or FTP server by entering this command:

transfer upload serverip *server-ip-address*

Note The server supports both, IPv4 and IPv6.

Step 6 Specify the directory path of the config file by entering this command:

transfer upload path *server-path-to-file*

Step 7 Specify the name of the config file to be uploaded by entering this command:

transfer upload filename *manual*.pac.

Step 8 If you are using an FTP server, enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering the **transfer upload start** command. Answer y when prompted to confirm the current settings and start the upload process.

Step 10 Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.

Backing Up and Restoring Controller Configuration

We recommend that you upload your controller's configuration file to a server to back it up. If you lose your configuration, you can then download the saved configuration to the controller.

Caution Do not download a configuration file to your controller directly that was uploaded from a different controller platform. For example, a Cisco 5508 controller does not support the configuration file from a Cisco 2504 controller. To properly convert the configuration files from one controller platform to another, use the WLC Config Converter tool available at https://cway.cisco.com/tools/WirelessConfigConverter/.

Note While controller configuration backup is in progress, we recommend you do not initiate any new configuration or modify any existing configuration settings. This is to avoid corrupting the configuration file.

Follow these guidelines when working with configuration files:

- Any CLI with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup. A configuration may be rejected if the validation fails. A configuration may fail if you have an invalid CLI. For example, if you have a CLI where you try to configure a WLAN without adding appropriate commands to add the WLAN.
- A configuration may be rejected if the dependencies are not addressed. For example, if you try to configure dependent parameters without using the add command. The XML validation may succeed but the configuration download infrastructure will immediately reject the configuration with no validation errors.

- An invalid configuration can be verified by using the **show invalid-config** command. The **show invalid-config** command reports the configuration that is rejected by the controller either as part of download process or by XML validation infrastructure.

Note You can also read and modify the configuration file via a text editor, to correct any incorrect configuration commands. After you are done, you can save the changes and once again try the configuration download to the controller in question.

- A wireless client that connects to the controller when Management over Wireless has been enabled can still conduct an upgrade using the newer HTTP transfer method.

Uploading Configuration Files

You can upload configuration files using either the GUI or the CLI.

Uploading the Configuration Files (GUI)

Step 1 Choose **Commands** > **Upload File** to open the **Upload File from Controller** page.

Step 2 From the **File Type** drop-down list, choose **Configuration**.

Step 3 (Optional) Encrypt the configuration file by checking the **Configuration File Encryption** check box and entering the encryption key in the **Encryption Key** field.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 5 In the **IP Address** field, enter the IP address of the server.

Step 6 In the **File Path** field, enter the directory path of the configuration file.

Step 7 In the **File Name** field, enter the name of the configuration file.

Step 8 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.
b) In the **Server Login Password** field, enter the password to log into the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 9 Click **Upload** to upload the configuration file to the server. A message appears indicating the status of the upload. If the upload fails, repeat this procedure and try again.

Uploading the Configuration Files (CLI)

Step 1 Specify the transfer mode used to upload the configuration file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 2 Specify the type of file to be uploaded by entering this command:

transfer upload datatype config

Step 3 (Optional) Encrypt the configuration file by entering these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key,* where *key* is the encryption key used to encrypt the file.

Step 4 Specify the IP address of the server by entering this command:
transfer upload serverip *server-ip-address*

Step 5 Specify the directory path of the configuration file by entering this command:
transfer upload path *server-path-to-file*

Step 6 Specify the name of the configuration file to be uploaded by entering this command:
transfer upload filename *filename*

Step 7 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the upload occurs:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 8 Initiate the upload process by entering this command:
transfer upload start

Step 9 When prompted to confirm the current settings, answer **y**.

Information similar to the following appears:

```
Mode............................................. TFTP
TFTP Server IP................................... 224.0.0.1
TFTP Path........................................ Config/
TFTP Filename.................................... AS_5520_x_Config.xml
Data Type........................................ Config File
Encryption....................................... Disabled

************************************************
***  WARNING: Config File Encryption Disabled  ***
************************************************

Are you sure you want to start? (y/N) Y
File transfer operation completed successfully.
```

If the upload fails, repeat this procedure and try again.

Downloading Configuration Files

You can download configuration files using either the GUI or the CLI.

Downloading the Configuration Files (GUI)

Step 1 Choose **Commands** > **Download File** to open the **Download File to Controller** page.

Step 2 From the **File Type** drop-down list, choose **Configuration**.

Step 3 If the configuration file is encrypted, check the **Configuration File Encryption** check box and enter the encryption key used to decrypt the file in the **Encryption Key** field.

Note The key that you enter here should match the one entered during the upload process.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 5 In the **IP Address** field, enter the IP address of the server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the **Maximum Retries** and **Timeout** fields should work correctly without any adjustment. However, you can change these values.

Step 6 (Optional) Enter the maximum number of times that the TFTP server attempts to download the configuration file in the **Maximum Retries** field and the amount of time (in seconds) that the TFTP server attempts to download the configuration file in the **Timeout** field.

Step 7 In the **File Path** field, enter the directory path of the configuration file.

Step 8 In the **File Name** field, enter the name of the configuration file.

Step 9 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.
b) In the **Server Login Password** field, enter the password to log into the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the file to the controller. A message appears indicating the status of the download, and the controller reboots automatically. If the download fails, repeat this procedure and try again.

Downloading the Configuration Files (CLI)

Note The controller does not support incremental configuration downloads. The configuration file contains all mandatory commands (all interface address commands, mgmtuser with read-write permission commands, and interface port or LAG enable or disable commands) required to successfully complete the download. For example, if you download only the **config time ntp server** *index server_address* command as part of the configuration file, the download fails. Only the commands present in the configuration file are applied to the controller, and any configuration in the controller prior to the download is removed.

Step 1 Specify the transfer mode used to download the configuration file by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 2 Specify the type of file to be downloaded by entering this command:

transfer download datatype config

Step 3 If the configuration file is encrypted, enter these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key*, where *key* is the encryption key used to decrypt the file.

Note The key that you enter here should match the one entered during the upload process.

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip *server-ip-address*

Step 5 Specify the directory path of the configuration file by entering this command:
transfer download path *server-path-to-file*

Step 6 Specify the name of the configuration file to be downloaded by entering this command:
transfer download filename *filename*

Step 7 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the download occurs:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering this command:
transfer download start

Step 10 When prompted to confirm the current settings and start the download process, answer **y**.

Information similar to the following appears:

```
Mode............................................. TFTP
TFTP Server IP................................... 224.0.0.1
TFTP Path........................................ Config/
TFTP Filename.................................... AS_5520_x_Config.xml
Data Type........................................ Config File
Encryption....................................... Disabled

************************************************
***  WARNING: Config File Encryption Disabled  ***
************************************************
```

```
Are you sure you want to start? (y/N) y

File transfer operation completed successfully.
```

If the download fails, repeat this procedure and try again.

Saving Configurations

Controllers contain two types of memory: volatile RAM and NVRAM. At any time, you can save the configuration changes from active volatile RAM to nonvolatile RAM (NVRAM). You are prompted to save your configuration automatically whenever you initiate a reboot of the controller or log out of a GUI or a CLI session. The following are some examples of the corresponding commands:

- **save config**—Saves the configuration from volatile RAM to NVRAM without resetting the controller.
- **reset system**—Prompts you to confirm that you want to save configuration changes before the controller reboots.
- **logout**—Prompts you to confirm that you want to save configuration changes before you log out.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. Controller software release 5.2 or later releases enable you to easily read and modify the configuration file by converting it to CLI format. When you upload the configuration file to a TFTP/FTP/SFTP server, the controller initiates the conversion from XML to CLI. You can then read or edit the configuration file in a CLI format on the server. When you are finished, you download the file back to the controller, where it is reconverted to an XML format and saved.

Step 1 Upload the configuration file to a TFTP/FTP/SFTP server by performing one of the following:

- Upload the file using the controller GUI.
- Upload the file using the controller CLI.

Step 2 Read or edit the configuration file on the server. You can modify or delete existing CLI commands and add new CLI commands to the file.

Note To edit the configuration file, you can use your text editor of choice such as Notepad or Wordpad on Windows platforms, VI editor on Linux, and so forth.

Step 3 Save your changes to the configuration file on the server.

Step 4 Download the configuration file to the controller by performing one of the following:

- Download the file using the controller GUI.
- Download the file using the controller CLI.

The controller converts the configuration file to an XML format, saves it to flash memory, and then reboots using the new configuration. CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter this command:

show invalid-config

Note You cannot execute this command after the **clear config** or **save config** command.

Step 5 If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP or FTP server for analysis. To do so, perform one of the following:

- Upload the invalid configuration using the controller GUI. Follow the instructions in the Uploading Configuration Files (GUI) section but choose **Invalid Config** from the **File Type** drop-down list in *Step 2* and skip *Step 3*.
- Upload the invalid configuration using the controller CLI. Follow the instructions in the Uploading Configuration Files (CLI) section but enter the transfer **upload datatype invalid-config command** in *Step 2* and skip *Step 3*.

Step 6 The controller does not support the uploading and downloading of port configuration CLI commands. If you want to configure the controller ports, enter these commands:

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}—Enables or disables the up and down link traps for a specific controller port or for all ports.
- **config port adminmode** {*port* | **all**} {**enable** | **disable**}—Enables or disables the administrative mode for a specific controller port or for all ports.

Step 7 Save your changes by entering this command:

save config

Clearing the Controller Configuration

Step 1 Clear the configuration by entering this command:

clear config

Enter **y** at the confirmation prompt to confirm the action.

Step 2 Reboot the system by entering this command:

reset system

Enter **n** to reboot without saving configuration changes. When the controller reboots, the configuration wizard starts automatically.

Step 3 Follow the instructions in the Configuring the Controller-Using the Configuration Wizard section to complete the initial configuration.

Erasing the Controller Configuration

Step 1 Reset the configuration by entering this command:

reset system

At the confirmation prompt, enter y to save configuration changes to NVRAM. The controller reboots.

Step 2 When you are prompted for a username, restore the factory-default settings by entering this command:

recover-config

The controller reboots and the configuration wizard starts automatically.

Step 3 Follow the instructions in the Configuring the Controller-Using the Configuration Wizard section to complete the initial configuration.

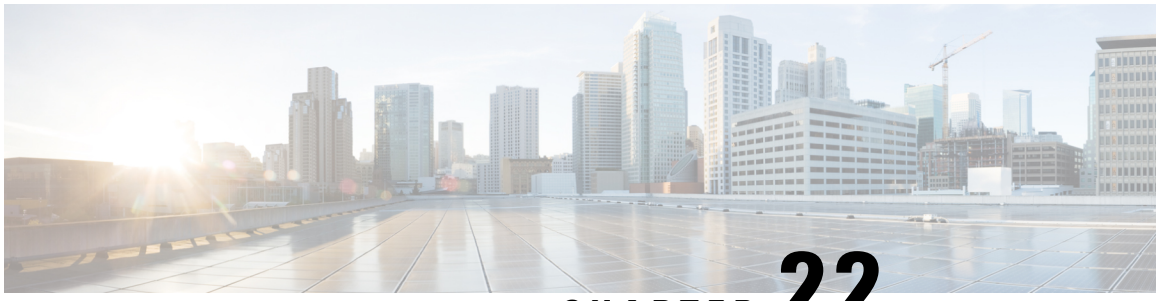
Resetting the Controller

You can reset the controller and view the reboot process on the CLI console using one of the following two methods:

- Turn the controller off and then turn it back on.
- On the CLI, enter reset system. At the confirmation prompt, enter y to save configuration changes to NVRAM. The controller reboots.

When the controller reboots, the CLI console displays the following reboot information:

- Initializing the system.
- Verifying the hardware configuration.
- Loading microcode into memory.
- Verifying the operating system software load.
- Initializing with its stored configurations.
- Displaying the login prompt.



CHAPTER 22

Managing User Accounts

- Configuring Guest User Accounts, on page 207
- Configuring Administrator Usernames and Passwords, on page 210
- Changing the Default Values for SNMP v3 Users, on page 212
- Generating a Certificate Signing Request using OpenSSL, on page 213

Configuring Guest User Accounts

Guest Accounts

The controller can provide guest user access on WLANs for which you must create guest user accounts. Guest user accounts can be created by network administrators, or, if you would like a non-administrator to be able to create guest user accounts on demand, you can do so through a lobby administrator account. The lobby ambassador has limited configurration privileges and has access only to the web pages used to manage the guest user accounts.

The lobby ambassador can specify the amount of time that the guest user accounts remain active. After the specified time elapses, the guest user accounts expire automatically.

This section contains the following subsections:

Restrictions on Managing User Accounts

- The local user database is limited to a maximum of 2048 entries, which is also the default value. This database is shared by local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries, and access point authorization list entries. Together they cannot exceed the configured maximum value.
- For net user accounts or guest user accounts, the following special characters are allowed along with alphanumeric characters: ~, @, #, $, %, ^, &, (,), !, _, -, `, ., [,], =, +, *, :, ;, {, }, ,, /, and \.

Creating a Lobby Ambassador Account

Creating a Lobby Ambassador Account (GUI)

Step 1 Choose **Management > Local Management Users** to open the Local Management Users page.

This page lists the names and access privileges of the local management users.

Note If you want to delete any of the user accounts from the controller, hover your cursor over the blue drop-down arrow and choose **Remove**. However, deleting the default administrative user prohibits both GUI and CLI access to the controller. Therefore, you must create a user with administrative privileges (ReadWrite) before you remove the default user.

Step 2 Click **New** to create a lobby ambassador account. The Local Management Users > New page appears.

Step 3 In the User Name text box, enter a username for the lobby ambassador account.

Note Management usernames must be unique because they are stored in a single database.

Step 4 In the **Password** and **Confirm Password** text boxes, enter a password for the lobby ambassador account.

Note Passwords are case sensitive. The settings for the management User Details parameters depends on the settings that you make in the Password Policy page. The following requirements are enforced on the 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 a management username or the reverse letters of a 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.
- If you want to downgrade from Release 8.6 to Release 8.5 or an earlier release, ensure that you have a management user account password that is less than or equal to 24 characters to be compatible with the earlier releases. Else, during the downgrade and before you can reboot the controller, you will be prompted with the following message:

  `"Warning!!! Please Configure Mgmt user compatible with older release"`

Step 5 Choose **LobbyAdmin** from the User Access Mode drop-down list. This option enables the lobby ambassador to create guest user accounts.

Note The ReadOnly option creates an account with read-only privileges, and the ReadWrite option creates an administrative account with both read and write privileges.

Step 6 Click **Apply** to commit your changes. The new lobby ambassador account appears in the list of local management users.

Step 7 Click **Save Configuration** to save your changes.

Creating a Lobby Ambassador Account (CLI)

Procedure

- To create a lobby ambassador account use the following command:

config mgmtuser add *lobbyadmin_username lobbyadmin_pwd* **lobby-admin**

Note Replacing **lobby-admin** with **read-only** creates an account with read-only privileges. Replacing **lobby-admin** with **read-write** creates an administrative account with both read and write privileges.

Creating Guest User Accounts as a Lobby Ambassador (GUI)

Step 1 Log into the controller as the lobby ambassador, using the username and password. The Lobby Ambassador Guest Management > Guest Users List page appears.

Step 2 Click **New** to create a guest user account. The Lobby Ambassador Guest Management > Guest Users List > New page appears.

Step 3 In the User Name text box, enter a name for the guest user. You can enter up to 24 characters.

Step 4 Perform one of the following:

- If you want to generate an automatic password for this guest user, select the **Generate Password** check box. The generated password is entered automatically in the Password and Confirm Password text boxes.
- If you want to create a password for this guest user, leave the **Generate Password** check box unselected and enter a password in both the **Password** and **Confirm Password** text boxes.

  Note Passwords can contain up to 24 characters (Release 8.5 and earlier releases) and 127 characters (Release 8.6 and later releases) and are case sensitive.

Step 5 From the Lifetime drop-down lists, choose the amount of time (in days, hours, minutes, and seconds) that this guest user account is to remain active. A value of zero (0) for all four text boxes creates a permanent account.

Default: 1 day

Range: 5 minutes to 30 days

Note The smaller of this value or the session timeout for the guest WLAN, which is the WLAN on which the guest account is created, takes precedence. For example, if a WLAN session timeout is due to expire in 30 minutes but the guest account lifetime has 10 minutes remaining, the account is deleted in 10 minutes upon guest account expiry. Similarly, if the WLAN session timeout expires before the guest account lifetime, the client experiences a recurring session timeout that requires reauthentication.

Note You can change a guest user account with a nonzero lifetime to another lifetime value at any time while the account is active. However, to make a guest user account permanent using the controller GUI, you must delete the account and create it again. If desired, you can use the **config netuser lifetime** *user_name 0* command to make a guest user account permanent without deleting and recreating it.

Step 6 From the WLAN SSID drop-down list, choose the SSID that will be used by the guest user. The only WLANs that are listed are those WLANs for which Layer 3 web authentication has been configured.

Note We recommend that you create a specific guest WLAN to prevent any potential conflicts. If a guest account expires and it has a name conflict with an account on the RADIUS server and both are on the same WLAN, the users associated with both accounts are disassociated before the guest account is deleted.

Step 7 In the Description text box, enter a description of the guest user account. You can enter up to 32 characters.

Step 8 Click **Apply** to commit your changes. The new guest user account appears in the list of guest users on the Guest Users List page.

From this page, you can see all of the guest user accounts, their WLAN SSID, and their lifetime. You can also edit or remove a guest user account. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.

Step 9 Repeat this procedure to create any additional guest user accounts.

Viewing Guest User Accounts

Viewing the Guest Accounts (GUI)

Choose **Security** > **AAA** > **Local Net Users**. The Local Net Users page appears.

From this page, you can see all of the local net user accounts (including guest user accounts) and can edit or remove them as desired. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.

Viewing the Guest Accounts (CLI)

Procedure

	Command or Action	Purpose
Step 1	To see all of the local net user accounts (including guest user accounts) using the controller CLI, enter this command:	**show netuser summary**

Configuring Administrator Usernames and Passwords

Administrator Usernames and Passwords

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

Configuring Usernames and Passwords (GUI)

Step 1 Choose **Management** > **Local Management Users**.

Step 2 Click **New**.

Step 3 Enter the username and password, and confirm the password.

Usernames and passwords are case-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.

Step 4 Choose the User Access Mode as one of the following:

- **ReadOnly**
- **ReadWrite**
- **LobbyAdmin**

Step 5 Click **Apply**.

Configuring Usernames and Passwords (CLI)

Step 1 Configure a username and password by entering one of these commands:

- **config mgmtuser add** *username password* **read-write** *description*—Creates a username-password pair with read-write privileges.
- **config mgmtuser add** *username password* **read-only** *description*—Creates a username-password pair with read-only privileges.

  Usernames and passwords are case-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.

  Note If you ever need to change the password for an existing username, enter the **config mgmtuser password** *username new_password* command.

- **config mgmtuser add** *username password* **lobby-admin** *description*—Creates a username-password pair with Lobby Administrator privileges.

Step 2 List the configured users by entering this command:

show mgmtuser

Restoring Passwords

Before you begin

Ensure that you are accessing the controller CLI through the console port.

Step 1 After the controller boots up, enter **Restore-Password** at the User prompt.

Note For security reasons, the text that you enter does not appear on the controller console.

Step 2 At the Enter User Name prompt, enter a new username.

Step 3 At the Enter Password prompt, enter a new password.

Step 4 At the Re-enter Password prompt, reenter the new password. The controller validates and stores your entries in the database.

Step 5 When the User prompt reappears, enter your new username.

Step 6 When the Password prompt appears, enter your new password. The controller logs you in with your new username and password.

Changing the Default Values for SNMP v3 Users

Information About Changing the Default Values for SNMP v3 Users

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

Note SNMP v3 is time sensitive. Ensure that you configure the correct time and time zone on your controller.

Changing the SNMP v3 User Default Values (GUI)

Step 1 Choose **Management** > **SNMP** > **SNMP V3 Users** to open the SNMP V3 Users page.

Step 2 If "default" appears in the User Name column, hover your cursor over the blue drop-down arrow for the desired user and choose **Remove** to delete this SNMP v3 user.

Step 3 Click **New** to add a new SNMP v3 user. The SNMP V3 Users > New page appears.

Step 4 In the User Profile Name text box, enter a unique name. Do not enter "default."

Step 5 Choose **Read Only** or **Read Write** from the Access Mode drop-down list to specify the access level for this user. The default value is Read Only.

Step 6 From the Authentication Protocol drop-down list, choose the desired authentication method: **None**, **HMAC-MD5** (Hashed Message Authentication Coding-Message Digest 5), or **HMAC-SHA** (Hashed Message Authentication Coding-Secure Hashing Algorithm). The default value is HMAC-SHA.

Step 7 In the Auth Password and Confirm Auth Password text boxes, enter the shared secret key to be used for authentication. You must enter at least 12 characters that include both letters and numbers.

Step 8 From the Privacy Protocol drop-down list, choose the desired encryption method: **None**, **CBC-DES** (Cipher Block Chaining-Digital Encryption Standard), or **CFB-AES-128** (Cipher Feedback Mode-Advanced Encryption Standard-128). The default value is CFB-AES-128.

Note In order to configure CBC-DES or CFB-AES-128 encryption, you must have selected either HMAC-MD5 or HMAC-SHA as the authentication protocol in Step 6.

Step 9 In the Priv Password and Confirm Priv Password text boxes, enter the shared secret key to be used for encryption. You must enter at least 12 characters that include both letters and numbers.

Step 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Step 12 Reboot the controller so that the SNMP v3 user that you added takes effect.

Changing the SNMP v3 User Default Values (CLI)

Step 1 See the current list of SNMP v3 users for this controller by entering this command:

show snmpv3user

Step 2 If "default" appears in the SNMP v3 User Name column, enter this command to delete this user:

config snmp v3user delete *username*

The *username* parameter is the SNMP v3 username (in this case, "default").

Step 3 Create a new SNMP v3 user by entering this command:

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} *auth_key encrypt_key*

where

- *username* is the SNMP v3 username.
- **ro** is read-only mode and **rw** is read-write mode.
- **none**, **hmacmd5**, and **hmacsha** are the authentication protocol options.
- **none**, **des**, and **aescfb128** are the privacy protocol options.
- *auth_key is the authentication shared secret key.*
- *encrypt_key is the encryption shared secret key.*

  Do not enter "default" for the *username*, *auth_key*, and *encrypt_key* parameters.

Step 4 Enter the **save config** command.

Step 5 Reboot the controller so that the SNMP v3 user that you added takes effect by entering **reset system** command.

Generating a Certificate Signing Request using OpenSSL

Step 1 Install and open the OpenSSL application.

Step 2 Enter the command:

```
OpenSSL> req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
```

Generating the CSR by the controller itself will use a 2048-bit key size and the mximum ECDSA key size is 256 bits.

Note You must provide the correct Common Name. Ensure that the host name that is used to create the certificate (Common Name) matches the Domain Name System (DNS) host name entry for the virtual interface IP on the controller. This name should exist in the DNS as well. Also, after you make the change to the VIP interface, you must reboot the system in order for this change to take effect.

After you issue the command, you are prompted to enter information such as country name, state, city, and so on.

Information similar to the following appears:

```
OpenSSL> req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................................................++++++
.....................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:CDE
Common Name (eg, YOUR name) []:XYZ.ABC
Email Address []:Test@abc.com


Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:
OpenSSL>
```

After you provide all the required details two files are generated:

- A new private key that includes the name *mykey.pem*
- A CSR that includes the name *myreq.pem*

Step 3 Copy and paste the Certificate Signing Request (CSR) information into any CA enrollment tool. After you submit the CSR to a third party CA, the third party CA digitally signs the certificate and sends back the signed certificate chain through e-mail. In case of chained certificates, you receive the entire chain of certificates from the CA. If you only have one intermediate certificate similar to the example above, you will receive the following three certificates from the CA:

- Root certificate.pem
- Intermediate certificate.pem
- Device certificate.pem

Note Ensure that the certificate is Apache-compatible with SHA1 encryption.

Step 4 Once you have all the three certificates, copy and paste into another file the contents of each .pem file in this order:

```
------BEGIN CERTIFICATE------
*Device cert*
------END CERTIFICATE------
------BEGIN CERTIFICATE------
*Intermediate CA cert *
------END CERTIFICATE--------
------BEGIN CERTIFICATE------
*Root CA cert *
------END CERTIFICATE------
```

Step 5 Save the file as *All-certs.pem*.

Step 6 Combine the All-certs.pem certificate with the private key that you generated along with the CSR (the private key of the device certificate, which is mykey.pem in this example), and save the file as final.pem.

Step 7 Create the All-certs.pem and final.pem files by entering these commands:

```
openssl> pkcs12 -export -in All-certs.pem -inkey mykey.pem
       -out All-certs.p12 -clcerts -passin pass:check123
       -passout pass:check123

openssl> pkcs12 -in All-certs.p12 -out final.pem
       -passin pass:check123 -passout pass:check123
```

final.pem is the file that we need to download to the controller.

Note You must enter a password for the parameters **-passin** and **-passout**. The password that is configured for the **-passout** parameter must match the certpassword parameter that is configured on the controller. In the above example, the password that is configured for both the **-passin** and **-passout** parameters is check123.

What to do next

Download the final.pem file to the controller either using CLI or GUI.

Downloading Third-Party Certificate (GUI)

Step 1 Copy the device certificate final.pem to the default directory on your TFTP server.

Step 2 Choose **Security > Web Auth > Certificate** to open the Web Authentication Certificate page.

Step 3 Check the **Download SSL Certificate** check box to view the Download SSL Certificate From Server parameters.

Step 4 In the **Server IP Address** text box, enter the IP address of the TFTP server.

Step 5 In the **File Path** text box, enter the directory path of the certificate.

Step 6 In the **File Name** text box, enter the name of the certificate.

Step 7 In the **Certificate Password** text box, enter the password to protect the certificate.

Step 8 Click **Apply**.

Step 9 After the download is complete, choose **Commands > Reboot** and click **Save and Reboot**.

Step 10 Click **OK** in order to confirm your decision to reboot the controller.

Downloading Third-Party Certificate (CLI)

Step 1 Move the *final.pem* file to the default directory on your TFTP server. Change the download settings by entering the following commands:

```
(Cisco Controller) > transfer download mode tftp
(Cisco Controller) > transfer download datatype webauthcert
(Cisco Controller) > transfer download serverip <TFTP server IP address>
(Cisco Controller) > transfer download path <absolute TFTP server path to the update file>
(Cisco Controller) > transfer download filename final.pem
```

Step 2 Enter the password for the .pem file so that the operating system can decrypt the SSL key and certificate.

```
(Cisco Controller) > transfer download certpassword password
```

Note Ensure that the value for *certpassword* is the same as the **-passout** parameter when you generate a CSR.

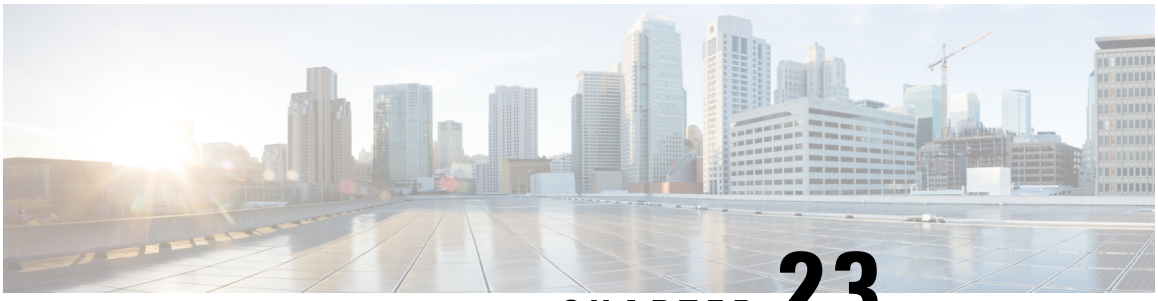
Step 3 Start the certificate and key download by entering the this command:

transfer download start

Example:

```
(Cisco Controller) > transfer download start

Mode............................................ TFTP
Data Type....................................... Site Cert
TFTP Server IP.................................. 10.77.244.196
TFTP Packet Timeout............................. 6
TFTP Max Retries................................ 10
TFTP Path......................................./
TFTP Filename................................... final.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use new certificate.
```

Step 4 Reboot the controller.



CHAPTER 23

Managing Web Authentication

- Obtaining a Web Authentication Certificate, on page 217
- Web Authentication Process, on page 220
- Choosing the Default Web Authentication Login Page, on page 223
- Using a Customized Web Authentication Login Page from an External Web Server, on page 229
- Downloading a Customized Web Authentication Login Page, on page 230
- Assigning Login, Login Failure, and Logout Pages per WLAN, on page 234
- Configuring Authentication for Sleeping Clients, on page 236

Obtaining a Web Authentication Certificate

Information About Web Authentication Certificates

The operating system of the controller automatically generates a fully functional web authentication certificate, so you do not need to do anything in order to use certificates with Layer 3 web authentication. However, if desired, you can prompt the operating system to generate a new web authentication certificate, or you can download an externally generated SSL certificate.

Starting with 7.0.250.0 and 7.3.101.0 releases (but not in 7.2.x release), SHA2 certificates are supported.

Note The WEB UI home page may not load when **ip http access class** command is enabled. When you encounter this issue, we recommend that you do the following:

1. Run the **show iosd liin** command.
2. Get the internet-address and configure the same ip as *permit* in the access-list.

Note For WEB UI access using TACACS+ server, custom method-list for authentication and authorization pointing to the TACACS+ server group does not work. You should use the default authorization method-list pointing to the same TACACS+ server group for the WEB UI to work.

Support for Chained Certificate

Cisco WLC allows the device certificate to be downloaded as a chained certificate (up to a level of 2) for web authentication. Wildcard certificates are also supported. For more information about chained certificates, see the *Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC* document at http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html.

Note While installing certificate for web authentication for Release 7.6, certificate load fails due to Missing Root CA cert error. Please download a chained certificate that includes intermediate Certificate Authority (CA) & root CA and install it on the Cisco WLC.

Obtaining a Web Authentication Certificate (GUI)

Step 1 Choose **Security** > **Web Auth** > **Certificate** to open the Web Authentication Certificate page.

This page shows the details of the current web authentication certificate.

Step 2 If you want to use a new operating system-generated web authentication certificate, follow these steps:

a) Click **Regenerate Certificate**. The operating system generates a new web authentication certificate, and a successfully generated web authentication certificate message appears.
b) Reboot the controller to register the new certificate.

Step 3 If you prefer to use an externally generated web authentication certificate, follow these steps:

a) Verify that the controller can ping the TFTP server.
b) Select the **Download SSL Certificate** check box.
c) In the Server IP Address text box, enter the IP address of the TFTP server.

The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

d) Enter the maximum number of times that each download can be attempted in the Maximum Retries text box and the amount of time (in seconds) allowed for each download in the Timeout text box.
e) In the Certificate File Path text box, enter the directory path of the certificate.
f) In the Certificate File Name text box, enter the name of the certificate (**certname**.pem).
g) In the Certificate Password text box, enter the password for the certificate.
h) Click **Apply** to commit your changes. The operating system downloads the new certificate from the TFTP server.
i) Reboot the controller to register the new certificate.

Obtaining a Web Authentication Certificate (CLI)

Step 1 See the current web authentication certificate by entering this command:

show certificate summary

Information similar to the following appears:

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:................ off
```

Step 2 If you want the operating system to generate a new web authentication certificate, follow these steps:

a) To generate the new certificate, enter this command:

config certificate generate webauth

b) To reboot the controller to register the new certificate, enter this command:

reset system

Step 3 If you prefer to use an externally generated web authentication certificate, follow these steps:

Note We recommend that the Common Name (CN) of the externally generated web authentication certificate be 1.1.1.1 (or the equivalent virtual interface IP address) in order for the client's browser to match the domains of the web authentication URL and the web authentication certificate.

a. Specify the name, path, and type of certificate to be downloaded by entering these commands:

transfer download mode tftp

transfer download datatype webauthcert

transfer download serverip *server_ip_address*

transfer download path *server_path_to_file*

transfer download filename *certname*.pem

transfer download certpassword *password*

transfer download tftpMaxRetries *retries*

transfer download tftpPktTimeout *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that each download can be attempted for the *retries* parameter and the amount of time (in seconds) allowed for each download for the *timeout* parameter.

b. Start the download process by entering this command:

transfer download start

c. Reboot the controller to register the new certificate by entering this command:

reset system

Web Authentication Process

Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic (except DHCP-related packets) from a particular client until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. When the clients attempt to join the wireless LAN, their users must enter the username and password when prompted by a login page.

Note If a client uses more than 20 DNS resolved addresses, the controller overwrites the 21st address in the first address space in the Mobile Station Control Block (MSCB) table, but the first address is still retained in the client. If the client again tries to use the first address, it will not be reachable because the controller does not have this address in the list of allowed addresses for the client's MSCB table.

Note One-Time Passwords (OTP) are not supported on web authentication.

When a client is associated with 802.1X + WebAuth Security and when the client roams, the 802.1X username is updated in the client information.

Note Web Authentication does not work with IPv6 URL when WLAN is LS however IPv4 with LS and IPv6 with CS works.. The re-directed web-auth page is not displayed when IPv6 URL is typed in the browser and WLAN is in Local Switching.

Disabling Security Alert for Web Authentication Process

When web authentication is enabled (under Layer 3 Security), users might receive a web-browser security alert the first time that they attempt to access a URL.

Figure 18: Typical Web-Browser Security Alert

Note When clients connect to a WebAuth SSID with preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.

After the user clicks **Yes** to proceed (or if the client's browser does not display a security alert), the web authentication system redirects the client to a login page.

Step 1 Click **View Certificate** on the Security Alert page.

Step 2 Click **Install Certificate**.

Step 3 When the Certificate Import Wizard appears, click **Next**.

Step 4 Choose **Place all certificates in the following store** and click **Browse**.

Step 5 Expand the **Trusted Root Certification Authorities** folder and choose **Local Computer**.

Step 6 Click **OK**.

Step 7 Click **Next** > **Finish**.

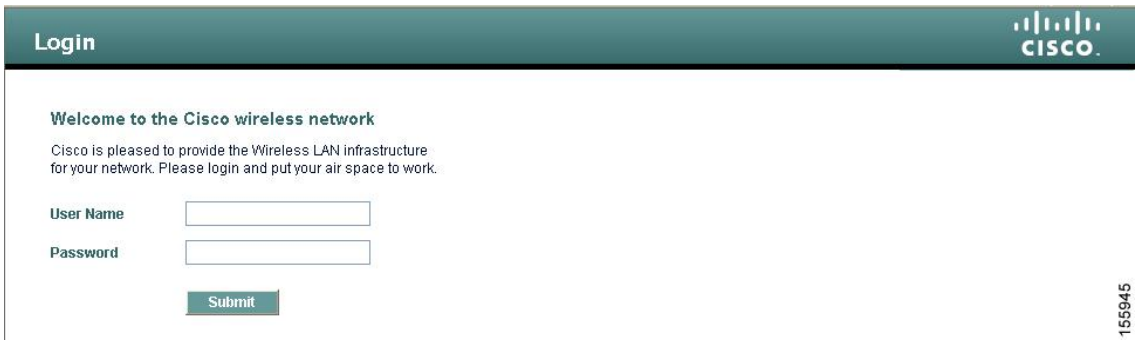
Step 8 When the "The import was successful" message appears, click **OK**.

Because the issuer text box is blank on the controller self-signed certificate, open Internet Explorer, choose **Tools** > **Internet Options** > **Advanced**, unselect the **Warn about Invalid Site Certificates** check box under Security, and click **OK**.

Step 9 Reboot the PC. On the next web authentication attempt, the login page appears.

Figure 19: Default Web Authentication Login Page

The following figure shows the default web authentication login page.



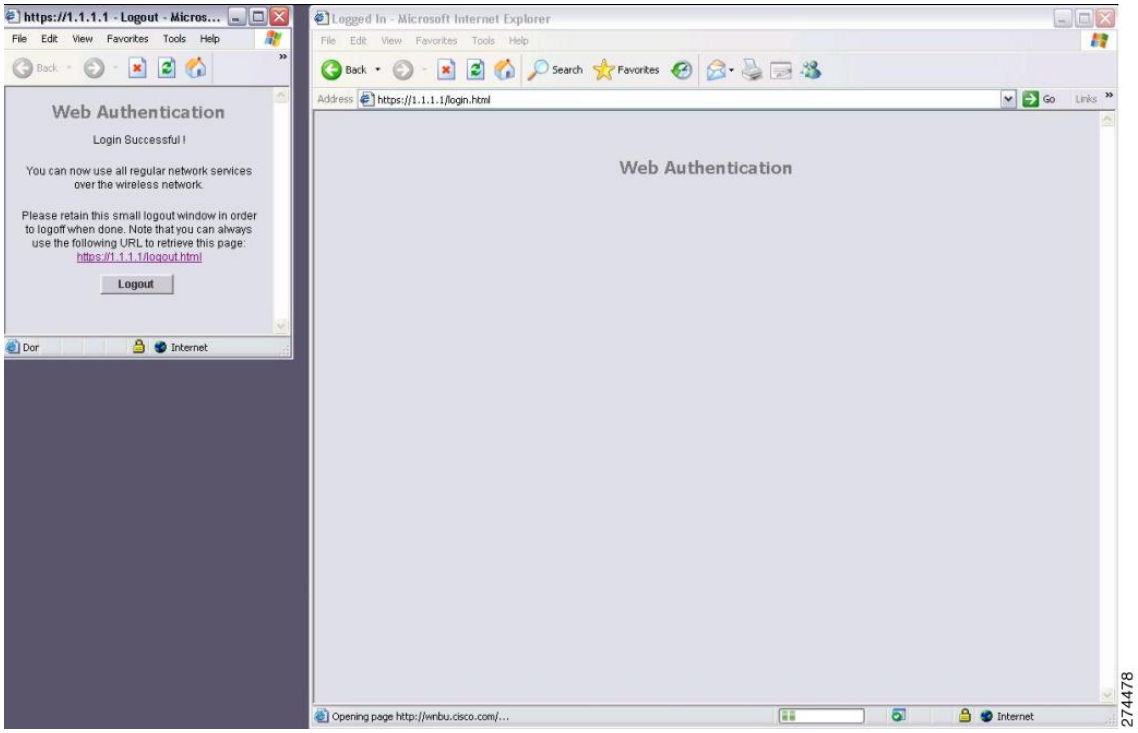
The default login page contains a Cisco logo and Cisco-specific text. You can choose to have the web authentication system display one of the following:

- The default login page
- A modified version of the default login page
- A customized login page that you configure on an external web server
- A customized login page that you download to the controller

The Choosing the Default Web Authentication Login Page section provides instructions for choosing how the web authentication login page appears.

When the user enters a valid username and password on the web authentication login page and clicks **Submit**, the web authentication system displays a successful login page and redirects the authenticated client to the requested URL.

Figure 20: Successful Login Page



The default successful login page contains a pointer to a virtual gateway address URL in the *https://<IP address>/logout.html* format. The IP address that you set for the controller virtual interface serves as the redirect address for the login page

Choosing the Default Web Authentication Login Page

Default Web Authentication Login Page

If you are using a custom web-auth bundle that is served by the internal controller web server, the page should not contain more than 5 elements (including HTML, CSS, and Images). This is because the internal controller web server implements a DoS protection mechanism that limits each client to open a maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection.

If you do not want users to connect to a web page using a browser that is configured with SSLv2 only, you can disable SSLv2 for web authentication by entering the **config network secureweb cipher-option sslv2 disable command**. If you enter this command, users must use a browser that is configured to use a more secure protocol such as SSLv3 or later releases. The default value is disabled.

Note Cisco TAC is not responsible for creating a custom webauth bundle.

If you have a complex custom web authentication module, it is recommended that you use an external web-auth config on the controller, where the full login page is hosted at an external web server.

This section contains the following subsections:

Choosing the Default Web Authentication Login Page (GUI)

Step 1 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 2 From the Web Authentication Type drop-down list, choose **Internal (Default)**.

Step 3 If you want to use the default web authentication login page as is, go to Step 8. If you want to modify the default login page, go to Step 4.

Step 4 If you want to hide the Cisco logo that appears in the top right corner of the default page, choose the Cisco Logo **Hide** option. Otherwise, click the **Show** option.

Step 5 If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter the desired URL in the Redirect URL After Login text box. You can enter up to 254 characters.

Step 6 If you want to create your own headline on the login page, enter the desired text in the Headline text box. You can enter up to 127 characters. The default headline is “Welcome to the Cisco wireless network.”

Step 7 If you want to create your own message on the login page, enter the desired text in the Message text box. You can enter up to 2047 characters. The default message is “Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.”

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Preview** to view the web authentication login page.

Step 10 If you are satisfied with the content and appearance of the login page, click **Save Configuration** to save your changes. Otherwise, repeat any of the previous steps as necessary to achieve your desired results.

Choosing the Default Web Authentication Login Page (CLI)

Step 1 Specify the default web authentication type by entering this command:

config custom-web webauth_type internal

Step 2 If you want to use the default web authentication login page as is, go to Step 7. If you want to modify the default login page, go to Step 3.

Step 3 To show or hide the Cisco logo that appears in the top right corner of the default login page, enter this command:

config custom-web weblogo {**enable** | **disable**}

Step 4 If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter this command:

config custom-web redirecturl *url*

You can enter up to 130 characters for the URL. To change the redirect back to the default setting, enter the **clear redirecturl** command.

Step 5 If you want to create your own headline on the login page, enter this command:

config custom-web webtitle *title*

You can enter up to 130 characters. The default headline is "Welcome to the Cisco wireless network." To reset the headline to the default setting, enter the **clear webtitle** command.

Step 6 If you want to create your own message on the login page, enter this command:

config custom-web webmessage *message*

You can enter up to 130 characters. The default message is "Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work." To reset the message to the default setting, enter the **clear webmessage** command.

Step 7 To enable or disable the web authentication logout popup window, enter this command:

config custom-web logout-popup {**enable** | **disable**}

Step 8 Enter the **save config** command to save your settings.

Step 9 Import your own logo into the web authentication login page as follows:

a. Make sure that you have a Trivial File Transfer Protocol (TFTP) server available for the file download. Follow these guidelines when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.

- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

b. Ensure that the controller can contact the TFTP server by entering this command:

ping ip-address

c. Copy the logo file (in .jpg, .gif, or .png format) to the default directory on your TFTP server. The maximum file size is 30 kilobits. For an optimal fit, the logo should be approximately 180 pixels wide and 360 pixels high.

d. Specify the download mode by entering this command:

transfer download mode tftp

e. Specify the type of file to be downloaded by entering this command:

transfer download datatype image

f. Specify the IP address of the TFTP server by entering this command:

transfer download serverip *tftp-server-ip-address*

Note Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

g. Specify the download path by entering this command:

transfer download path *absolute-tftp-server-path-to-file*

h. Specify the file to be downloaded by entering this command:

transfer download filename {*filename.jpg* | *filename.gif* | *filename.png*}

i. View your updated settings and answer *y* to the prompt to confirm the current download settings and start the download by entering this command:

transfer download start

j. Save your settings by entering this command:

save config

Note If you ever want to remove this logo from the web authentication login page, enter the **clear webimage** command.

Step 10 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 233 section to verify your settings.

Example: Creating a Customized Web Authentication Login Page

This section provides information on creating a customized web authentication login page, which can then be accessed from an external web server.

Here is a web authentication login page template. It can be used as a model when creating your own customized page:

Note We recommend that you follow the Cisco guidelines to create a customized web authentication login page. If you have upgraded to the latest versions of Google Chrome or Mozilla Firefox browsers, ensure that your webauth bundle has the following line in the *login.html* file:

```
<body onload="loadAction();">
```

For more information about this issue, see CSCvj17640.

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>

function submitAction(){
 var link = document.location.href;
 var searchString = "redirect=";
 var equalIndex = link.indexOf(searchString);
 var redirectUrl = "";

 if (document.forms[0].action == "") {
  var url = window.location.href;
  var args = new Object();
  var query = location.search.substring(1);
  var pairs = query.split("&");
  for(var i=0;i<pairs.length;i++){
  var pos = pairs[i].indexOf('=');
   if(pos == -1) continue;
    var argname = pairs[i].substring(0,pos);
    var value = pairs[i].substring(pos+1);
    args[argname] = unescape(value);
  }
   document.forms[0].action = args.switch_url;
  }

      if(equalIndex >= 0) {
  equalIndex += searchString.length;
  redirectUrl = "";
  redirectUrl += link.substring(equalIndex);
  }
  if(redirectUrl.length > 255)
  redirectUrl = redirectUrl.substring(0,255);
  document.forms[0].redirect_url.value = redirectUrl;
  document.forms[0].buttonClicked.value = 4;
        document.forms[0].submit();
}

 function loadAction(){
      var url = window.location.href;
      var args = new Object();
      var query = location.search.substring(1);
      var pairs = query.split("&");
      for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
```

```
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
      }
//alert( "AP MAC Address is " + args.ap_mac);
      //alert( "The Switch URL to post user credentials is " + args.switch_url);
      document.forms[0].action = args.switch_url;

      // This is the status code returned from webauth login action
      // Any value of status code from 1 to 5 is error condition and user
      // should be shown error as below or modify the message as it suits
      // the customer
      if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your part.");
      }
      else if(args.statusCode == 2){
       alert("You are not configured to authenticate against web portal. No further action
 is required on your part.");
      }
      else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the username is
 already logged into the system?");
      }
      else if(args.statusCode == 4){
        alert("The User has been excluded. Please contact the administrator.");
      }
      else if(args.statusCode == 5){
        alert("Invalid username and password. Please try again.");
      }
      else if(args.statusCode == 6){
        alert("Invalid email address format. Please try again.");
      }
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="https://209.165.200.225/login.html">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username" SIZE="25"
MAXLENGTH="63" VALUE="">
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password" name="password"
 SIZE="25" MAXLENGTH="24">
</td>
</tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
```

```
</td>
</tr>
</table>
</div>

</form>
</body>
</html>
```

These parameters are added to the URL when the user's Internet browser is redirected to the customized login page:

- **ap_mac**—The MAC address of the access point to which the wireless user is associated.
- **switch_url**—The URL of the controller to which the user credentials should be posted.
- **redirect**—The URL to which the user is redirected after authentication is successful.
- **statusCode**—The status code returned from the controller's web authentication server.
- **wlan**—The WLAN SSID to which the wireless user is associated.

The available status codes are as follows:

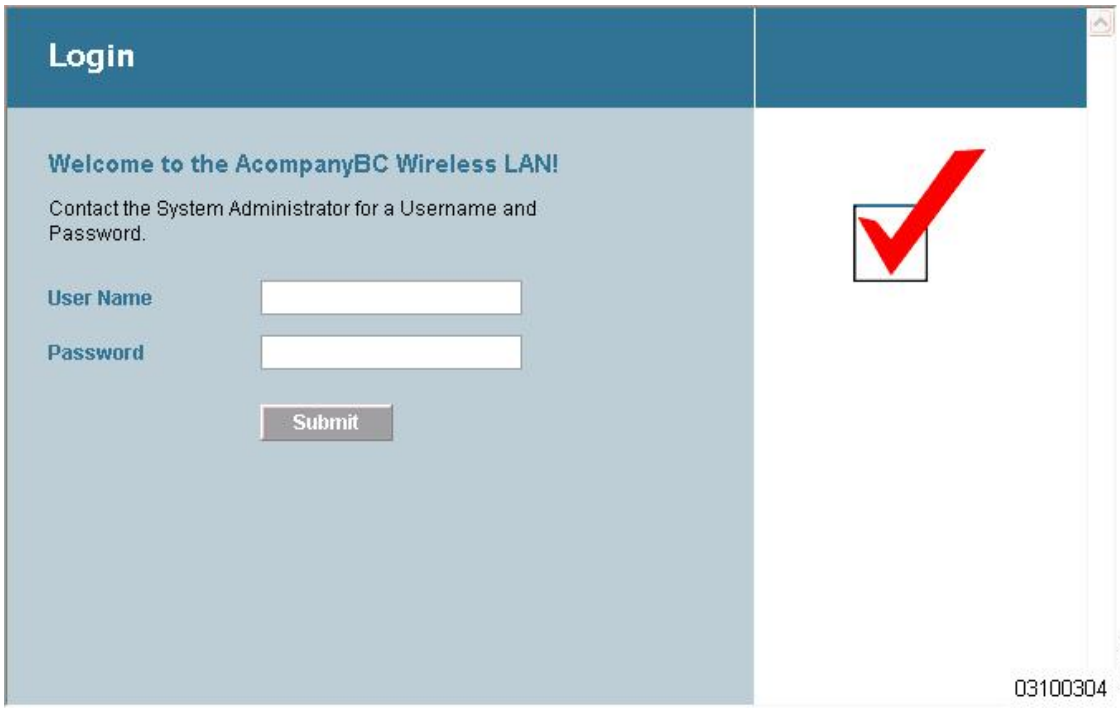
- Status Code 1: "You are already logged in. No further action is required on your part."
- Status Code 2: "You are not configured to authenticate against web portal. No further action is required on your part."
- Status Code 3: "The username specified cannot be used at this time. Perhaps the username is already logged into the system?"
- Status Code 4: "You have been excluded."
- Status Code 5: "The User Name and Password combination you have entered is invalid. Please try again."

Note For additional information, see the *External Web Authentication with Wireless LAN Controllers Configuration Example* at http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71881-ext-web-auth-wlc.html.

Example: Modified Default Web Authentication Login Page Example

Figure 21: Modified Default Web Authentication Login Page Example

This figure shows an example of a modified default web authentication login page.



These CLI commands were used to create this login page:

- **config custom-web weblogo** *disable*
- **config custom-web webtitle** *Welcome to the AcompanyBC Wireless LAN!*
- **config custom-web webmessage** *Contact the System Administrator for a Username and Password.*
- **transfer download** *start*
- **config custom-web redirecturl** *url*

Using a Customized Web Authentication Login Page from an External Web Server

Information About Customized Web Authentication Login Page

You can customize the web authentication login page to redirect to an external web server. When you enable this feature, the user is directed to your customized login page on the external web server.

You must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under **Layer 3 Security > Web Policy** on the **WLANs > Edit** page.

Choosing a Customized Web Authentication Login Page from an External Web Server (GUI)

Step 1 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 2 From the Web Authentication Type drop-down list, choose **External (Redirect to external server)**.

Step 3 In the Redirect URL after login text box, enter the URL that you want the user to be redirected after a login.

For example, you may enter your company's URL here and the users will be directed to that URL after login. The maximum length is 254 characters. By default, the user is redirected to the URL that was entered in the user's browser before the login page was served. of the customized web authentication login page on your web server. You can enter up to 252 characters.

Step 4 In the External Webauth URL text box, enter the URL that is to be used for external web authentication.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Choosing a Customized Web Authentication Login Page from an External Web Server (CLI)

Step 1 Specify the web authentication type by entering this command:

config custom-web webauth_type external

Step 2 Specify the URL of the customized web authentication login page on your web server by entering this command:

config custom-web ext-webauth-url *url*

You can enter up to 252 characters for the URL.

Step 3 Specify the IP address of your web server by entering this command:

config custom-web ext-webserver {**add** | **delete**} *server_IP_address*

Step 4 Enter the **save config** command to save your settings.

Step 5 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 233 section to verify your settings.

Downloading a Customized Web Authentication Login Page

You can compress the page and image files used for displaying a web authentication login page into a.tar file for download to a controller. These files are known as the webauth bundle. The maximum allowed size of the files in their uncompressed state is 1 MB. When the .tar file is downloaded from a local TFTP server, it enters the controller’s file system as an untarred file.

You can download a login page example from Cisco Prime Infrastructure and use it as a starting point for your customized login page. For more information, see the Cisco Prime Infrastructure documentation.

Note If you load a webauth bundle with a .tar compression application that is not GNU compliant, the controller cannot extract the files in the bundle and the following error messages appear: "Extracting error" and "TFTP transfer failed." Therefore, we recommend that you use an application that complies with GNU standards, such as PicoZip, to compress the .tar file for the webauth bundle.

Note Configuration backups do not include extra files or components, such as the webauth bundle or external licenses, that you download and store on your controller, so you should manually save external backup copies of those files or components.

Note If the customized webauth bundle has more than 3 separated elements, we advise you to use an external server to prevent page load issues that may be caused because of TCP rate-limiting policy on the controller.

Prerequisites for Downloading a Customized Web Authentication Login Page

- Name the login page `login.html`. The controller prepares the web authentication URL based on this name. If the server does not find this file after the webauth bundle has been untarred, the bundle is discarded, and an error message appears.
- Include input text boxes for both a username and password.
- Retain the redirect URL as a hidden input item after extracting from the original URL.
- Extract and set the action URL in the page from the original URL.
- Include scripts to decode the return status code.
- Make sure that all paths used in the main page (to refer to images, for example).
- Ensure that no filenames within the bundle are greater than 30 characters.

Downloading a Customized Web Authentication Login Page (GUI)

Step 1 Copy the .tar file containing your login page to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the **File Type** drop-down list, choose **Webauth Bundle**.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in the 7.4 and later releases)

Step 5 In the **IP Address** text box, enter the IP address of the server.

Step 6 If you are using a TFTP server, enter the maximum number of times the controller should attempt to download the .tar file in the Maximum Retries text box.

The range is 1 to 254.

The default is 10.

Step 7 If you are using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the *.tar file in the Timeout text box.

The range is 1 to 254 seconds.

The default is 6 seconds.

Step 8 In the **File Path** text box, enter the path of the .tar file to be downloaded. The default value is "/."

Step 9 In the **File Name** text box, enter the name of the .tar file to be downloaded.

Step 10 If you are using an FTP server, follow these steps:

a. In the **Server Login Username** text box, enter the username to log into the FTP server.

b. In the **Server Login Password** text box, enter the password to log into the FTP server.

c. In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 11 Click **Download** to download the .tar file to the controller.

Step 12 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 13 From the Web Authentication Type drop-down list, choose **Customized (Downloaded)**.

Step 14 Click **Apply**.

Step 15 Click **Preview** to view your customized web authentication login page.

Step 16 If you are satisfied with the content and appearance of the login page, click **Save Configuration**.

Downloading a Customized Web Authentication Login Page (CLI)

Step 1 Copy the .tar file containing your login page to the default directory on your server.

Step 2 Specify the download mode by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the type of file to be downloaded by entering this command:

transfer download datatype webauthbundle

Step 4 Specify the IP address of the TFTP server by entering this command:

transfer download serverip *tftp-server-ip-address*.

Note Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

Step 5 Specify the download path by entering this command:

transfer download path *absolute-tftp-server-path-to-file*

Step 6 Specify the file to be downloaded by entering this command:

transfer download filename *filename.tar*

Step 7 View your updated settings and answer **y** to the prompt to confirm the current download settings and start the download by entering this command:

transfer download start

Step 8 Specify the web authentication type by entering this command:

config custom-web webauth_type *customized*

Step 9 Enter the **save config** command to save your settings.

Example: Customized Web Authentication Login Page

Figure 22: Customized Web Authentication Login Page Example

This figure shows an example of a customized web authentication login page.

Verifying the Web Authentication Login Page Settings (CLI)

Verify your changes to the web authentication login page by entering this command:

show custom-web

Assigning Login, Login Failure, and Logout Pages per WLAN

Assigning Login, Login Failure, and Logout Pages per WLAN

You can display different web authentication login, login failure, and logout pages to users per WLAN. This feature enables user-specific web authentication pages to be displayed for a variety of network users, such as guest users or employees within different departments of an organization.

Different login pages are available for all web authentication types (internal, external, and customized). However, different login failure and logout pages can be specified only when you choose customized as the web authentication type.

This section contains the following subsections:

Assigning Login, Login Failure, and Logout Pages per WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to which you want to assign a web login, login failure, or logout page.

Step 3 Choose **Security** > **Layer 3**.

Step 4 Make sure that **Web Policy** and **Authentication** are selected.

Step 5 To override the global authentication configuration web authentication pages, select the **Override Global Config** check box.

Step 6 When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wireless guest users:

- **Internal**—Displays the default web login page for the controller. This is the default value.
- **Customized**—Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

  Note These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.

- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 7 If you chose External as the web authentication type in Step 6, choose **AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 8 Establish the priority in which the servers are contacted to perform web authentication as follows:

Note The default order is local, RADIUS, LDAP.

a. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.

b. Click **Up** and **Down** until the desired server type is at the top of the box.

c. Click the **<** arrow to move the server type to the priority box on the left.

d. Repeat these steps to assign priority to the other servers.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Assigning Login, Login Failure, and Logout Pages per WLAN (CLI)

Step 1 Determine the ID number of the WLAN to which you want to assign a web login, login failure, or logout page by entering this command:

show wlan summary

Step 2 If you want wireless guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the WLAN for which it should display:

- **config wlan custom-web login-page** *page_name wlan_id—Defines a customized login page for a* given WLAN.
- **config wlan custom-web loginfailure-page** *page_name wlan_id—Defines a customized login* failure page for a given WLAN.

  Note To use the controller's default login failure page, enter the **config wlan custom-web loginfailure-page none** *wlan_id* command.

- **config wlan custom-web logout-page** *page_name wlan_id—Defines a customized logout page for* a given WLAN.

  Note To use the controller's default logout page, enter the **config wlan custom-web logout-page none** *wlan_id* command.

Step 3 Redirect wireless guess users to an external server before accessing the web login page by entering this command to specify the URL of the external server:

config wlan custom-web ext-webauth-url *ext_web_url wlan_id*

Step 4 Define the order in which web authentication servers are contacted by entering this command:

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS and LDAP.

Note All external servers must be preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page and the LDAP Servers page.

Step 5 Define which web authentication page displays for a wireless guest user by entering this command:

config wlan custom-web webauth-type {**internal** | **customized** | **external**} *wlan_id*

where

- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web login page that was configured in *Step 2*.

  Note You do not need to define the web authentication type in *Step 5* for the login failure and logout pages as they are always customized.

- **external** redirects users to the URL that was configured in *Step 3*.

Step 6 Use a WLAN-specific custom web configuration rather than a global custom web configuration by entering this command:

config wlan custom-web global disable *wlan_id*

Note If you enter the **config wlan custom-web global enable** *wlan_id* command, the custom web authentication configuration at the global level is used.

Step 7 Save your changes by entering this command:

save config

Configuring Authentication for Sleeping Clients

Authentication of Sleeping Clients

Clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can configure the duration on a WLAN and on a user group policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is lesser than the time configured on the sleeping timer of the WLAN, then the lifetime of the client is used as the sleeping time.

Note The sleeping timer expires every 5 minutes.

This feature is supported in the following FlexConnect scenario: local switching and central authentication.

Caution If the MAC address of a client that goes to sleep mode is spoofed, the fake device such as a laptop can be authenticated.

Following are some guidelines in a mobility scenario:

- L2 roaming in the same subnet is supported.
- Anchor sleeping timer is applicable.
- The sleeping client information is shared between multiple autoanchors when a sleeping client moves from one anchor to another.

Supported Mobility Scenarios

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two controllers in a mobility group. A client that is associated with one controller goes to sleep and then wakes up and gets associated with the other controller.
- Suppose there are three controllers in a mobility group. A client that is associated with the second controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third controller.
- A client sleeps, wakes up and gets associated with the same or different export foreign controller that is anchored to the export anchor.

This section contains the following subsections:

Restrictions for Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security. Web passthrough is supported on Release 8.0 and later.
- You can configure the sleeping clients only on a per-WLAN basis.
- The authentication of sleeping clients feature is not supported with Layer 2 security and web authentication enabled.
- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.
- In a High Availability scenario, the client entry is synchronized between active and standby, but the sleeping timer is not synchronized. If the active controller fails, the client has to get reauthenticated when it associates with the standby controller.
- The number of sleeping clients that are supported depends on the controller platform:
  - Cisco 2504 Wireless Controller—500
  - Cisco 5508 Wireless Controller—1000
  - Cisco 5520 Wireless Controller—25000

- Cisco Flex 7510 Wireless Controller—25000 with Release 7.6 and later; 9000 in earlier releases
- Cisco 8510 Wireless Controller—25000 with Release 7.6 and later; 9000 in earlier releases
- Cisco 8540 Wireless Controller—64000
- Cisco WiSM2—1000
- Cisco Virtual Wireless LAN Controller—500
- Cisco Wireless Controller on Cisco Services-Ready Engine (SRE)—500

- New mobility is not supported.

Configuring Authentication for Sleeping Clients (GUI)

Step 1 Choose **WLANs**.

Step 2 Click the corresponding WLAN ID.

The **WLANs > Edit** page is displayed.

Step 3 Click the **Security** tab and then click the **Layer 3** tab.

Step 4 Select the **Sleeping Client** check box to enable authentication for sleeping clients.

Step 5 Enter the **Sleeping Client Timeout**, which is the duration for which the sleeping clients are to be remembered before reauthentication becomes necessary.

The default timeout is 12 hours.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

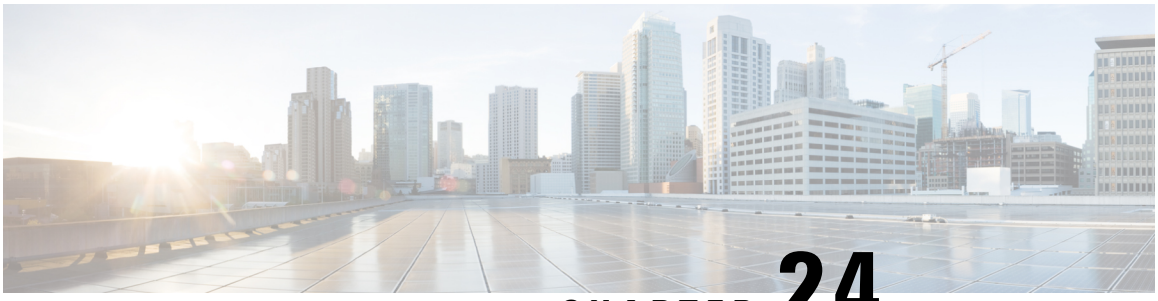
Configuring Authentication for Sleeping Clients (CLI)

Procedure

- Enable or disable authentication for sleeping clients on a WLAN by entering this command:
  config wlan custom-web sleep-client {**enable** | **disable**} *wlan-id*
- Configure the sleeping client timeout on a WLAN by entering this command:
  config wlan custom-web sleep-client timeout *wlan-id duration*
- View the sleeping client configuration on a WLAN by entering this command:
  show wlan *wlan-id*
- Delete any unwanted sleeping client entries by entering this command:
  config custom-web sleep-client delete *client-mac-addr*
- View a summary of all the sleeping client entries by entering this command:
  show custom-web sleep-client summary

- View the details of a sleeping client entry based on the MAC address of the client by entering this command:

  show custom-web sleep-client detail *client-mac-addr*



CHAPTER 24

Configuring Wired Guest Access

- Wired Guest Access, on page 241
- Prerequisites for Configuring Wired Guest Access, on page 242
- Restrictions for Configuring Wired Guest Access, on page 242
- Configuring Wired Guest Access (GUI), on page 242
- Configuring Wired Guest Access (CLI), on page 244
- Supporting IPv6 Client Guest Access, on page 247

Wired Guest Access

Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

Wired guest access can be configured in a standalone configuration or in a dual-controller configuration that uses both an anchor controller and a foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired guest access ports initially terminate on a Layer 2 access switch or switch port configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

Note Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

Note You can specify the amount of bandwidth allocated to a wired guest user in the network by configuring a QoS role and a bandwidth contract.

You can create a basic peer to peer WLAN ACL and apply it to the wired guest WLAN. This will not block peer to peer traffic and the guest users can still communicate with each other.

This section contains the following subsections:

Prerequisites for Configuring Wired Guest Access

To configure wired guest access on a wireless network, you must perform the following:

1. Configure a dynamic interface (VLAN) for wired guest user access
2. Create a wired LAN for guest user access
3. Configure the controller
4. Configure the anchor controller (if terminating traffic on another controller)
5. Configure security for the guest LAN
6. Verify the configuration

Restrictions for Configuring Wired Guest Access

- Wired guest access interfaces must be tagged.
- Wired guest access ports must be in the same Layer 2 network as the foreign controller.
- Up to five wired guest access LANs can be configured on a controller. Also in a wired guest access LAN, multiple anchors are supported.
- Layer 3 web authentication and web passthrough are supported for wired guest access clients. Layer 2 security is not supported.
- Do not trunk a wired guest VLAN to multiple foreign controllers, as it might produce unpredictable results.
- The controller does not use the callStationIDType parameter configured for the Radius server while authenticating wired clients, instead the controller uses the system MAC address configured for the callStationIDType parameter.

Configuring Wired Guest Access (GUI)

Step 1 To create a dynamic interface for wired guest user access, choose **Controller** > **Interfaces**. The Interfaces page appears.

Step 2 Click **New** to open the **Interfaces > New** page.

Step 3 Enter a name and VLAN ID for the new interface.

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

Step 5 In the **Port Number** text box, enter a valid port number. You can enter a number between 0 and 25 (inclusive).

Step 6 Select the **Guest LAN** check box.

Step 7 Click **Apply** to commit your changes.

Step 8 To create a wired LAN for guest user access, choose **WLANs**.

Step 9 On the WLANs page, choose **Create New** from the drop-down list and click **Go**. The **WLANs** > **New page** appears.

Step 10 From the Type drop-down list, choose **Guest LAN**.

Step 11 In the **Profile Name** text box, enter a name that identifies the guest LAN. Do not use any spaces.

Step 12 From the WLAN ID drop-down list, choose the ID number for this guest LAN.

Note You can create up to five guest LANs, so the WLAN ID options are 1 through 5 (inclusive).

Step 13 Click **Apply** to commit your changes.

Step 14 Select the **Enabled** check box for the Status parameter.

Step 15 Web authentication (Web-Auth) is the default security policy. If you want to change this to web passthrough, choose the **Security** tab after completing *Step 16* and *Step 17*.

Step 16 From the Ingress Interface drop-down list, choose the VLAN that you created in *Step 3*. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 17 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

Step 18 If you want to change the authentication method (for example, from web authentication to web passthrough), choose **Security** > **Layer 3**. The **WLANs > Edit (Security > Layer 3)** page appears.

Step 19 From the Layer 3 Security drop-down list, choose one of the following:

- **None**—Layer 3 security is disabled.
- **Web Authentication**—Causes users to be prompted for a username and password when connecting to the wireless network. This is the default value.
- **Web Passthrough**—Allows users to access the network without entering a username and password.

  Note There should not be a Layer 3 gateway on the guest wired VLAN, as this would bypass the web authentication done through the controller.

Step 20 If you choose the Web Passthrough option, an **Email Input** check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

Step 21 To override the global authentication configuration set on the Web Login page, select the **Override Global Config** check box.

Step 22 When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wired guest users:

- **Internal**—Displays the default web login page for the controller. This is the default value.
- **Customized**—Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

  Note These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.

- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 23 If you chose External as the web authentication type in *Step 22*, choose **Security > AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note You can configure the Authentication and LDAP Server using both IPv4 and IPv6 addresses.

Note The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 24 To establish the priority in which the servers are contacted to perform web authentication as follows:

Note The default order is local, RADIUS, LDAP.

a. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.

b. Click **Up** and **Down** until the desired server type is at the top of the box.

c. Click the **<** arrow to move the server type to the priority box on the left.

d. Repeat these steps to assign priority to the other servers.

Step 25 Click **Apply**.

Step 26 Click **Save Configuration**.

Step 27 Repeat this process if a second (anchor) controller is being used in the network.

Configuring Wired Guest Access (CLI)

Step 1 Create a dynamic interface (VLAN) for wired guest user access by entering this command:

config interface create *interface_name vlan_id*

Step 2 If link aggregation trunk is not configured, enter this command to map a physical port to the interface:

config interface port *interface_name primary_port* {*secondary_port*}

Step 3 Enable or disable the guest LAN VLAN by entering this command:

config interface guest-lan *interface_name* {**enable | disable}**

This VLAN is later associated with the ingress interface created in *Step 5*.

Step 4 Create a wired LAN for wired client traffic and associate it to an interface by entering this command:

config guest-lan create *guest_lan_id interface_name*

The guest LAN ID must be a value between 1 and 5 (inclusive).

Note To delete a wired guest LAN, enter the **config guest-lan delete** *guest_lan_id command.*

Step 5 Configure the wired guest VLAN's ingress interface, which provides a path between the wired guest client and the controller by way of the Layer 2 access switch by entering this command:

config guest-lan ingress-interface *guest_lan_id interface_name*

Step 6 Configure an egress interface to transmit wired guest traffic out of the controller by entering this command:

config guest-lan interface *guest_lan_id interface_name*

Note If the wired guest traffic is terminating on another controller, repeat *Step 4* and *Step 6* for the terminating (anchor) controller and *Step 1* through *Step 5* for the originating (foreign) controller. Additionally, configure the **config mobility group anchor add** {**guest-lan** *guest_lan_id* | **wlan** *wlan_id} IP_address* command for both controllers.

Step 7 Configure the security policy for the wired guest LAN by entering this command:

config guest-lan security {**web-auth enable guest_lan_id** | **web-passthrough enable** *guest_lan_id*}

Note Web authentication is the default setting.

Step 8 Enable or disable a wired guest LAN by entering this command:

config guest-lan {enable | disable} *guest_lan_id*

Step 9 If you want wired guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the guest LAN for which it should display:

- **config guest-lan custom-web login-page** *page_name guest_lan_id—Defines a web login page.*
- **config guest-lan custom-web loginfailure-page** *page_name guest_lan_id—Defines a web login failure* page.

  Note To use the controller's default login failure page, enter the **config guest-lan custom-web loginfailure-page none** *guest_lan_id* command.

- **config guest-lan custom-web logout-page** *page_name guest_lan_id*—Defines a web logout page.

  Note To use the controller's default logout page, enter the **config guest-lan custom-web logout-page none** *guest_lan_id* command.

Step 10 If you want wired guest users to be redirected to an external server before accessing the web login page, enter this command to specify the URL of the external server:

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

Step 11 If you want to define the order in which local (controller) or external (RADIUS, LDAP) web authentication servers are contacted, enter this command:

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS, LDAP.

Note All external servers must be preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page or the LDAP Servers page.

Step 12 Define the web login page for wired guest users by entering this command:

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

where

- **internal** displays the default web login page for the controller. This is the default value.

- **customized** displays the custom web pages (login, login failure, or logout) that were configured in *Step 9*.
- **external** redirects users to the URL that was configured in *Step 10*.

Step 13 Use a guest-LAN specific custom web configuration rather than a global custom web configuration by entering this command:

config guest-lan custom-web global disable *guest_lan_id*

Note If you enter the **config guest-lan custom-web global enable** *guest_lan_id* command, the custom web authentication configuration at the global level is used.

Step 14 Save your changes by entering this command:

save config

Note Information on the configured web authentication appears in both the **show run-config** and **show running-config** commands.

Step 15 Display the customized web authentication settings for a specific guest LAN by entering this command:

show custom-web {all | guest-lan guest_lan_id}

Note If internal web authentication is configured, the Web Authentication Type displays as internal rather than external (controller level) or customized (WLAN profile level).

Step 16 Display a summary of the local interfaces by entering this command:

show interface summary

Note The interface name of the wired guest LAN in this example is *wired-guest* and its VLAN ID is 236.

Display detailed interface information by entering this command:

show interface detailed *interface_name*

Step 17 Display the configuration of a specific wired guest LAN by entering this command:

show guest-lan *guest_lan_id*

Note Enter the **show guest-lan summary** command to see all wired guest LANs configured on the controller.

Step 18 Display the active wired guest LAN clients by entering this command:

show client summary guest-lan

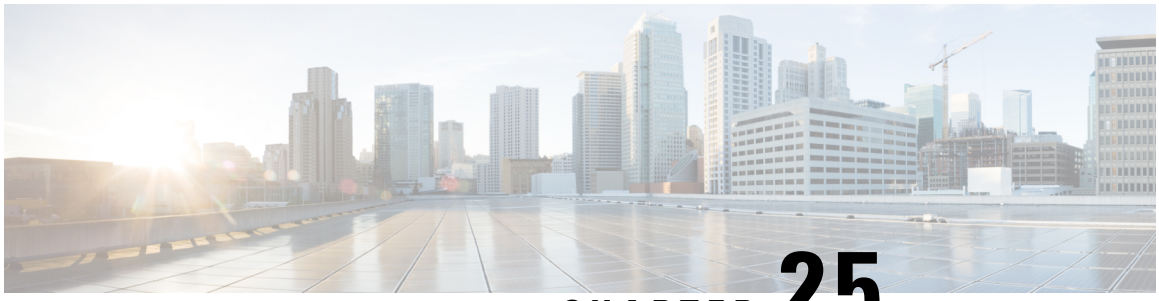
Step 19 Display detailed information for a specific client by entering this command:

show client detail *client_mac*

Supporting IPv6 Client Guest Access

The client is in WebAuth Required state until the client is authenticated. The controller intercepts both IPv4 and IPv6 traffic in this state and redirects it to the virtual IP address of the controller. Once authenticated, the user's MAC address is moved to the run state and both IPv4 and IPv6 traffic is allowed to pass.

In order to support the redirection of IPv6-only clients, the controller automatically creates an IPv6 virtual address based on the IPv4 virtual address configured on the controller. The virtual IPv6 address follows the convention of [::ffff:<virtual IPv4 address>]. For example, a virtual IP address of 192.0.2.1 would translate into [::ffff:192.0.2.1]. For an IPv6 captive portal to be displayed, the user must request an IPv6 resolvable DNS entry such as ipv6.google.com which returns a DNSv6 (AAAA) record.



CHAPTER 25

Troubleshooting

- Interpreting LEDs, on page 249
- System Messages, on page 250
- Viewing System Resources, on page 253
- Using the CLI to Troubleshoot Problems, on page 254
- Configuring System and Message Logging, on page 255
- Viewing Access Point Event Logs, on page 262
- Uploading Logs and Crash Files, on page 263
- Uploading Core Dumps from the Controller, on page 265
- Uploading Packet Capture Files, on page 268
- Monitoring Memory Leaks, on page 271
- Troubleshooting CCXv5 Client Devices, on page 272
- Using the Debug Facility, on page 282
- Configuring Wireless Sniffing, on page 287
- Troubleshooting Access Points Using Telnet or SSH, on page 289
- Debugging the Access Point Monitor Service, on page 291
- Troubleshooting Memory Leaks, on page 291
- Troubleshooting OfficeExtend Access Points, on page 292

Interpreting LEDs

Information About Interpreting LEDs

This section describes how to interpret controller LEDs and lightweight access point LEDs.

Interpreting Controller LEDs

See the quick start guide for your specific controller for a description of the LED patterns. See the list of controllers and the respective documentation at http://www.cisco.com/c/en/us/products/wireless/index.html.

Interpreting Lightweight Access Point LEDs

See the quick start guide or hardware installation guide for your specific access point for a description of the LED patterns. See the list of access points and the respective documentation at http://www.cisco.com/c/en/us/products/wireless/index.html.

System Messages

Information About System Messages

This table lists some common system messages and their descriptions. For a complete list of system messages, see the *Cisco Wireless LAN Controller System Message Guide, Release 7.0*.

Table 8: System Messages and Descriptions

Error Message	Description
apf_utils.c 680: Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx:xx	A client is sending an association request on a security-enabled WLAN with the protected bit set to 0 (in the Capability field of the association request). As designed, the controller rejects the association request, and the client sees an association failure.
dtl_arp.c 480: Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx:xx	The controller's network processing unit (NPU) sends a timeout message to the central processing unit (CPU) indicating that a particular client has timed out or aged out. This situation typically occurs when the CPU has removed a wireless client from its internal database but has not notified the NPU. Because the client remains in the NPU database, it ages out on the network processor and notifies the CPU. The CPU finds the client that is not present in its database and then sends this message.
STATION_DISASSOCIATE	The client may have intentionally terminated usage or may have experienced a service disruption.
STATION_DEAUTHENTICATE	The client may have intentionally terminated usage or this message could indicate an authentication issue.
STATION_AUTHENTICATION_FAIL	Check disable, key mismatch, or other configuration issues.
STATION_ASSOCIATE_FAIL	Check load on the Cisco radio or signal quality issues.
LRAD_ASSOCIATED	The associated lightweight access point is now managed by this controller.
LRAD_DISASSOCIATED	The lightweight access point may have associated to a different controller or may have become completely unreachable.
LRAD_UP	The lightweight access point is operational; no action required.
LRAD_DOWN	The lightweight access point may have a problem or is administratively disabled.

Error Message	Description
LRADIF_UP	The Cisco radio is UP.
LRADIF_DOWN	The Cisco radio may have a problem or is administratively disabled.
LRADIF_LOAD_PROFILE_FAILED	The client density may have exceeded system capacity.
LRADIF_NOISE_PROFILE_FAILED	The non-802.11 noise has exceeded the configured threshold.
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 interference has exceeded threshold on channel; check channel assignments.
LRADIF_COVERAGE_PROFILE_FAILED	A possible coverage hole has been detected. Check the lightweight access point history to see if it is a common problem and add lightweight access points if necessary.
LRADIF_LOAD_PROFILE_PASSED	The load is now within threshold limits.
LRADIF_NOISE_PROFILE_PASSED	The detected noise is now less than threshold.
LRADIF_INTERFERENCE_PROFILE_PASSED	The detected interference is now less than threshold.
LRADIF_COVERAGE_PROFILE_PASSED	The number of clients receiving a poor signal are within threshold.
LRADIF_CURRENT_TXPOWER_CHANGED	Informational message.
LRADIF_CURRENT_CHANNEL_CHANGED	Informational message.
LRADIF_RTS_THRESHOLD_CHANGED	Informational message.
LRADIF_ED_THRESHOLD_CHANGED	Informational message.
LRADIF_FRAGMENTATION_THRESHOLD_CHANGED	Informational message.
RRM_DOT11_A_GROUPING_DONE	Informational message.
RRM_DOT11_B_GROUPING_DONE	Informational message.
ROGUE_AP_DETECTED	May be a security issue. Use maps and trends to investigate.
ROGUE_AP_REMOVED	A detected rogue access point has timed out. The unit might have shut down or moved out of the coverage area.
AP_MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
LINK_UP	Positive confirmation message.
LINK_DOWN	A port may have a problem or is administratively disabled.
LINK_FAILURE	A port may have a problem or is administratively disabled.

Error Message	Description
AUTHENTICATION_FAILURE	An attempted security breech has occurred. Investigate.
STP_NEWROOT	Informational message.
STP_TOPOLOGY_CHANGE	Informational message.
IPSEC_ESP_AUTH_FAILURE	Check WLAN IPsec configuration.
IPSEC_ESP_REPLAY_FAILURE	Check for an attempt to spoof an IP address.
IPSEC_ESP_POLICY_FAILURE	Check for a IPsec configuration mismatch between WLAN and client.
IPSEC_ESP_INVALID_SPI	Informational message.
IPSEC_OTHER_POLICY_FAILURE	Check for a IPsec configuration mismatch between WLAN and client.
IPSEC_IKE_NEG_FAILURE	Check for a IPsec IKE configuration mismatch between WLAN and client.
IPSEC_SUITE_NEG_FAILURE	Check for a IPsec IKE configuration mismatch between WLAN and client.
IPSEC_INVALID_COOKIE	Informational message.
RADIOS_EXCEEDED	The maximum number of supported Cisco radios has been exceeded. Check for a controller failure in the same Layer 2 network or add another controller.
SENSED_TEMPERATURE_HIGH	Check fan, air conditioning, and/or other cooling arrangements.
SENSED_TEMPERATURE_LOW	Check room temperature and/or other reasons for low temperature.
TEMPERATURE_SENSOR_FAILURE	Replace temperature sensor as soon as possible.
TEMPERATURE_SENSOR_CLEAR	The temperature sensor is operational.
POE_CONTROLLER_FAILURE	Check ports; a possible serious failure has been detected.
MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
SWITCH_UP	The controller is responding to SNMP polls.
SWITCH_DOWN	The controller is not responding to SNMP polls; check controller and SNMP settings.
RADIUS_SERVERS_FAILED	Check network connectivity between RADIUS and the controller.
CONFIG_SAVED	The running configuration has been saved to flash; it will be active after a reboot.

Error Message	Description
MULTIPLE_USERS	Another user with the same username has logged in.
FAN_FAILURE	Monitor controller temperature to avoid overheating.
POWER_SUPPLY_CHANGE	Check for a power-supply malfunction.
COLD_START	The controller may have been rebooted.
WARM_START	The controller may have been rebooted.

Viewing System Resources

Viewing System Resources

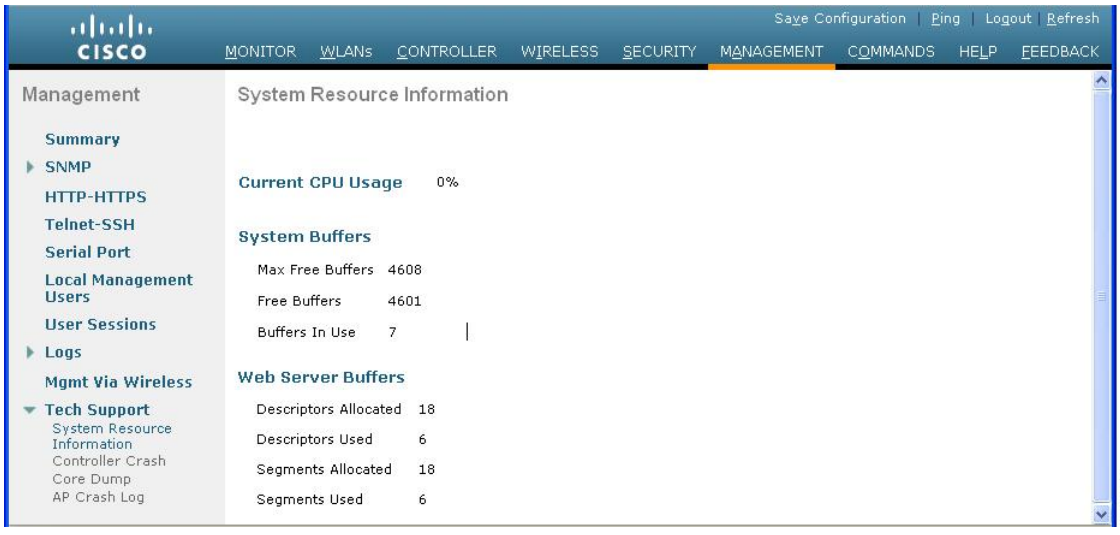
You can determine the amount of system resources being used by the controller. Specifically, you can view the current controller CPU usage, system buffers, and web server buffers.

The controllers have multiple CPUs, so you can view individual CPU usage. For each CPU, you can see the percentage of the CPU in use and the percentage of the CPU time spent at the interrupt level (for example, 0%/3%).

Viewing System Resources (GUI)

On the controller GUI, choose **Management > Tech Support > System Resource Information**. The System Resource Information page appears.

Figure 23: System Resource Information Page



Viewing System Resources (CLI)

On the controller CLI, enter these commands:

- **show cpu**

  Where the first number is the CPU percentage that the controller spent on the user application and the second number is the CPU percentage that the controller spent on the OS services.

- **show tech-support**
- **show system top**

  Provides an ongoing look at processor activity in real time. It displays a list of the most CPU-intensive tasks performed on the system.

- **show system iostat summary**

  Provides CPU statistics, input and output statistics for devices and partitions.

- **show system iostat detail**

  Provides CPU statistics, input and output statistics for devices and partitions with extended statistics.

Using the CLI to Troubleshoot Problems

If you experience any problems with your controller, you can use the commands in this section to gather information and debug issues.

Procedure

- **show process cpu**—Shows how various tasks in the system are using the CPU at that instant in time. This command is helpful in understanding if any single task is monopolizing the CPU and preventing other tasks from being performed.

  The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task that is divided by a range of system priorities.

  The CPU Use field shows the CPU usage of a particular task.

  The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in a system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

Note If you want to see the total CPU usage as a percentage, enter the **show cpu** command.

- **show process memory**—Shows the allocation and deallocation of memory from various processes in the system at that instant in time.

  In the example above, the following fields provide information:

  The Name field shows the tasks that the CPU is to perform.

The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task that is divided by a range of system priorities.

The BytesInUse field shows the actual number of bytes used by dynamic memory allocation for a particular task.

The BlocksInUse field shows the chunks of memory that are assigned to perform a particular task.

The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a "T"). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

- **show tech-support**—Shows an array of information that is related to the state of the system, including the current configuration, last crash file, CPU utilization, and memory utilization.
- **show run-config**—Shows the complete configuration of the controller. To exclude access point configuration settings, use the **show run-config no-ap** command.

Note If you want to see the passwords in clear text, enter the **config passwd-cleartext enable command**. To execute this command, you must enter an admin password. This command is valid only for this particular session. It is not saved following a reboot.

- **show run-config commands**—Shows the list of configured commands on the controller. This command shows only values that you configured. It does not show system-configured default values.

Configuring System and Message Logging

System and Message Logging

System logging allows controllers to log their system events to up to three remote syslog servers. The controller sends a copy of each syslog message as it is logged to each syslog server configured on the controller. Being able to send the syslog messages to multiple servers ensures that the messages are not lost due to the temporary unavailability of one syslog server. Message logging allows system messages to be logged to the controller buffer or console.

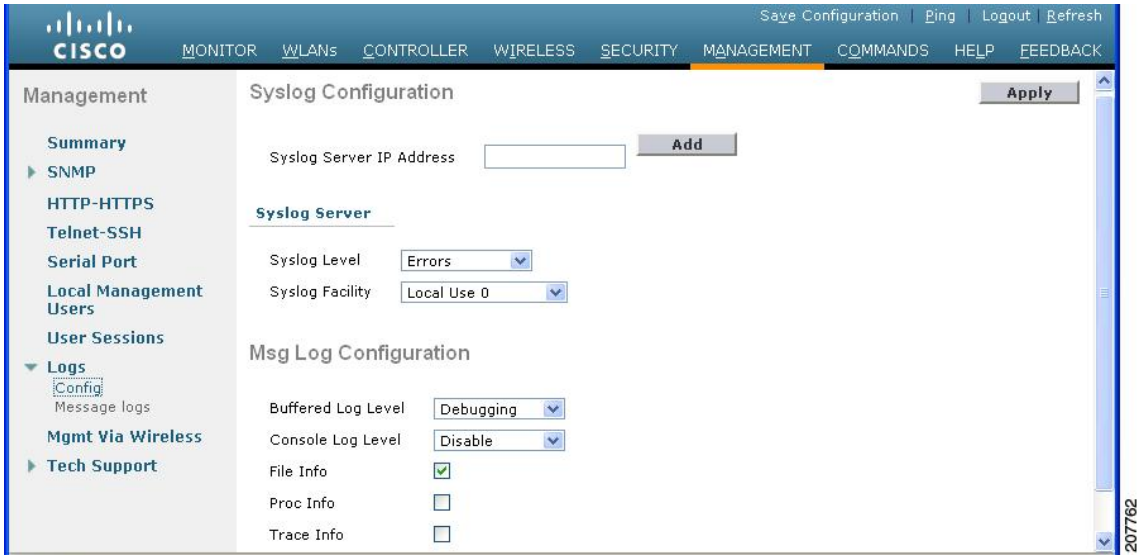
For more information about system messages and trap logs, see http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-system-message-guides-list.html.

This section contains the following subsections:

Configuring System and Message Logging (GUI)

Step 1 Choose **Management > Logs > Config**. The Syslog Configuration page appears.

Figure 24: Syslog Configuration Page



Step 2 In the **Syslog Server IP Address (IPv4/IPv6)** text box, enter the IPv4/IPv6 address of the server to which to send the syslog messages and click **Add**. You can add up to three syslog servers to the controller. The list of syslog servers that have already been added to the controller appears below this text box.

Note If you want to remove a syslog server from the controller, click **Remove** to the right of the desired server.

Step 3 To set the severity level for filtering syslog messages to the syslog servers, choose one of the following options from the **Syslog Level** drop-down list:

- **Emergencies** = Severity level 0
- **Alerts** = Severity level 1 (default value)
- **Critical** = Severity level 2
- **Errors** = Severity level 3
- **Warnings** = Severity level 4
- **Notifications** = Severity level 5
- **Informational** = Severity level 6
- **Debugging** = Severity level 7

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog servers. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog servers.

Note If you have enabled logging of debug messages to the logging buffer, some messages from application debug could be listed in message log with severity that is more than the level set. For example, if you execute the **debug client** *mac-addr* command, the client event log could be listed in message log even though the message severity level is set to **Errors**.

Step 4 To set the facility for outgoing syslog messages to the syslog servers, choose one of the following options from the **Syslog Facility** drop-down list:

- **Kernel** = Facility level 0
- **User Process** = Facility level 1
- **Mail** = Facility level 2
- **System Daemons** = Facility level 3
- **Authorization** = Facility level 4
- **Syslog** = Facility level 5 (default value)
- **Line Printer** = Facility level 6
- **USENET** = Facility level 7
- **Unix-to-Unix Copy** = Facility level 8
- **Cron** = Facility level 9
- **FTP Daemon** = Facility level 11
- **System Use 1** = Facility level 12
- **System Use 2** = Facility level 13
- **System Use 3** = Facility level 14
- **System Use 4** = Facility level 15
- **Local Use 0** = Facility level 16
- **Local Use 2** = Facility level 17
- **Local Use 3** = Facility level 18
- **Local Use 4** = Facility level 19
- **Local Use 5** = Facility level 20
- **Local Use 5** = Facility level 21
- **Local Use 5** = Facility level 22
- **Local Use 5** = Facility level 23

Step 5 Click **Apply**.

Step 6 To set the severity level for logging messages to the controller buffer and console, choose one of the following options from both the **Buffered Log Level** and **Console Log Level** drop-down lists:

- **Emergencies** = Severity level 0
- **Alerts** = Severity level 1
- **Critical** = Severity level 2
- **Errors** = Severity level 3 (default value)
- **Warnings** = Severity level 4
- **Notifications** = Severity level 5
- **Informational** = Severity level 6
- **Debugging** = Severity level 7
- **Disable**— This option is available only for Console Log level. Select this option to disable console logging.

If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

Step 7 Select the **File Info** check box if you want the message logs to include information about the source file. The default value is enabled.

Step 8 Select the **Trace Info** check box if you want the message logs to include traceback information. The default is disabled.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Viewing Message Logs (GUI)

To view message logs using the controller GUI, choose **Management > Logs > Message Logs**. The Message Logs page appears.

Note To clear the current message logs from the controller, click **Clear**.

Configuring System and Message Logging (CLI)

Step 1 Enable system logging and set the IP address of the syslog server to which to send the syslog messages by entering this command:

config logging syslog host *server_IP_address*

You can add up to three syslog servers to the controller.

Note To remove a syslog server from the controller by entering this command: **config logging syslog host** *server_IP_address* **delete**

Step 2 Set the severity level for filtering syslog messages to the syslog server by entering this command:

config logging syslog level *severity_level*

where *severity_level* is one of the following:

- emergencies = Severity level 0
- alerts = Severity level 1
- critical = Severity level 2
- errors = Severity level 3
- warnings = Severity level 4
- notifications = Severity level 5
- informational = Severity level 6
- debugging = Severity level 7

Note As an alternative, you can enter a number from 0 through 7 for the *severity_level* parameter.

Note If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog server. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog server.

Step 3 Set the severity level for filtering syslog messages for a particular access point or for all access points by entering this command:

config ap logging syslog level *severity_level* {*Cisco_AP* | **all**}

where *severity_level* is one of the following:

- emergencies = Severity level 0
- alerts = Severity level 1
- critical = Severity level 2
- errors = Severity level 3
- warnings = Severity level 4
- notifications = Severity level 5
- informational = Severity level 6
- debugging = Severity level 7

Note If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the access point. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the access point.

Step 4 Set the facility for outgoing syslog messages to the syslog server by entering this command:

config logging syslog facility *facility-code*

where *facility-code* is one of the following:

- ap = AP related traps.
- authorization = Authorization system. Facility level = 4.
- auth-private = Authorization system (private). Facility level = 10.
- cron = Cron/at facility. Facility level = 9.
- daemon = System daemons. Facility level = 3.
- ftp = FTP daemon. Facility level = 11.
- kern = Kernel. Facility level = 0.
- local0 = Local use. Facility level = 16.
- local1 = Local use. Facility level = 17.
- local2 = Local use. Facility level = 18.
- local3 = Local use. Facility level = 19.
- local4 = Local use. Facility level = 20.
- local5 = Local use. Facility level = 21.
- local6 = Local use. Facility level = 22.
- local7 = Local use. Facility level = 23.
- lpr = Line printer system. Facility level = 6.
- mail = Mail system. Facility level = 2.
- news = USENET news. Facility level = 7.
- sys12 = System use. Facility level = 12.
- sys13 = System use. Facility level = 13.
- sys14 = System use. Facility level = 14.
- sys15 = System use. Facility level = 15.
- syslog = The syslog itself. Facility level = 5.

- user = User process. Facility level = 1.
- uucp = Unix-to-Unix copy system. Facility level = 8.

Step 5 Configure the syslog facility for AP using the following command:

config logging syslog facility *AP*

where *AP* can be:

- associate= Associated sys log for AP
- disassociate=Disassociate sys log for AP

Step 6 Configure the syslog facility for an AP or all APs by entering this command:

config ap logging syslog facility *facility-level* {*Cisco_AP* | **all**}

where *facility-level* is one of the following:

- auth = Authorization system
- cron = Cron/at facility
- daemon = System daemons
- kern = Kernel
- local0 = Local use
- local1 = Local use
- local2 = Local use
- local3 = Local use
- local4 = Local use
- local5 = Local use
- local6 = Local use
- local7 = Local use
- lpr = Line printer system
- mail = Mail system
- news = USENET news
- sys10 = System use
- sys11 = System use
- sys12 = System use
- sys13 = System use
- sys14 = System use
- sys9 = System use
- syslog = Syslog itself
- user = User process
- uucp = Unix-to-Unix copy system

Step 7 Configure the syslog facility for Client by entering this command:

config logging syslog facility *Client*

where *facility-code* can be:

- assocfail Dot11= association fail syslog for clients
- associate Dot11=association syslog for clients

- authentication=authentication success syslog for clients
- authfail Dot11=authentication fail syslog for clients
- deauthenticate Dot11=deauthentication syslog for clients
- disassociate Dot11=disassociation syslog for clients
- excluded Excluded=syslog for clients

Step 8 Set the severity level for logging messages to the controller buffer and console, enter these commands:

- **config logging buffered** *severity_level*
- **config logging console** *severity_level*

where *severity_level* is one of the following:

- emergencies = Severity level 0
- alerts = Severity level 1
- critical = Severity level 2
- errors = Severity level 3
- warnings = Severity level 4
- notifications = Severity level 5
- informational = Severity level 6
- debugging = Severity level 7

Note As an alternative, you can enter a number from 0 through 7 for the *severity_level* parameter.

Note If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

Step 9 Save debug messages to the controller buffer, the controller console, or a syslog server by entering these commands:

- **config logging debug buffered {enable | disable}**
- **config logging debug console {enable | disable}**
- **config logging debug syslog {enable | disable}**

  By default, the console command is enabled, and the buffered and syslog commands are disabled.

Step 10 To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information by entering this command:

config logging fileinfo {enable | disable}

The default value is enabled.

Step 11 Configure the controller to include process information in the message logs or to prevent the controller from displaying this information by entering this command:

config logging procinfo {**enable** | **disable**}

The default value is disabled.

Step 12 Configure the controller to include traceback information in the message logs or to prevent the controller from displaying this information by entering this command:

config logging traceinfo {enable | disable}

The default value is disabled.

Step 13 Enable or disable timestamps in log messages and debug messages by entering these commands:

- **config service timestamps log {datetime | disable}**
- **config service timestamps debug {datetime | disable}**

  where

  - **datetime** = Messages are timestamped with the standard date and time. This is the default value.
  - **disable** = Messages are not timestamped.

Step 14 Save your changes by entering this command:

save config

Viewing System and Message Logs (CLI)

To see the logging parameters and buffer contents, enter this command:

show logging

Viewing Access Point Event Logs

Information About Access Point Event Logs

Access points log all system messages (with a severity level greater than or equal to notifications) to the access point event log. The event log can contain up to 1024 lines of messages, with up to 128 characters per line. When the event log becomes filled, the oldest message is removed to accommodate a new event message. The event log is saved in a file on the access point flash, which ensures that it is saved through a reboot cycle. To minimize the number of writes to the access point flash, the contents of the event log are written to the event log file during normal reload and crash scenarios only.

Viewing Access Point Event Logs (CLI)

Use these CLI commands to view or clear the access point event log from the controller:

- To see the contents of the event log file for an access point that is joined to the controller, enter this command:

show ap eventlog *Cisco_AP*

Information similar to the following appears:

```
AP event log download has been initiated
Waiting for download to complete

AP event log download completed.
 ====================== AP Event log Contents ====================
*Sep 22 11:44:00.573: %CAPWAP-5-CHANGED: CAPWAP changed state to IMAGE
*Sep 22 11:44:01.514: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to down
*Sep 22 11:44:01.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1,
changed state to down
*Sep 22 11:44:53.539: *** Access point reloading. Reason: NEW IMAGE DOWNLOAD ***
*Mar 1 00:00:39.078: %CAPWAP-3-ERRORLOG: Did not get log server settings from DHCP.
*Mar 1 00:00:42.142: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:00:42.151: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Mar 1 00:00:42.158: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 00:00:43.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed
 state to up
*Mar 1 00:00:43.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed
 state to up
*Mar 1 00:00:48.078: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER
*Mar 1 00:01:42.144: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:01:48.121: %CAPWAP-3-CLIENTERRORLOG: Set Transport Address: no more AP manager
 IP addresses remain
*Mar 1 00:01:48.122: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
```

- To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, enter this command:

  clear ap-eventlog {**specific** *Cisco_AP* | **all**}

Uploading Logs and Crash Files

Upload Logs and Crash Files

- Follow the instructions in this section to upload logs and crash files from the controller. However, before you begin, ensure you have a TFTP or FTP server available for the file upload. Follow these guidelines when setting up a TFTP or FTP server:
  - If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.

- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

This section contains the following subsections:

Uploading Logs and Crash Files (GUI)

Step 1 Choose **Command > Upload File**. The Upload File from Controller page appears.

Step 2 From the **File Type** drop-down list, choose one of the following:

- **Event Log**
- **Message Log**
- **Trap Log**
- **Crash File**

Step 3 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in the 7.4 and later releases)

Step 4 In the **IP Address** text box, enter the IP address of the server.

Step 5 In the **File Path** text box, enter the directory path of the log or crash file.

Step 6 In the **File Name** text box, enter the name of the log or crash file.

Step 7 If you chose FTP as the Transfer Mode, follow these steps:

a. In the **Server Login Username** text box, enter the FTP server login name.

b. In the **Server Login Password** text box, enter the FTP server login password.

c. In the **Server Port Number** text box, enter the port number of the FTP server. The default value for the server port is 21.

Step 8 Click **Upload** to upload the log or crash file from the controller. A message appears indicating the status of the upload.

Uploading Logs and Crash Files (CLI)

Step 1 To transfer the file from the controller to a server, enter this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 2 To specify the type of file to be uploaded, enter this command:

transfer upload datatype *datatype*

where *datatype* is one of the following options:

- **crashfile**—Uploads the system's crash file.
- **errorlog**—Uploads the system's error log.
- **panic-crash-file**—Uploads the kernel panic information if a kernel panic occurs.
- **systemtrace**—Uploads the system's trace file.
- **traplog**—Uploads the system's trap log.
- **watchdog-crash-file**—Uploads the console dump resulting from a software-watchdog-initiated reboot of the controller following a crash. The software watchdog module periodically checks the integrity of the internal software and makes sure that the system does not stay in an inconsistent or nonoperational state for a long period of time.

Step 3 To specify the path to the file, enter these commands:

- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

Step 4 If you are using an FTP server, also enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 5 To see the updated settings, enter this command:

transfer upload start

Step 6 When prompted to confirm the current settings and start the software upload, answer **y**.

Uploading Core Dumps from the Controller

Uploading Core Dumps from the Controller

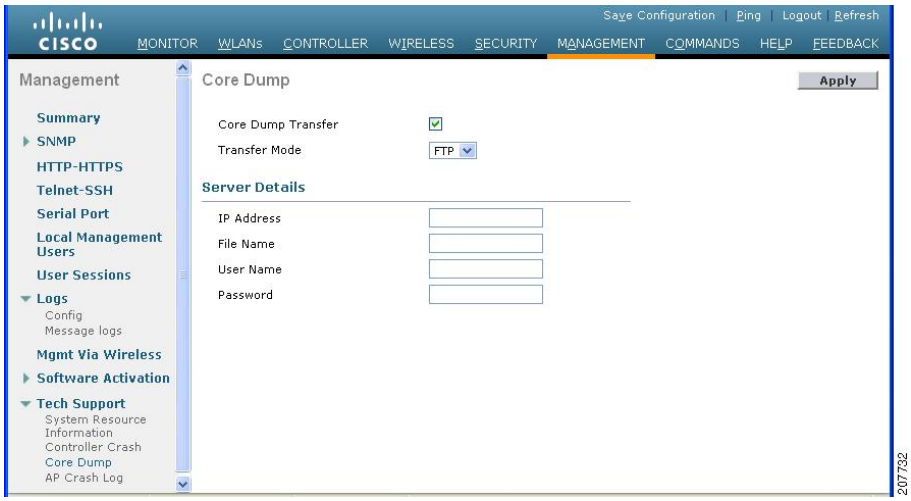
To help troubleshoot controller crashes, you can configure the controller to automatically upload its core dump file to an FTP server after experiencing a crash. However, you cannot automatically send crash files to an FTP server.

This section contains the following subsections:

Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI)

Step 1 Choose **Management > Tech Support > Core Dump** to open the Core Dump page.

Figure 25: Core Dump Page



Step 2 To enable the controller to generate a core dump file following a crash, select the **Core Dump Transfer** check box.

Step 3 To specify the type of server to which the core dump file is uploaded, choose **FTP** from the **Transfer Mode** drop-down list.

Step 4 In the **IP Address** text box, enter the IP address of the FTP server.

Note The controller must be able to reach the FTP server.

Step 5 In the **File Name** text box, enter the name that the controller uses to label the core dump file.

Step 6 In the **User Name** text box, enter the username for FTP login.

Step 7 In the **Password** text box, enter the password for FTP login.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (CLI)

Step 1 To enable or disable the controller to generate a core dump file following a crash, enter this command:

config coredump {**enable** | **disable**}

Step 2 To specify the FTP server to which the core dump file is uploaded, enter this command:

config coredump ftp *server_ip_address filename*

where

- *server_ip_address* is the IP address of the FTP server to which the controller sends its core dump file.

  Note The controller must be able to reach the FTP server.

- *filename* is the name that the controller uses to label the core dump file.

Step 3 To specify the username and password for FTP login, enter this command:
config coredump username *ftp_username* **password** *ftp_password*

Step 4 To save your changes, enter this command:
save config

Step 5 To see a summary of the controller's core dump file, enter this command:
show coredump summary

Example:

Information similar to the following appears:

```
Core Dump is enabled

FTP Server IP................................... 10.10.10.17
FTP Filename.................................... file1
FTP Username.................................... ftpuser
FTP Password.................................... *********
```

Uploading Core Dumps from Controller to a Server (CLI)

Step 1 To see information about the core dump file in flash memory, enter this command:

show coredump summary

Information similar to the following appears:

```
Core Dump is disabled

Core Dump file is saved on flash

Sw Version..................................... 6.0.83.0
Time Stamp..................................... Wed Feb  4 13:23:11 2009
File Size...................................... 9081788
File Name Suffix........................... filename.gz
```

Step 2 To transfer the file from the controller to a server, enter these commands:

- **transfer upload mode** {**tftp** | **ftp** | **sftp**}
- **transfer upload datatype coredump**

- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

Note After the file is uploaded, it ends with a .gz suffix. If desired, you can upload the same core dump file multiple times with different names to different servers.

Step 3 If you are using an FTP server, also enter these commands:

- **transfer upload username** *username*

  transfer upload password *password*
- **transfer upload port** *port*

Note The default value for the *port* parameter is 21.

Step 4 To view the updated settings, enter this command:

transfer upload start

Step 5 When prompted to confirm the current settings and start the software upload, answer y.

Uploading Packet Capture Files

Uploading Packet Capture Files

When a controller's data plane crashes, it stores the last 50 packets that the controller received in flash memory. This information can be useful in troubleshooting the crash.

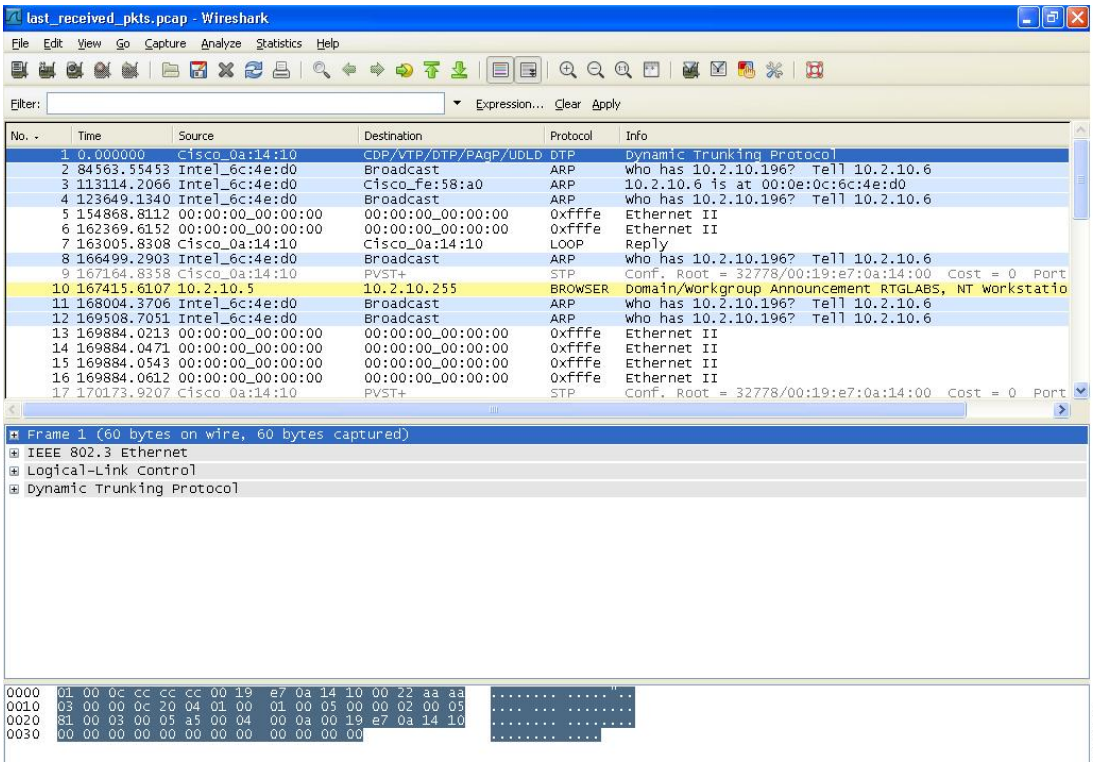
When a crash occurs, the controller generates a new packet capture file (*.pcap) file, and a message similar to the following appears in the controller crash file:

```
Last 5 packets processed at each core are stored in
 "last_received_pkts.pcap" captured file.
   - Frame 36,38,43,47,49, processed at core #0.
   - Frame 14,27,30,42,45, processed at core #1.
   - Frame 15,18,20,32,48, processed at core #2.
   - Frame 11,29,34,37,46, processed at core #3.
   - Frame 7,8,12,31,35, processed at core #4.
   - Frame 21,25,39,41,50, processed at core #5.
   - Frame 16,17,19,22,33, processed at core #6.
   - Frame 6,10,13,23,26, processed at core #7.
   - Frame 9,24,28,40,44, processed at core #8.
   - Frame 1,2,3,4,5, processed at core #9.
```

You can use the controller GUI or CLI to upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file.

Figure 26: Sample Output of Packet Capture File in Wireshark

This figure shows a sample output of the packet capture in Wireshark.



This section contains the following subsections:

Restrictions for Uploading Packet Capture Files

- Only Cisco 5508 WLCs generate packet capture files. This feature is not available on other controller platforms.
- Ensure that you have a TFTP or FTP server available for the file upload. Follow these guidelines when setting up a TFTP or FTP server:
  - If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Uploading Packet Capture Files (GUI)

Step 1 Choose **Commands > Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **Packet Capture**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in the 7.4 and later releases)

Step 4 In the **IP Address** text box, enter the IP address of the server.

Step 5 In the **File Path** text box, enter the directory path of the packet capture file.

Step 6 In the **File Name** text box, enter the name of the packet capture file. These files have a .pcap extension.

Step 7 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** text box, enter the username to log into the FTP server.
b) In the **Server Login Password** text box, enter the password to log into the FTP server.
c) In the **Server Port Number** text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 8 Click **Upload** to upload the packet capture file from the controller. A message appears indicating the status of the upload.

Step 9 Use Wireshark or another standard packet capture tool to open the packet capture file and see the last 50 packets that were received by the controller.

Uploading Packet Capture Files (CLI)

Step 1 Log on to the controller CLI.

Step 2 Enter the **transfer upload mode** {**tftp** | **ftp** | **sftp**} command.

Step 3 Enter the **transfer upload datatype packet-capture** command.

Step 4 Enter the **transfer upload serverip** *server-ip-address* command.

Step 5 Enter the **transfer upload path** *server-path-to-file* command.

Step 6 Enter the **transfer upload filename** *last_received_pkts*.pcap command.

Step 7 If you are using an FTP server, enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the *port* parameter is 21.

Step 8 Enter the **transfer upload start** command to see the updated settings and then answer **y** when prompted to confirm the current settings and start the upload process.

Step 9 Use Wireshark or another standard packet capture tool to open the packet capture file and see the last 50 packets that were received by the controller.

Monitoring Memory Leaks

This section provides instructions for troubleshooting hard-to-solve or hard-to-reproduce memory problems.

Caution The commands in this section can be disruptive to your system and should be run only when you are advised to do so by the Cisco Technical Assistance Center (TAC).

This section contains the following subsection:

Monitoring Memory Leaks (CLI)

Step 1 To enable or disable monitoring for memory errors and leaks, enter this command:

config memory monitor errors {**enable** | **disable**}

The default value is disabled.

Note Your changes are not saved across reboots. After the controller reboots, it uses the default setting for this feature.

Step 2 If you suspect that a memory leak has occurred, enter this command to configure the controller to perform an auto-leak analysis between two memory thresholds (in kilobytes):

config memory monitor leaks *low_thresh high_thresh*

If the free memory is lower than the *low_thresh* threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 kilobytes, and you cannot set it below this value.

Set the *high_thresh* threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified *high_thresh* threshold, the process of tracking and freeing memory allocation begins. As a result, the **debug memory events enable** command shows all allocations and frees, and the **show memory monitor detail** command starts to detect any suspected memory leaks. The default value for this parameter is 30000 kilobytes.

Step 3 To see a summary of any discovered memory issues, enter this command:

show memory monitor

Information similar to the following appears:

```
Memory Leak Monitor Status:
low_threshold(10000), high_threshold(30000), current status(disabled)

-----------------------------------------

Memory Error Monitor Status:
Crash-on-error flag currently set to (disabled)
```

```
No memory error detected.
```

Step 4 To see the details of any memory leaks or corruption, enter this command:

show memory monitor detail

Information similar to the following appears:

```
Memory error detected. Details:
------------------------------------------------
-  Corruption detected at pmalloc entry address:        (0x179a7ec0)
-  Corrupt entry:headerMagic(0xdeadf00d),trailer(0xabcd),poison(0xreadceef),
entrysize(128),bytes(100),thread(Unknown task name, task id = (332096592)),
file(pmalloc.c),line(1736),time(1027)

Previous 1K memory dump from error location.
------------------------------------------------
(179a7ac0): 00000000 00000000 00000000 ceeff00d readf00d 00000080 00000000 00000000
(179a7ae0): 17958b20 00000000 1175608c 00000078 00000000 readceef 179a7afc 00000001
(179a7b00): 00000003 00000006 00000001 00000004 00000001 00000009 00000009 0000020d
(179a7b20): 00000001 00000002 00000002 00000001 00000004 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 192f465e 7791acc8 e5032242 5365788c a1b7cee6 00000000 00000000
(179a7b60): 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 17958dc0 00000000 1175608c 00000078 00000000 readceef
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000004 00000001 00003763
(179a7bc0): 00000002 00000002 00000010 00000001 00000002 00000000 0000001e 00000013
(179a7be0): 0000001a 00000089 00000000 00000000 000000d8 00000000 00000000 17222194
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): readf00d 00000080 00000000 00000000 179a7b78 00000000 1175608c 00000078
```

Step 5 If a memory leak occurs, enter this command to enable debugging of errors or events during memory allocation:
debug memory {errors | events} {enable | disable}

Troubleshooting CCXv5 Client Devices

Information About Troubleshooting CCXv5 Client Devices

The controller supports three features designed to help troubleshoot communication problems with CCXv5 clients: diagnostic channel, client reporting, and roaming and real-time diagnostics.

Restrictions for CCXv5 Client Devices

Diagnostic channel, client reporting, and roaming and real-time diagnostics features are supported only on CCXv5 clients. They are not supported for use with non-CCX clients or with clients running an earlier version of CCX.

Configuring 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 controller GUI or CLI to enable the diagnostic channel, and you can use the controller **diag-channel** 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. CCX Diagnostic feature has been tested only with clients having Cisco ADU card

Configuring the Diagnostic Channel (GUI)

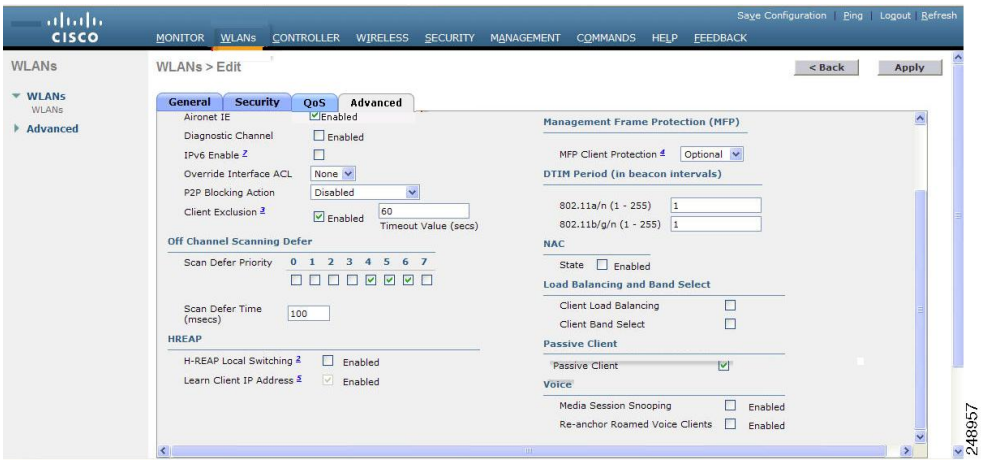
Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Create a new WLAN or click the ID number of an existing WLAN.

Note We recommend that you create a new WLAN on which to run the diagnostic tests.

Step 3 When the **WLANs > Edit** page appears, choose the **Advanced** tab to open the **WLANs > Edit (Advanced)** page.

Figure 27: WLANs > Edit (Advanced) Page



Step 4 If you want to enable diagnostic channel troubleshooting on this WLAN, select the **Diagnostic Channel** check box. Otherwise, leave this check box unselected, which is the default value.

Note You can use the CLI to initiate diagnostic tests on the client.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring the Diagnostic Channel (CLI)

Step 1 To enable diagnostic channel troubleshooting on a particular WLAN, enter this command:

config wlan diag-channel {**enable** | **disable**} *wlan_id*

Step 2 To verify that your change has been made, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... employee1
Network Name (SSID).............................. employee
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. Infinity
Interface........................................ virtual
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Enabled
...
```

Step 3 To send a request to the client to perform the DHCP test, enter this command:

config client ccx dhcp-test *client_mac_address*

Note This test does not require the client to use the diagnostic channel.

Step 4 To send a request to the client to perform the default gateway ping test, enter this command:

config client ccx default-gw-ping *client_mac_address*

Note This test does not require the client to use the diagnostic channel.

Step 5 To send a request to the client to perform the DNS server IP address ping test, enter this command:

config client ccx dns-ping *client_mac_address*

Note This test does not require the client to use the diagnostic channel.

Step 6 To send a request to the client to perform the DNS name resolution test to the specified host name, enter this command:

config client ccx dns-resolve *client_mac_address host_name*

Note This test does not require the client to use the diagnostic channel.

Step 7 To send a request to the client to perform the association test, enter this command:

config client ccx test-association *client_mac_address ssid bssid* {**802.11a | 802.11b | 802.11g**} *channel*

Step 8 To send a request to the client to perform the 802.1X test, enter this command:

config client ccx test-dot1x *client_mac_address profile_id bssid* {**802.11a** | **802.11b** | **802.11g**} *channel*

Step 9 To send a request to the client to perform the profile redirect test, enter this command:

config client ccx test-profile *client_mac_address profile_id*

The *profile_id* should be from one of the client profiles for which client reporting is enabled.

Note Users are redirected back to the parent WLAN, not to any other profile. The only profile shown is the user's parent profile. Note however that parent WLAN profiles can have one child diagnostic WLAN.

Step 10 Use these commands if necessary to terminate or clear a test:

- To send a request to the client to terminate the current test, enter this command:

  config client ccx test-abort *client_mac_address*

  Only one test can be pending at a time, so this command terminates the current pending test.

- To clear the test results on the controller, enter this command:

  config client ccx clear-results *client_mac_address*

Step 11 To send a message to the client, enter this command:

config client ccx send-message *client_mac_address message_id*

where *message_id* is one of the following:

- 1 = The SSID is invalid.
- 2 = The network settings are invalid.
- 3 = There is a WLAN credibility mismatch.
- 4 = The user credentials are incorrect.
- 5 = Please call support.
- 6 = The problem is resolved.
- 7 = The problem has not been resolved.
- 8 = Please try again later.
- 9 = Please correct the indicated problem.
- 10 = Troubleshooting is refused by the network.
- 11 = Retrieving client reports.
- 12 = Retrieving client logs.
- 13 = Retrieval complete.
- 14 = Beginning association test.
- 15 = Beginning DHCP test.

- 16 = Beginning network connectivity test.
- 17 = Beginning DNS ping test.
- 18 = Beginning name resolution test.
- 19 = Beginning 802.1X authentication test.
- 20 = Redirecting client to a specific profile.
- 21 = Test complete.
- 22 = Test passed.
- 23 = Test failed.
- 24 = Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25 = Log retrieval refused by the client.
- 26 = Client report retrieval refused by the client.
- 27 = Test request refused by the client.
- 28 = Invalid network (IP) setting.
- 29 = There is a known outage or problem with the network.
- 30 = Scheduled maintenance period.
- 31 = The WLAN security method is not correct.
- 32 = The WLAN encryption method is not correct.
- 33 = The WLAN authentication method is not correct.

Step 12 To see the status of the last test, enter this command:

show client ccx last-test-status *client_mac_address*

Information similar to the following appears for the default gateway ping test:

```
Test Type..................................... Gateway Ping Test
Test Status................................... Pending/Success/Timeout

Dialog Token.................................. 15
Timeout....................................... 15000 ms
Request Time.................................. 1329 seconds since system boot
```

Step 13 To see the status of the last test response, enter this command:

show client ccx last-response-status *client_mac_address*

Information similar to the following appears for the 802.1X authentication test:

```
Test Status................................... Success

Response Dialog Token......................... 87
Response Status............................... Successful
Response Test Type............................ 802.1x Authentication Test
Response Time................................. 3476 seconds since system boot
```

Step 14 To see the results from the last successful diagnostics test, enter this command:

show client ccx results *client_mac_address*

Information similar to the following appears for the 802.1X authentication test:

```
dot1x Complete..................................... Success
EAP Method......................................... *1,Host OS Login Credentials
dot1x Status.................................... 255
```

Step 15 To see the relevant data frames captured by the client during the previous test, enter this command:

show client ccx frame-data *client_mac_address*

Information similar to the following appears:

```
LOG Frames:

Frame Number:...................................... 1
Last Frame Number:................................. 1120
Direction:......................................... 1
Timestamp:......................................... 0d 00h 50m 39s 863954us
Frame Length:...................................... 197
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd bd b0  ............D...
00000010: 00 12 44 bd bd b0 f0 af  43 70 00 f2 82 01 00 00  ..D.....Cp......
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 32 33 2d  31 30 00 00 00 00 00 00  ...AP23-10......
00000050: 00 00 00 00 00 00 26 96  06 00 40 96 00 ff ff dd  ......&...@.....
00000060: 18 00 50 f2 01 01 00 00  50 f2 05 01 00 00 50 f2  ..P.....P.....P.
00000070: 05 01 00 00 40 96 00 28  00 dd 06 00 40 96 01 01  ....@..(....@...

00000080: 00 dd 05 00 40 96 03 04  dd 16 00 40 96 04 00 02  ....@......@....
00000090: 07 a4 00 00 23 a4 00 00  42 43 00 00 62 32 00 00  ....#...BC..b2..
000000a0: dd 05 00 40 96 0b 01 dd  18 00 50 f2 02 01 01 82  ...@......P.....
000000b0: 00 03 a4 00 00 27 a4 00  00 42 43 5e 00 62 32 2f  .....'...BC^.b2/

LOG Frames:

Frame Number:...................................... 2
Last Frame Number:................................. 1120
Direction:......................................... 1
Timestamp:......................................... 0d 00h 50m 39s 878289us
Frame Length:...................................... 147
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 0d ed c3 a0 22  ..............."
00000010: 00 0d ed c3 a0 22 00 bd  4d 50 a5 f7 78 08 00 00  ....."..MP..x...
00000020: 64 00 01 00 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 84 00 0f 00 ff  l...............
00000040: 03 19 00 72 6f 67 75 65  2d 74 65 73 74 31 00 00  ...rogue-test1..
00000050: 00 00 00 00 00 00 23 96  06 00 40 96 00 10 00 dd  ......#...@.....
00000060: 06 00 40 96 01 01 00 dd  05 00 40 96 03 04 dd 05  ..@.......@.....
00000070: 00 40 96 0b 01 dd 18 00  50 f2 02 01 01 81 00 03  .@......P.......

00000080: a4 00 00 27 a4 00 00 42  43 5e 00 62 32 2f 00 d2  ...'...BC^.b2/..
00000090: b4 ab 84                                          ...

LOG Frames:

Frame Number:...................................... 3
Last Frame Number:................................. 1120
```

```
Direction:..................................... 1
Timestamp:..................................... 0d 00h 50m 39s 881513us
Frame Length:.................................. 189
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd 80 30  ............D..0
00000010: 00 12 44 bd 80 30 60 f7  46 c0 8b 4b d1 05 00 00  ..D..0`.F..K....
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 00 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 34 30 2d  31 37 00 00 00 00 00 00  ...AP40-17......
00000050: 00 00 00 00 00 00 26 dd  18 00 50 f2 01 01 00 00  ......&...P.....
00000060: 50 f2 05 01 00 00 50 f2  05 01 00 00 40 96 00 28  P.....P.....@..(
00000070: 00 dd 06 00 40 96 01 01  00 dd 05 00 40 96 03 04  ....@.......@...

00000080: dd 16 00 40 96 04 00 05  07 a4 00 00 23 a4 00 00  ...@........#...
00000090: 42 43 00 00 62 32 00 00  dd 05 00 40 96 0b 01 dd  BC..b2.....@....
000000a0: 18 00 50 f2 02 01 01 85  00 03 a4 00 00 27 a4 00  ..P..........'..
000000b0: 00 42 43 5e 00 62 32 2f  00 0b 9a 1d 6f           .BC^.b2/....o
...
```

Configuring Client Reporting

The client reporting protocol is used by the client and the access point to exchange client information. Client reports are collected automatically when the client associates. You can use the controller GUI or CLI to send a client report request to any CCXv5 client any time after the client associates. There are four types of client reports:

- **Client profile**—Provides information about the configuration of the client.
- **Operating parameters**—Provides the details of the client's current operational modes.
- **Manufacturers' information**—Provides data about the wireless LAN client adapter in use.
- **Client capabilities**—Provides information about the client's capabilities.

Configuring Client Reporting (GUI)

Step 1 Choose **Monitor > Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client. The **Clients > Detail** page appears.

Step 3 To send a report request to the client, click **Send CCXV5 Req**.

Note You must create a Trusted Profile using ACAU for Cisco CB21AG or equivalent software from your CCXv5 vendor.

Step 4 To view the parameters from the client, click **Display**. The Client Reporting page appears.

Step 5 Click the link for the desired client profile. The Profile Details page appears displaying the client profile details, including the SSID, power save mode, radio channel, data rates, and 802.11 security settings.

Configuring Client Reporting (CLI)

Step 1 To send a request to the client to send its profiles, enter this command:

config client ccx get-profiles *client_mac_address*

Step 2 To send a request to the client to send its current operating parameters, enter this command:

config client ccx get-operating-parameters *client_mac_address*

Step 3 To send a request to the client to send the manufacturer's information, enter this command:

config client ccx get-manufacturer-info *client_mac_address*

Step 4 To send a request to the client to send its capability information, enter this command:

config client ccx get-client-capability *client_mac_address*

Step 5 To clear the client reporting information, enter this command:

config client ccx clear-reports *client_mac_address*

Step 6 To see the client profiles, enter this command:

show client ccx profiles *client_mac_address*

Step 7 To see the client operating parameters, enter this command:

show client ccx operating-parameters *client_mac_address*

Step 8 To see the client manufacturer information, enter this command:

show client ccx manufacturer-info *client_mac_address*

Step 9 To see the client's capability information, enter this command:

show client ccx client-capability *client_mac_address*

Note This command displays the client's available capabilities, not current settings for the capabilities.

Configuring Roaming and Real-Time Diagnostics

You can use roaming and real-time logs and statistics to solve system problems. The event log enables you to identify and track the behavior of a client device. It is especially useful when attempting to diagnose difficulties that a user may be having on a WLAN. The event log provides a log of events and reports them to the access point. There are three categories of event logs:

- Roaming log—This log provides a historical view of the roaming events for a given client. The client maintains a minimum of five previous roaming events including failed attempts and successful roams.
- Robust Security Network Association (RSNA) log—This log provides a historical view of the authentication events for a given client. The client maintains a minimum of five previous authentication attempts including failed attempts and successful ones.

- Syslog—This log provides internal system information from the client. For example, it may indicate problems with 802.11 operation, system operation, and so on.

The statistics report provides 802.1X and security information for the client. You can use the controller CLI to send the event log and statistics request to any CCXv5 client any time after the client associates.

Configuring Roaming and Real-Time Diagnostics (CLI)

Step 1 To send a log request, enter this command:

config client ccx log-request *log_type client_mac_address*

where *log_type* is roam, rsna, or syslog.

Step 2 To view a log response, enter this command:

show client ccx log-response *log_type client_mac_address*

where *log_type* is roam, rsna, or syslog.

Information similar to the following appears for a log response with a *log_type* of roam:

```
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 13s 322396us
                         Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3125(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 16s 599006us
                         Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3235(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 19s 882921us
                         Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3234(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 08s 815477us
                         Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:d2, Transition
 Time=3281(ms)
                          Transition Reason: First association to WLAN
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 26s 637084us
                         Source BSSID=00:0b:85:81:06:d2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3313(ms)
```

Information similar to the following appears for a log response with a *log_type* of rsna:

```
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246578us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
```

```
                            AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                          RSNA Result: Success
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246625us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                          RSNA Result: Success
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 01s 624375us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
            RSNA Result: Success
```

Information similar to the following appears for a log response with a *log_type* of syslog:

```
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278987us
                         Client SysLog = '<11> Jun 19 11:49:47 uraval3777 Mandatory elements missing
 in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278990us
                         Client SysLog = '<11> Jun 19 11:49:50 uraval3777 Mandatory elements missing
 in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278993us
                         Client SysLog = '<11> Jun 19 11:49:53 uraval3777 Mandatory elements missing
 in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278996us
                         Client SysLog = '<11> Jun 19 11:49:56 uraval3777 Mandatory elements missing
 in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279000us
                         Client SysLog = '<11> Jun 19 11:50:00 uraval3777 Mandatory elements missing
 in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279003us
                         Client SysLog = '<11> Jun 19 11:50:03 uraval3777 Mandatory elements missing
 in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279009us
                         Client SysLog = '<11> Jun 19 11:50:09 uraval3777 Mandatory elements missing
 in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279012us
                         Client SysLog = '<11> Jun 19 11:50:12 uraval3777 Mandatory elements missing
 in the OID response'
```

Step 3 To send a request for statistics, enter this command:

config client ccx stats-request *measurement_duration stats_name client_mac_address*

where *stats_name* is dot11 or security.

Step 4 To view the statistics response, enter this command:

show client ccx stats-report *client_mac_address*

Information similar to the following appears:

```
Measurement duration = 1

     dot11TransmittedFragmentCount       = 1
     dot11MulticastTransmittedFrameCount = 2
     dot11FailedCount                    = 3
     dot11RetryCount                     = 4
     dot11MultipleRetryCount             = 5
     dot11FrameDuplicateCount            = 6
     dot11RTSSuccessCount                = 7
     dot11RTSFailureCount                = 8
     dot11ACKFailureCount                = 9
     dot11ReceivedFragmentCount          = 10
     dot11MulticastReceivedFrameCount    = 11
     dot11FCSErrorCount                  = 12
     dot11TransmittedFrameCount          = 13
```

Using the Debug Facility

Using the Debug Facility

The debug facility enables you to display all packets going to and from the controller CPU. You can enable it for received packets, transmitted packets, or both. By default, all packets received by the debug facility are displayed. However, you can define access control lists (ACLs) to filter packets before they are displayed. Packets not passing the ACLs are discarded without being displayed.

Each ACL includes an action (permit, deny, or disable) and one or more fields that can be used to match the packet. The debug facility provides ACLs that operate at the following levels and on the following values:

- Driver ACL
  - NPU encapsulation type
  - Port
- Ethernet header ACL
  - Destination address
  - Source address
  - Ethernet type
  - VLAN ID
- IP header ACL
  - Source address

    - Destination address
    - Protocol
    - Source port (if applicable)
    - Destination port (if applicable)
- EoIP payload Ethernet header ACL
    - Destination address
    - Source address
    - Ethernet type
    - VLAN ID
- EoIP payload IP header ACL
    - Source address
    - Destination address
    - Protocol
    - Source port (if applicable)
    - Destination port (if applicable)
- CAPWAP payload 802.11 header ACL
    - Destination address
    - Source address
    - BSSID
    - SNAP header type
- CAPWAP payload IP header ACL
    - Source address
    - Destination address
    - Protocol
    - Source port (if applicable)
    - Destination port (if applicable)

At each level, you can define multiple ACLs. The first ACL that matches the packet is the one that is selected.

This section contains the following subsection:

Configuring the Debug Facility (CLI)

Step 1 To enable the debug facility, enter this command:

- **debug packet logging enable** {**rx** | **tx** | **all**} *packet_count display_size*

  where

  - **rx** displays all received packets, **tx** displays all transmitted packets, and **all** displays both transmitted and received packets.
  - *packet_count* is the maximum number of packets to log. You can enter a value between 1 and 65535 packets, and the default value is 25 packets.
  - *display_size* is the number of bytes to display when printing a packet. By default, the entire packet is displayed.

  Note To disable the debug facility, enter this command: **debug packet logging disable**.

- **debug packet logging acl driver** *rule_index action npu_encap port*

  where

  - *rule_index* is a value between 1 and 6 (inclusive).
  - *action* is permit, deny, or disable.
  - *npu_encap* specifies the NPU encapsulation type, which determines how packets are filtered. The possible values include dhcp, dot11-mgmt, dot11-probe, dot1x, eoip-ping, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rbcp, wired-guest, or any.
  - *port* is the physical port for packet transmission or reception.

- Use these commands to configure packet-logging ACLs:

  debug packet logging acl eth *rule_index action dst src type vlan*

  where

  - *rule_index* is a value between 1 and 6 (inclusive).
  - *action* is permit, deny, or disable.
  - *dst* is the destination MAC address.
  - *src* is the source MAC address.
  - *type* is the two-byte type code (such as 0x800 for IP, 0x806 for ARP). This parameter also accepts a few common string values such as “ip” (for 0x800) or “arp” (for 0x806).
  - *vlan* is the two-byte VLAN ID.

- **debug packet logging acl ip** *rule_index action src dst proto src_port dst_port*

  where

  - *proto* is a numeric or any string recognized by getprotobyname(). The controller supports the following strings: ip, icmp, igmp, ggp, ipencap, st, tcp, egp, pup, udp, hmp, xns-idp, rdp, iso-tp4, xtp, ddp, idpr-cmtp, rspf, vmtp, ospf, ipip, and encap.

- *src_port* is the UDP/TCP two-byte source port (for example, telnet, 23) or "any." The controller accepts a numeric or any string recognized by getservbyname(). The controller supports the following strings: tcpmux, echo, discard, systat, daytime, netstat, qotd, msp, chargen, ftp-data, ftp, fsp, ssh, telnet, smtp, time, rlp, nameserver, whois, re-mail-ck, domain, mtp, bootps, bootpc, tftp, gopher, rje, finger, www, link, kerberos, supdup, hostnames, iso-tsap, csnet-ns, 3com-tsmux, rtelnet, pop-2, pop-3, sunrpc, auth, sftp, uucp-path, nntp, ntp, netbios-ns, netbios-dgm, netbios-ssn, imap2, snmp, snmp-trap, cmip-man, cmip-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-rtmp, at-nbp, at-echo, at-zis, qmtp, z3950, ipx, imap3, ulistserv, https, snpp, saft, npmp-local, npmp-gui, and hmmp-ind.
- *dst_port* is the UDP/TCP two-byte destination port (for example, telnet, 23) or "any." The controller accepts a numeric or any string recognized by getservbyname(). The controller supports the same strings as those for the *src_port*.

- **debug packet logging acl eoip-eth** *rule_index action dst src type vlan*
- **debug packet logging acl eoip-ip** *rule_index action src dst proto src_port dst_port*
- **debug packet logging acl lwapp-dot11** *rule_index action dst src bssid snap_type*

  where

  - *bssid* is the Basic Service Set Identifier.
  - *snap_type* is the Ethernet type.

- **debug packet logging acl lwapp-ip** *rule_index action src dst proto src_port dst_port*

Note To remove all configured ACLs, enter this command: **debug packet logging acl clear-all**.

Step 2 To configure the format of the debug output, enter this command:

debug packet logging format {**hex2pcap** | **text2pcap**}

The debug facility supports two output formats: hex2pcap and text2pcap. The standard format used by IOS supports the use of hex2pcap and can be decoded using an HTML front end. The text2pcap option is provided as an alternative so that a sequence of packets can be decoded from the same console log file.

Figure 28: Sample Hex2pcap Output

This figure shows an example of hex2pcap output.

```
tx len=118, encap=n/a, port=1
[0000]: 000C316E 7F80000B 854008c0 08004500 ..1n.....@.@..E.
[0010]: 00680000 40004001 5FBE0164 6C0E0164 .h..@.@._>.dl..d
[0020]: 6C010800 08D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
rx len=118, encap=ip, port=1
[0000]: 000B8540 08C0000C 316E7F80 08004500 ...@.@..1n....E.
[0010]: 00680000 4000FF01 A0BD0164 6C010164 .h..@....=.dl..d
[0020]: 6C0E0000 10D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
```

212235

Figure 29: Sample Text2pcap Output

This figure shows an example of text2pcap output.

```
tx len=118, encap=n/a, port=1
0000 00 0C 31 6E 7F 80 00 0B 85 40 08 c0 08 00 45 00 ..1n.....@.@..E.
0010 00 68 00 00 40 00 40 01 5F BE 01 64 6C 0E 01 64 .h..@.@._>.dl..d
0020 6C 01 08 00 08 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..1n....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
```

232343

Step 3 To determine why packets might not be displayed, enter this command:

debug packet error {**enable** | **disable**}

Step 4 To display the status of packet debugging, enter this command:

show debug packet

Information similar to the following appears:

```
Status..................................... disabled
Number of packets to display..... 25
Bytes/packet to display..... 0
Packet display format..... text2pcap

Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
```

```
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
EoIP-IP ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
LWAPP-Dot11 ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
LWAPP-IP ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled?
```

Configuring Wireless Sniffing

Wireless Sniffing

The controller enables you to configure an access point as a network "sniffer," which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on. Sniffers allow you to monitor and record network activity and to detect problems.

This section contains the following subsections:

Prerequisites for Wireless Sniffing

To perform wireless sniffing, you need the following hardware and software:

- A dedicated access point—An access point configured as a sniffer cannot simultaneously provide wireless access service on the network. To avoid disrupting coverage, use an access point that is not part of your existing wireless network.
- A remote monitoring device—A computer capable of running the analyzer software.
- Software and supporting files, plug-ins, or adapters—Your analyzer software may require specialized files before you can successfully enable

Restrictions on Wireless Sniffing

- Supported third-party network analyzer software applications are as follows:
  - Wildpackets Omnipeek or Airopeek
  - AirMagnet Enterprise Analyzer
  - Wireshark
- The latest version of Wireshark can decode the packets by going to the Analyze mode. Select **decode as**, and switch UDP5555 to decode as PEEKREMOTE..
- You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a Cisco WLC. To disable IP-MAC address binding, enter the **config network ip-mac-binding disable** command in the controller CLI.
- You must enable WLAN 1 in order to use an access point in sniffer mode if the access point is joined to a Cisco WLC. If WLAN 1 is disabled, the access point cannot send packets.

Configuring Sniffing on an Access Point (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the **All APs** page.

Step 2 Click the name of the access point that you want to configure as the sniffer. The **All APs > Details** for page appears.

Step 3 From the **AP Mode** drop-down list, choose **Sniffer**.

Step 4 Click **Apply**.

Step 5 Click **OK** when prompted that the access point will be rebooted.

Step 6 Choose **Wireless > Access Points > Radios > 802.11a/n (or 802.11b/g/n)** to open the **802.11a/n/ac (or 802.11b/g/n) Radios** page.

Step 7 Hover your cursor over the blue drop-down arrow for the desired access point and choose **Configure**. The **802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure** page appears.

Step 8 Select the **Sniff** check box to enable sniffing on this access point, or leave it unselected to disable sniffing. The default value is unchecked.

Step 9 If you enabled sniffing in Step 8, follow these steps:

a) From the Channel drop-down list, choose the channel on which the access point sniffs for packets.

b) In the **Server IP Address** text box, enter the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark.

Step 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Configuring Sniffing on an Access Point (CLI)

Step 1 Configure the access point as a sniffer by entering this command:

config ap mode sniffer *Cisco_AP*

where *Cisco_AP* is the access point configured as the sniffer.

Step 2 When warned that the access point will be rebooted and asked if you want to continue, enter **Y**. The access point reboots in sniffer mode.

Step 3 Enable sniffing on the access point by entering this command:

config ap sniff {802.11a | 802.11b} enable *channel server_IP_address Cisco_AP*

where

- *channel* is the radio channel on which the access point sniffs for packets. The default values are 36 (802.11a/n/ac) and 1 (802.11b/g/n).
- *server_IP_address* is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark.
- *Cisco_AP* is the access point configured as the sniffer.

Note To disable sniffing on the access point, enter the **config ap sniff** {**802.11a | 802.11b**} **disable** *Cisco_AP* command.

Step 4 Save your changes by entering this command:

save config

Step 5 See the sniffer configuration settings for an access point by entering this command:

show ap config {**802.11a | 802.11b**} *Cisco_AP*

Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- The **upgrade** command cannot be used when a Telnet or SSH session is enabled.

Information About Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- To avoid potential conflicts and security threats to the network, the following commands are unavailable while a Telnet or SSH session is enabled: **config terminal, telnet, ssh, rsh, ping, traceroute, clear, clock, crypto, delete, fsck, lwapp, mkdir, radius, release, reload, rename, renew, rmdir, save, set, test, upgrade**.
- Commands available during a Telnet or SSH session include **debug, disable, enable, help, led, login, logout, more, no debug, show, systat, undebug** and **where**.

Note For instructions on configuring Telnet or SSH sessions on the controller, see the "Telnet and Secure Shell Sessions" section.

You can configure Telnet or SSH by using the controller CLI in software release 5.0 or later releases or using the controller GUI in software release 6.0 or later releases.

Troubleshooting Access Points Using Telnet or SSH (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the **All APs** page.

Step 2 Click the name of the access point for which you want to enable Telnet or SSH.

Step 3 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 4 Select the **Telnet** check box to enable Telnet connectivity on this access point. The default value is unchecked.

Step 5 Select the **SSH** check box to enable SSH connectivity on this access point. The default value is unchecked.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Troubleshooting Access Points Using Telnet or SSH (CLI)

Step 1 Enable Telnet or SSH connectivity on an access point by entering this command:

config ap {**telnet** | **ssh**} **enable** *Cisco_AP*

The default value is disabled.

Note Disable Telnet or SSH connectivity on an access point by entering this command: **config ap** {**telnet** | **ssh**} **disable** *Cisco_AP*

Step 2 Save your changes by entering this command:

save config

Step 3 See whether Telnet or SSH is enabled on an access point by entering this command:

show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 5
Cisco AP Name.................................... AP33
Country code..................................... Multiple Countries:US,AE,AR,AT,AU,BH
Reg. Domain allowed by Country................... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 2
MAC Address...................................... 00:19:2f:11:16:7a
IP Address Configuration......................... Static IP assigned
```

```
IP Address..................................... 10.22.8.133
IP NetMask..................................... 255.255.248.0
Gateway IP Addr................................ 10.22.8.1
Domain.....................................
Name Server.....................................
Telnet State................................... Enabled
Ssh State...................................... Enabled
...
```

Debugging the Access Point Monitor Service

Debugging the Access Point Monitor Service

The controller sends access point status information to the Cisco 3300 Series Mobility Services Engine (MSE) using the access point monitor service.

The MSE sends a service subscription and an access point monitor service request to get the status of all access points currently known to the controller. When any change is made in the status of an access point, a notification is sent to the MSE.

This section contains the following subsection:

Debugging Access Point Monitor Service Issues (CLI)

If you experience any problems with the access point monitor service, enter this command:

debug service ap-monitor {all | error | event | nmsp | packet} {enable | disable}

where

- **all** configures debugging of all access point status messages.
- **error** configures debugging of access point monitor error events.
- **event** configures debugging of access point monitor events.
- **nmsp** configures debugging of access point monitor NMSP events.
- **packet** configures debugging of access point monitor packets.
- **enable** enables the debub service ap-monitor mode.
- **disable** disables the debug service ap-monitor mode.

Troubleshooting Memory Leaks

Troubleshooting Memory Leaks

To investigate the cause for low memory state, follow these steps:

Step 1 **show memory statistics**

Step 2 **test system cat** */proc/meminfo*

Step 3 **show system top**

```
PID
1078 root      18   0  4488  888  756 S    0  0.1   0:00.00 gettyOrMwar
1081 root      20   0  980m 557m  24m S    0 56.9  41:33.32 switchdrvr
```

In this example, the PID to focus on is 1081.

Step 4 **test system cat** */proc/1081/smaps*

Step 5 **show system timers ticks-exhausted**

```
Timer Ticks ..................................... 3895180 ticks   (779036 seconds)
```

Here focus on the seconds value 779036.

Step 6 **show memory allocations [all/<pid>] [all/<pool-size>] [<start_time>] [<end_time>]**

If you see any allocations, they are probable memory leak candidates. You need to check if these are valid allocations made earlier to the low memory state issue.

Troubleshooting OfficeExtend Access Points

Troubleshooting OfficeExtend Access Points

This section provides troubleshooting information if you experience any problems with your OfficeExtend access points.

For information about troubleshooting Cisco 600 Series OfficeExtend APs, see http://www.cisco.com/c/en/us/support/docs/wireless/aironet-600-series-officeextend-access-point/113003-office-extend-config-00.html#troubleshoot.

This section contains the following subsections:

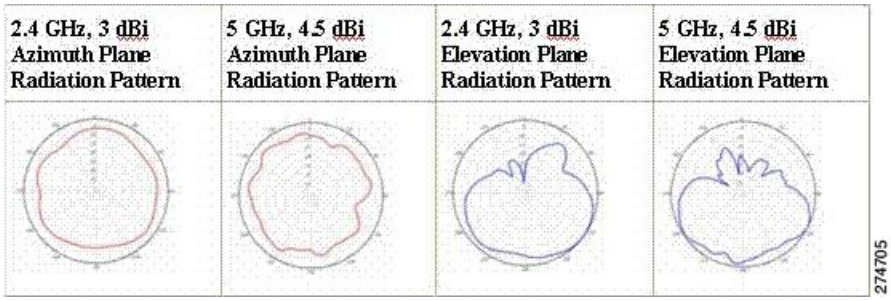
Interpreting OfficeExtend LEDs

The LED patterns are different for 1130 series and 1140 series OfficeExtend access points. For a description of the LED patterns, see the *Cisco OfficeExtend Access Point Quick Start Guide* at http://www.cisco.com/c/en/us/products/wireless/index.html.

Positioning OfficeExtend Access Points for Optimal RF Coverage

When positioning your OfficeExtend access point, consider that its RF signals are emitted in a cone shape spreading outward from the LED side of the access point. Ensure to mount the access point so that air can flow behind the metal back plate and prevent the access point from overheating.

Figure 30: OfficeExtend Access Point Radiation Patterns



Troubleshooting Common Problems

Most of the problems experienced with OfficeExtend access points are one of the following:

- The access point cannot join the controller because of network or firewall issues.

  Resolution: Follow the instructions in the Viewing Access Point Join Information section to see join statistics for the OfficeExtend access point, or find the access point's public IP address and perform pings of different packet sizes from inside the company.

- The access point joins but keeps dropping off. This behavior usually occurs because of network problems or when the network address translation (NAT) or firewall ports close because of short timeouts.

  Resolution: Ask the teleworker for the LED status.

- Clients cannot associate because of NAT issues.

  Resolution: Ask the teleworker to perform a speed test and a ping test. Some servers do not return big packet pings.

- Clients keep dropping data. This behavior usually occurs because the home router closes the port because of short timeouts.

  Resolution: Perform client troubleshooting in Cisco Prime Infrastructure to determine if the problem is related to the OfficeExtend access point or the client.

- The access point is not broadcasting the enterprise WLAN.

  Resolution: Ask the teleworker to check the cables, power supply, and LED status. If you still cannot identify the problem, ask the teleworker to try the following:

  - Connect to the home router directly and see if the PC is able to connect to an Internet website such as https://www.cisco.com/. If the PC cannot connect to the Internet, check the router or modem. If the PC can connect to the Internet, check the home router configuration to see if a firewall or MAC-based filter is enabled that is blocking the access point from reaching the Internet.
  - Log on to the home router and check to see if the access point has obtained an IP address. If it has, the access point's LED normally blinks orange.

- The access point cannot join the controller, and you cannot identify the problem.

  Resolution: A problem could exist with the home router. Ask the teleworker to check the router manual and try the following:

  - Assign the access point a static IP address based on the access point's MAC address.

- Put the access point in a demilitarized zone (DMZ), which is a small network inserted as a neutral zone between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.
- If problems still occur, contact your company's IT department for assistance.

- The teleworker experiences problems while configuring a personal SSID on the access point.

  Resolution: Clear the access point configuration and return it to factory default settings by clicking **Clear Config** on the access point GUI or by entering the **clear ap config Cisco_AP** command and then configuring a personal SSID on an OfficeExtend Access Point. If problems still occur, contact your company's IT department for assistance.

- The home network needs to be rebooted.

  Resolution: Ask the teleworker to follow these steps:

  Leave all devices networked and connected, and then power down all the devices.

  Turn on the cable or DSL modem, and then wait for 2 minutes. (Check the LED status.)

  Turn on the home router, and then wait for 2 minutes. (Check the LED status.)

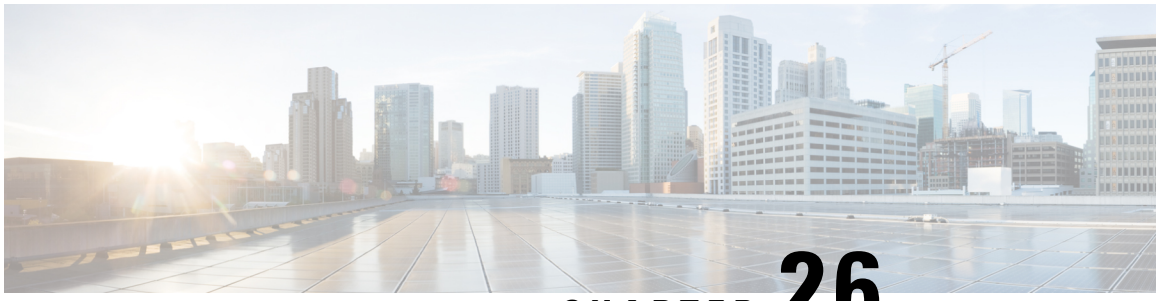
  Turn on the access point, and then wait for 5 minutes. (Check the LED status.)

  Turn on the client.

PART II

Ports and Interfaces

- Overview of Ports and Interfaces, on page 297
- Configuring the Management Interface, on page 305
- Configuring the AP-Manager Interface, on page 311
- Configuring Virtual Interfaces, on page 317
- Configuring Service-Port Interfaces, on page 319
- Configuring Dynamic Interfaces, on page 323
- Configuring Ports, on page 329
- Information About Using Cisco 5500 Series Controller USB Console Port, on page 331
- Configuring Link Aggregation, on page 333
- Configuring Multiple AP-Manager Interfaces, on page 339
- Configuring VLAN Select, on page 343
- Configuring Multicast Optimization, on page 349



CHAPTER 26

Overview of Ports and Interfaces

Three concepts are key to understanding how controllers connect to a wireless network: ports, interfaces, and WLANs.

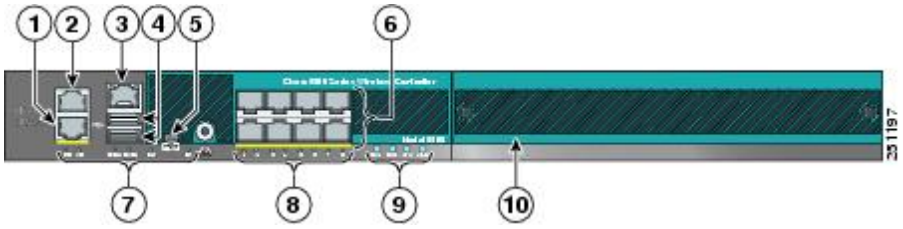
- Ports, on page 297
- Distribution System Ports, on page 298
- Interfaces, on page 300
- Dynamic AP Management, on page 301
- WLANs, on page 301

Ports

A port is a physical entity that is used for connections on the controller platform. controllers have two types of ports:

- Distribution system ports
- Service port

Figure 31: Ports on the Cisco 5508 Wireless Controllers



1	Redundant port (RJ-45)	6	SFP distribution system ports 1–8
2	Service port (RJ-45)	7	Management port LEDs
3	Console port (RJ-45)	8	SFP distribution port Link and Activity LEDs

4	USB ports 0 and 1 (Type A)	9	Power supply (PS1 and PS2), System (SYS), and Alarm (ALM) LEDs
5	Console port (Mini USB Type B) **Note** You can use only one console port (either RJ-45 or mini USB). When you connect to one console port, the other is disabled.	10	Expansion module slot

For more information about Cisco Unified Wireless Network Protocol and Port Matrix, see http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113344-cuwn-ppm.html.

Note For a comparison of ports in different controllers, see https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html.

This section contains the following subsections:

Distribution System Ports

A distribution system port connects the controller to a neighbor switch and serves as the data path between these two devices.

Restrictions for Configuring Distribution System Ports

- Each distribution system port is, by default, an 802.1Q VLAN trunk port. The VLAN trunking characteristics of the port are not configurable.

  Note Some controllers support link aggregation (LAG), which bundles all of the controller's distribution system ports into a single 802.3ad port channel. Cisco 5508 WLCs support LAG, and LAG is enabled automatically on the controllers within the Cisco WiSM2.

- Controller configuration in access mode is not supported. We recommend that you configure controllers in trunk mode when you configure controller ports on a switch.

- If an IPv6 packet is destined to controller management IPv6 address and the client VLAN is different from the controller management VLAN, then the IPv6 packet is switched out of the WLC box. If the same IPv6 packet comes as a network packet to the WLC, management access is not denied.

Service Port

The service port can be used management purposes, primarily for out-of-band management. However, AP management traffic is not possible across the service port. In most cases, the service port is used as a "last resort" means of accessing the controller GUI for management purposes. For example, in the case where the system distribution ports on the controller are down or their communication to the wired network is otherwise degraded.

The service port is controlled by the service-port interface and is reserved for out-of-band management of the controller and system recovery and maintenance in the event of a network failure. It is also the only port that is active when the controller is in boot mode. The service port is not capable of carrying 802.1Q tags, so it must be connected to an access port on the neighbor switch. Use of the service port is optional.

Service ports are not intended for high volume of traffic. We recommend that you use the management interface through the system distribution ports (dedicated or LAG).

Service ports can be used for SNMP polling in Release 8.2 or a later release.

Note The service port is not auto-sensing. You must use the correct straight-through or crossover Ethernet cable to communicate with the service port.

Caution Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller. We recommend that you place the service port in a VLAN or a subnet that is dedicated to out-of-band management.

Note For Cisco 5520 and 8540 Wireless Controllers, the disabling of administrative mode of the port does not physically disable the port. Only the packets are blocked due to which switchover does not happen.

For information about service ports in the applicable controllers, see the respecitve controller documentation:

- Cisco 3504 WLC Deployment Guide
- Cisco 5508 WLC Installation Guide
- Cisco WiSM2 Deployment Guide
- Cisco Flex 7510 WLC Deployment Guide
- Cisco 5520 WLC Deployment Guide
- Cisco 8510 WLC Installation Guide
- Cisco 8540 WLC Deployment Guide

Interfaces

An interface is a logical entity on the controller. An interface has multiple parameters associated with it, including an IP address, default gateway (for the IP subnet), primary physical port, secondary physical port, VLAN identifier, and DHCP server.

These five types of interfaces are available on the controller. Four of these are static and are configured at setup time:

Note A interface that is static means that at least one must exist in the controller and cannot be deleted. However, you can choose to modify the parameters for these interfaces after the initial setup.

- Management interface (static and configured at setup time; mandatory)
- AP-manager interface (static and configured at setup time; mandatory)

  Note You are not required to configure an AP-manager interface on Cisco 5508 and later controller models explicitly because this function can be enabled by default on the management interface itself.

- Virtual interface (static and configured at setup time; mandatory)
- Service-port interface (static and configured at setup time; optional)
- Dynamic interface (user-defined)

Note Typically, you define the management, AP-manager, virtual, and service-port interface parameters using the Startup Wizard. However, you can display and configure interface parameters through either the GUI or CLI after the controller is running.

When LAG is disabled, each interface is mapped to at least one primary port, and some interfaces (management and dynamic) can be mapped to an optional secondary (or backup) port. If the primary port for an interface fails, the interface automatically moves to the backup port. In addition, multiple interfaces can be mapped to a single controller port.

The Cisco 5508 and later controller models mark packets greater than 1500 bytes as long. However, the packets are not dropped. The workaround for this is to configure the MTU on a switch to less than 1500 bytes.

Note Interfaces that are quarantined are not displayed on the **Controller > Interfaces** page. For example, if there are 6 interfaces and one of them is quarantined, the quarantined interface is not displayed and the details of the other 5 interfaces are displayed on the GUI. You can get the total number of interfaces that is inclusive of quarantined interfaces through the count displayed on the top-right corner of the GUI.

This section contains the following subsections:

Restrictions on Configuring Interfaces

- Each physical port on the wireless controller can have only one AP-manager configured with it. For the Cisco 5508 controllers, the management interface with AP-management enabled cannot fail over to the backup port, which is primary for the AP-manager on the management or dynamic VLAN interface.
- Cisco 5508 controllers do not support fragmented pings on any interface.
- When the port comes up in VMware ESXi with configuration for NIC teaming, the vWLC may lose connectivity. However, the Cisco vWLC resumes connectivity after a while.
- IPv4 address needs to be configured on the interface prior to configuring the IPv6 address.

Dynamic AP Management

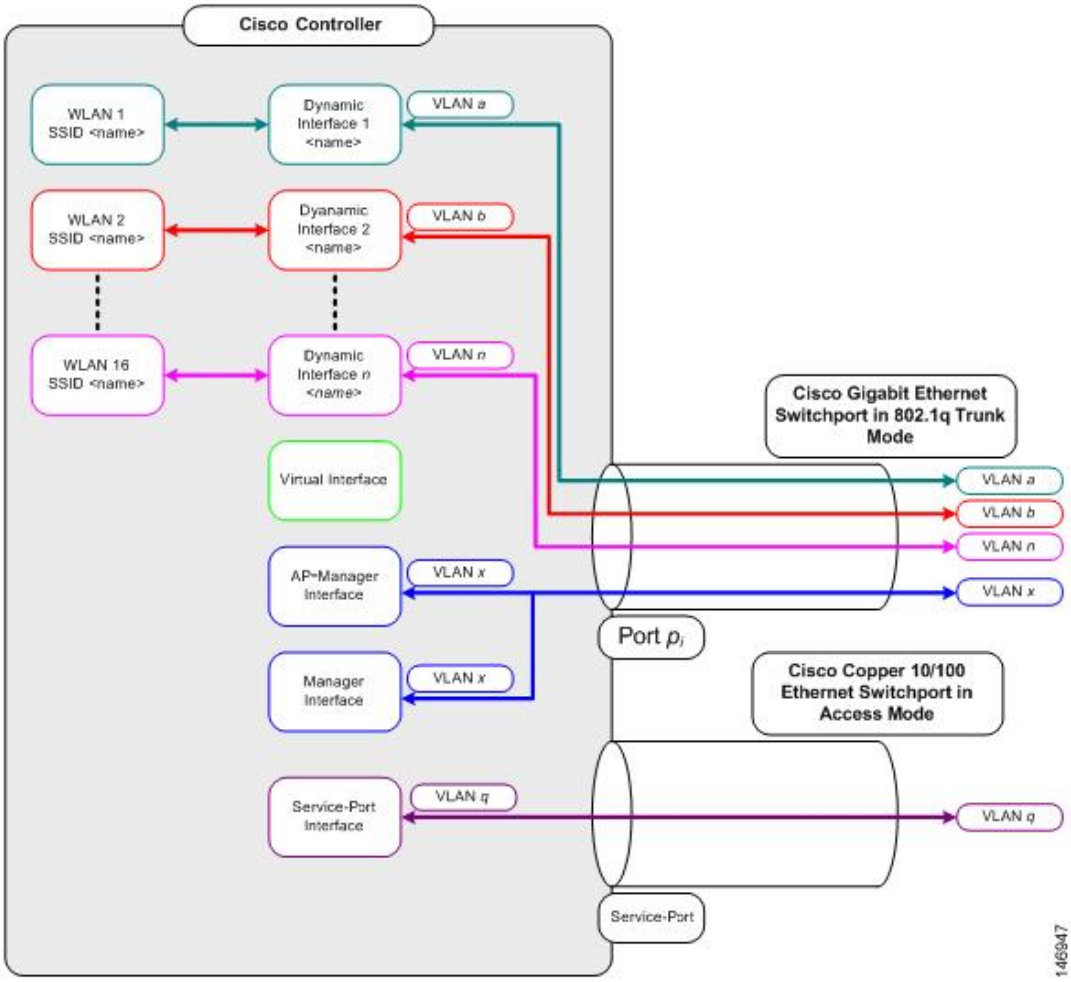
A dynamic interface is created as a WLAN interface by default. However, any dynamic interface can be configured as an AP-manager interface, with one AP-manager interface allowed per physical port. A dynamic interface with the Dynamic AP Management option enabled is used as the tunnel source for packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller.

Note If link aggregation (LAG) is enabled, there can be only one AP-manager interface.

WLANs

A WLAN associates a service set identifier (SSID) to an interface or an interface group. It is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. Up to 512 WLANs can be configured per controller.

Figure 32: Relationship between Ports, Interfaces, and WLANs



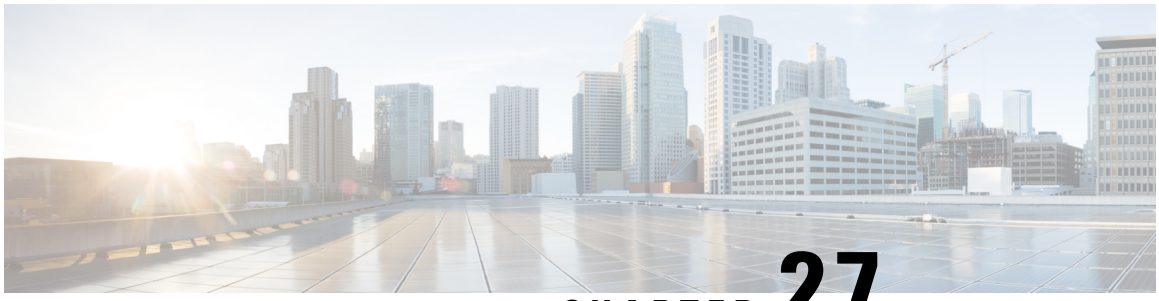
Each controller port connection is an 802.1Q trunk and should be configured as such on the neighbor switch. On Cisco switches, the native VLAN of an 802.1Q trunk is an untagged VLAN. If you configure an interface to use the native VLAN on a neighboring Cisco switch, make sure you configure the interface on the controller to be untagged.

Note A zero value for the VLAN identifier (on the **Controller > Interfaces** page) means that the interface is untagged.

The default (untagged) native VLAN on Cisco switches is VLAN 1. When controller interfaces are configured as tagged (meaning that the VLAN identifier is set to a nonzero value), the VLAN must be allowed on the 802.1Q trunk configuration on the neighbor switch and not be the native untagged VLAN.

We recommend that tagged VLANs be used on the controller. You should also allow only relevant VLANs on the neighbor switch's 802.1Q trunk connections to controller ports. All other VLANs should be disallowed or pruned in the switch port trunk configuration. This practice is extremely important for optimal performance of the controller.

Note We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.



CHAPTER 27

Configuring the Management Interface

- Management Interface, on page 305
- Configuring the Management Interface (GUI), on page 306
- Configuring the Management Interface (CLI), on page 307

Management Interface

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points, for all CAPWAP or intercontroller mobility messaging and tunneling traffic. You can access the GUI of the controller by entering the management interface IP address of the controller in the address field of your browser. The AP management is enabled by default on the management interface.

For CAPWAP, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.

Note To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator should ensure that only authorized clients gain access to the management network through proper CPU ACLs, or use a firewall between the client dynamic interface and the management network.

Caution Do not map a guest WLAN to the management interface. If the EoIP tunnel breaks, the client could obtain an IP and be placed on the management subnet.

In a High Availability environment with Release 8.0 or a later release, ensure that the management interface and the redundancy management interface (RMI) are tagged for the HA-SSO to work as expected.

This section contains the following subsections:

Configuring the Management Interface (GUI)

Step 1 Choose **Controller > Interfaces** to open the Interfaces page.

Step 2 Click the management link.

The **Interfaces > Edit** page appears.

Step 3 Set the management interface parameters:

Note The management interface uses the controller's factory-set distribution system MAC address.

- Quarantine and quarantine VLAN ID, if applicable
- NAT address (only Cisco 2504 and 5508 controllers are configured for dynamic AP management.)

  Note Check the **Enable NAT Address** check box and enter the external NAT IP address if you want to be able to deploy your Cisco 2504 and 5508 controllers behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

  Note If a Cisco 2504 or 5508 controller is configured with an external NAT IP address under the management interface, the APs in local mode cannot associate with the controller. The workaround is to either ensure that the management interface has a globally valid IP address or ensure that external NAT IP address is valid internally for the local APs.

  Note The NAT parameters are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. The NAT parameters do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

- VLAN identifier

  Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- Configuring Management Interface using IPv4— Fixed IP address, IP netmask, and default gateway.
  - Configuring Management Interface using IPv6—Fixed IPv6 address, prefix-length (interface subnet mask for IPv6) and the link local address of the IPv6 gateway router.

Note
- In a setup where IPv6 is used, we recommend the APs to be at least one hop away from the controller. As the IPv6 packets are always sent to the Gateway, if the AP and controller are in the same subnet, it increases the packet hops and impacts the performance.
- Once the primary IPv6 Address, prefix length, and primary IPv6 gateway are configured on the management interface, they cannot be changed back to default values (:: /128).
- In a setup where IPv6 CAPWAP is used, we recommend that the APs are at least 1 hop away from the controller because all IPv6 traffic is first forwarded to the gateway.
- A configuration backup must be carried out before configuring IPv6 in case the user wants to revert back to IPv4 only management interface.
- When more than 1300 IPv6 APs are in use, on a single Catalyst 6000 Switch, then assign APs on multiple VLANs.

- Dynamic AP management (for Cisco 2504 or 5508 controllers only)

  Note For Cisco 5508 controllers, the dynamic AP management parameter is enabled by default. If needed, this function can be disabled on the management interface and enabled for another dynamic interface.

- Physical port assignment (for all controllers except the Cisco 2504 or 5508 controllers)
- Primary and secondary DHCP servers
- Access control list (ACL) setting, if required

Step 4 Click **Save Configuration**.

Step 5 If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring the Management Interface (CLI)

Step 1 Enter the **show interface detailed management** command to view the current management interface settings.

Note The management interface uses the controller's factory-set distribution system MAC address.

Step 2 Enter the **config wlan disable** *wlan-number* command to disable each WLAN that uses the management interface for distribution system communication.

Step 3 Enter these commands to define the management interface:

a) **Using IPv4 Address**

- **config interface address management** *ip-addr ip-netmask gateway*
- **config interface quarantine vlan management** *vlan_id*

  Note Use the **config interface quarantine vlan management** *vlan_id* command to configure a quarantine VLAN on the management interface.

- **config interface vlan management** {*vlan-id* | *0*}

Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- **config interface ap-manager management** {**enable** | **disable**}

  Note Use the **config interface ap-manager management** {**enable** | **disable**} command to enable or disable dynamic AP management for the management interface. For Cisco 5508 controllers, the management interface acts like an AP-manager interface by default. If required, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

- **config interface port management** *primary-port* [*secondary-port*] (for all controllers except the 5508 controller)
- **config interface dhcp management** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- **config interface acl management** *access-control-list-name*

b) **Using IPv6 Address**

Note we recommend the APs to be at least one hop away from the controller. As the IPv6 packets are always sent to the Gateway, if the AP and controller are in same subnet, it increases the packet hops and impacts the performance.

- **config ipv6 interface address management** *primary ip-address prefix-length IPv6_Gateway_Address*

  Note Once the Primary IPv6 Address, Prefix Length, and Primary IPv6 Gateway are configured on the management interface, they cannot be changed back to default values (:: /128). A configuration backup must be carried out before configuring IPv6 in case the user wants to revert back to IPv4 only management interface.

- **config interface quarantine vlan management** *vlan_id*

  Note Use the **config interface quarantine vlan management** *vlan_id* command to configure a quarantine VLAN on the management interface.

- **config interface vlan management** {*vlan-id* | *0*}

  Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- **config interface ap-manager management** {**enable** | **disable**}

  Note Use the **config interface ap-manager management** {**enable** | **disable**} command to enable or disable dynamic AP management for the management interface. For Cisco 5508 WLCs, the management interface acts like an AP-manager interface by default. If desired, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

- **config interface port management** *physical-ds-port-number* (for all controllers except the 5508 WLC)
- **config interface dhcp management** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- **config ipv6 interface acl management** *access-control-list-name*

Step 4 Enter these commands if you want to be able to deploy your controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT):

- **config interface nat-address management** {**enable** | **disable**}
- **config interface nat-address management set** *public_IP_address*

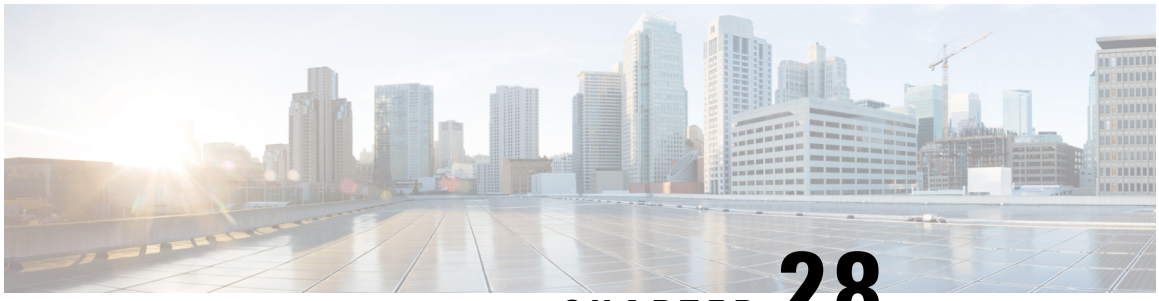
NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

Note These commands are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. These commands do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

Step 5 Enter the **save config** command.

Step 6 Enter the **show interface detailed management** command to verify that your changes have been saved.

Step 7 If you made any changes to the management interface, enter the **reset system** command to reboot the controller in order for the changes to take effect.



CHAPTER 28

Configuring the AP-Manager Interface

- AP-Manager Interface, on page 311
- Restrictions for Configuring AP Manager Interface, on page 311
- Configuring the AP-Manager Interface (GUI), on page 312
- Configuring the AP Manager Interface (CLI), on page 313
- Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller, on page 313

AP-Manager Interface

A controller configured with IPv4 has one or more AP-manager interfaces, which are used for all Layer 3 communications between the controller and lightweight access points after the access points have joined the controller. The AP-manager IP address is used as the tunnel source for CAPWAP packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller.

Note A controller configured with IPv6 has only one AP-manager and is applicable on management interface. You cannot remove the AP-manager configured on management interface.

Note The controller does not support jumbo frames. To avoid having the controller transmit CAPWAP packets to the AP that will necessitate fragmentation and reassembly, reduce MTU/MSS on the client side.

A controller configured with IPv6 does not support Dynamic AP-Manager. By default, the management interface acts like an AP-manager interface. Link Aggregation (LAG) is used for IPv6 AP load balancing.

This section contains the following subsections:

Restrictions for Configuring AP Manager Interface

- For IPv4—The MAC address of the management interface and the AP-manager interface is the same as the base LAG MAC address.
- An AP-manager interface is not required to be configured. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.

- If link aggregation (LAG) is enabled, there can be only one AP-manager interface. But when LAG is disabled, one or more AP-manager interfaces can be created, generally one per physical port.
  - When LAG is enabled—Supports only one AP Manager, which can either be on the management or dynamic interface with AP management.
  - When LAG is disabled—Supports one AP Manager per port. The Dynamic Interface tied to a VLAN can act as an AP Manager (when enabled).

Note When you enable LAG, all the ports would lose their AP Manager status and the AP management reverts back onto the Management interface.

- Port redundancy for the AP-manager interface is not supported. You cannot map the AP-manager interface to a backup port.
- It is not possible to have APs and a non-AP-manager interface on the same VLAN. If they are in the same VLAN, the controller will move the traffic up on the incorrect VLAN as the controller gets the CAPWAP discovery on the non-AP-manager interface.

Configuring the AP-Manager Interface (GUI)

Step 1 Choose **Controller > Interfaces** to open the **Interfaces** page.

Step 2 Click AP-Manager Interface.

The **Interface > Edit** page is displayed.

Note For IPv6 only—A controller configured with IPv6 address does not support Dynamic AP-Manager. By default, the management interface acts like an AP-manager interface.

Step 3 Set the AP-Manager Interface parameters:

Note For Cisco 5508 WLCs, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

- Physical port assignment
- VLAN identifier

Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the AP-manager interface.

Note The gig/wired subinterface is numbered with VLAN number and dot11 subinterface is numbered with the WLAN ID. The first configured WLAN becomes dot11 0.1 & dot11 1.1 and second WLAN ID subinterface becomes dot11 0.2 & dot11 1.2 onwards. This dot11 sub interface number cannot be mapped with a VLAN ID because multiple WLANs can be assigned with a same VLAN number. We cannot have duplicate subinterface created in the system. The native subinterface configuration in wired interface is the AP native VLAN configuration, if VLAN support is enabled in FlexConnect mode or else the native interface is always gig prime interface in AP (Local / Flex with no VLAN support).

- Fixed IP address, IP netmask, and default gateway

- Primary and secondary DHCP servers
- Access control list (ACL) name, if required

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

Step 5 If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring the AP Manager Interface (CLI)

Before you begin

For Cisco 5508 WLCs, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

A controller configured with IPv6 address does not support Dynamic AP-Manager. The management interface acts like an AP-manager interface by default.

Step 1 Enter the **show interface summary** command to view the current interfaces.

Step 2 Enter the **show interface detailed** *interface-name* command to view the current AP-manager interface settings.

Step 3 Enter the **config wlan disable** *wlan-id* command to disable each WLAN that uses the AP-manager interface for distribution system communication.

Step 4 Enter these commands to define the AP-manager interface:

- **config interface address management** *ip-addr ip-netmask gateway*
- **config interface vlan management** {*vlan-id* | *0*}

  Note Enter *0* for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the AP-manager interface.

- **config interface port management** *physical-ds-port-number*
- **config interface dhcp management** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- **config interface acl management** *access-control-list-name*

Step 5 Enter the **save config** command to save your changes.

Step 6 Enter the **show interface detailed** *interface-name* command to verify that your changes have been saved.

Configuration Example: Configuring AP-Manager on a Cisco 5500 Series Controller

For a Cisco 5508 WLC, we recommend that you have eight dynamic AP-manager interfaces and associate them to the eight Gigabit ports of the controller when LAG is not used. If you are using the management

interface, which acts like an AP-manager interface by default, you must create only seven more dynamic AP-manager interfaces and associate them to the remaining seven Gigabit ports.

Note For IPv6 only—A controller configured with IPv6 address does not support Dynamic AP-Manager. By default, the management interface acts like an AP-manager interface. Use LAG for IPv6 AP load balancing.

Figure 33: Dynamic Interface Example with Dynamic AP Management

This figure shows a dynamic interface that is enabled as a dynamic AP-manager interface and associated to port number 2.

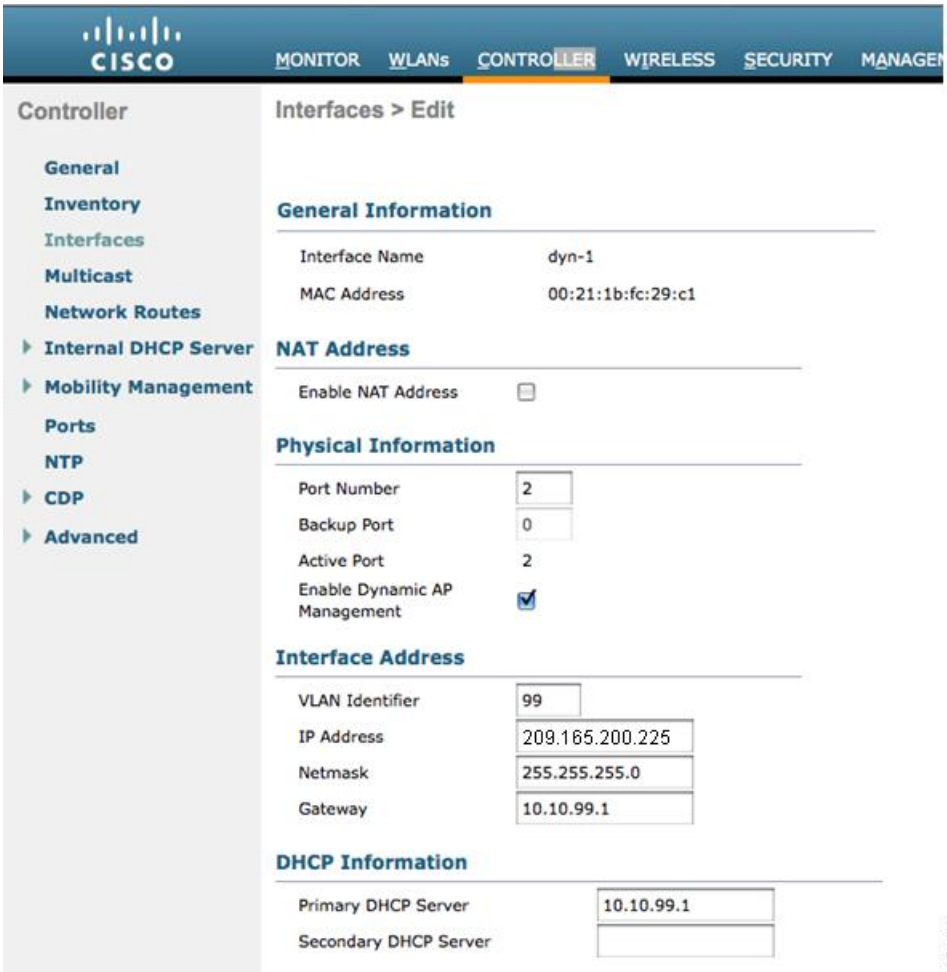
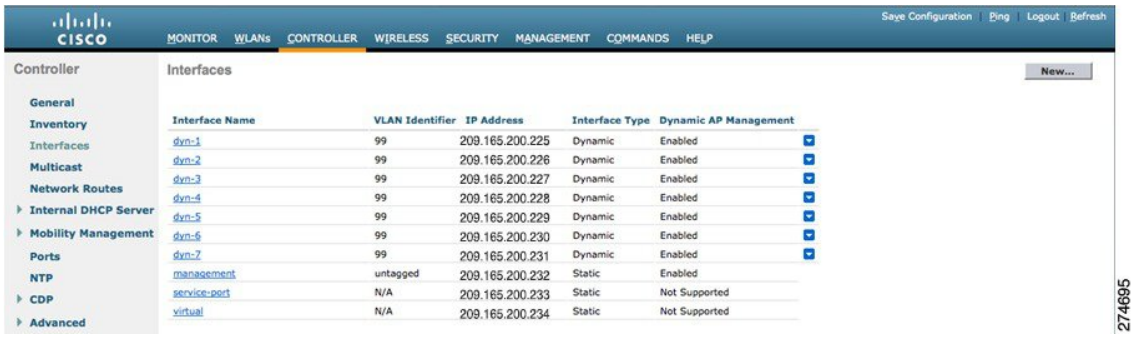
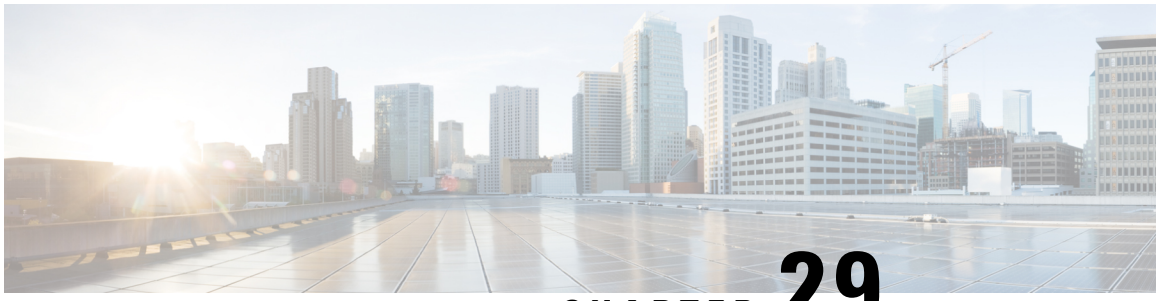


Figure 34: Cisco 5508 WLC Interface Configuration Example

This figure shows a Cisco 5508 WLC with LAG disabled, the management interface used as one dynamic AP-manager interface, and seven additional dynamic AP-manager interfaces, each mapped to a different Gigabit port.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Controller
General
Inventory
Interfaces
Multicast
Network Routes
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Advanced
Interfaces
New...
Interface Name VLAN Identifier IP Address Interface Type Dynamic AP Management
dyn-1 99 209.165.200.225 Dynamic Enabled
dyn-2 99 209.165.200.226 Dynamic Enabled
dyn-3 99 209.165.200.227 Dynamic Enabled
dyn-4 99 209.165.200.228 Dynamic Enabled
dyn-5 99 209.165.200.229 Dynamic Enabled
dyn-6 99 209.165.200.230 Dynamic Enabled
dyn-7 99 209.165.200.231 Dynamic Enabled
management untagged 209.165.200.232 Static Enabled
service-port N/A 209.165.200.233 Static Not Supported
virtual N/A 209.165.200.234 Static Not Supported
274695



CHAPTER 29

Configuring Virtual Interfaces

- Virtual Interface, on page 317
- Configuring Virtual Interfaces (GUI), on page 318
- Configuring Virtual Interfaces (CLI), on page 318

Virtual Interface

The virtual interface is used to support mobility management, Dynamic Host Configuration Protocol (DHCP) relay, and embedded Layer 3 security such as guest web authentication. It also maintains the DNS gateway host name used by Layer 3 security and mobility managers to verify the source of certificates when Layer 3 web authorization is enabled.

Specifically, the virtual interface plays these two primary roles:

- Acts as the DHCP server placeholder for wireless clients that obtain their IP address from a DHCP server.
- Serves as the redirect address for the web authentication login page.

The virtual interface IP address is used only in communications between the controller and wireless clients. It never appears as the source or destination address of a packet that goes out a distribution system port and onto the switched network. For the system to operate correctly, the virtual interface IP address must be set (it cannot be 0.0.0.0), and no other device on the network can have the same address as the virtual interface. Therefore, the virtual interface must be configured with an unassigned and unused gateway IP address. The virtual interface IP address is not pingable and should not exist in any routing table in your network. In addition, the virtual interface cannot be mapped to a physical port.

We recommend that you configure a non-routable IP address for the virtual interface, ideally not overlapping with the network infrastructure addresses or external. Use one of the options proposed on RFC5737, for example, 192.0.2.0/24, 198.51.100.0/24, and 203.0.113.0/24 networks. This is to avoid using an IP address that is assigned to another device or system.

Restrictions

- All controllers within a mobility group must be configured with the same virtual interface IP address. Otherwise, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time.

This section contains the following subsections:

Configuring Virtual Interfaces (GUI)

Step 1 Choose **Controller > Interfaces** to open the Interfaces page.

Step 2 Click **Virtual.**

The Interfaces > Edit page appears.

Step 3 Enter the following parameters:

- Any valid unassigned, and unused gateway IP address
- DNS gateway hostname

Note To ensure connectivity and web authentication, the DNS server should always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then the same DNS host name must be configured on the DNS server(s) used by the client.

Step 4 Click **Save Configuration**.

Step 5 If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring Virtual Interfaces (CLI)

Step 1 Enter the **show interface detailed virtual** command to view the current virtual interface settings.

Step 2 Enter the **config wlan disable wlan-number** command to disable each WLAN that uses the virtual interface for distribution system communication.

Step 3 Enter these commands to define the virtual interface:

- **config interface address virtual** *ip-address*

  Note For *ip-address*, enter a valid, unassigned, and unused gateway IP address.

- **config interface hostname virtual** *dns-host-name*

Step 4 Enter the **reset system** command. At the confirmation prompt, enter Y to save your configuration changes to NVRAM. The controller reboots.

Step 5 Enter the **show interface detailed virtual** command to verify that your changes have been saved.

CHAPTER 30

Configuring Service-Port Interfaces

- Service-Port Interfaces, on page 319
- Restrictions on Configuring Service-Port Interfaces, on page 320
- Configuring Service-Port Interfaces Using IPv4 (GUI), on page 320
- Configuring Service-Port Interfaces Using IPv4 (CLI), on page 320
- Configuring Service-Port Interface Using IPv6 (GUI), on page 321
- Configuring Service-Port Interfaces Using IPv6 (CLI), on page 322

Service-Port Interfaces

The service-port interface controls communications through and is statically mapped by the system to the service port. The service port can be used for out-of-band management.

The service port can obtain an IPv4 address using DHCP, or it can be assigned a static IPv4 address, but a default gateway cannot be assigned to the service-port interface. Static IPv4 routes can be defined through the controller for remote network access to the service port.

If the service port is in use, the management interface must be on a different supernet from the service-port interface.

Similarly, the service port can be statically assigned an IPv6 address or select an IPv6 address using Stateless Address Auto-Configuration (SLAAC). The default gateway cannot be assigned to the service-port interface. Static IPv6 routes can be defined through the controller for remote network access to the service port.

Note This is the only SLAAC interface on the controller, all other interfaces must be statically assigned (just like for IPv4).

Note User does not require IPv6 static routes to reach service port from the same network, but IPv6 routes requires to access service port from different network. The IPv6 static routes should be as same as IPv4.

The service-port interface supports the following protocols:

- SSH and Telnet
- HTTP and HTTPS

- SNMP
- FTP, TFTP, and SFTP
- Syslog
- ICMP (ping)
- NTP

Note TACACS+ and RADIUS are not supported through the service port.

This section contains the following subsections:

Restrictions on Configuring Service-Port Interfaces

- Only Cisco Flex 7510 and Cisco 5508 WLCs have a physical service-port interface that is reachable from the external network.
- You must not use the service-port for continuous SNMP polling and management functions except when the management interface of the controller is unreachable.

Configuring Service-Port Interfaces Using IPv4 (GUI)

Step 1 Choose **Controller** > **Interfaces** to open the Interfaces page.

Step 2 Click the service-port link to open the Interfaces > Edit page.

Step 3 Enter the Service-Port Interface parameters:

Note The service-port interface uses the controller's factory-set service-port MAC address.

- DHCP protocol (enabled)
- DHCP protocol (disabled) and IP address and IP netmask

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

Step 5 If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring Service-Port Interfaces Using IPv4 (CLI)

Step 1 To view the current service-port interface settings, enter this command:

show interface detailed service-port

Note The service-port interface uses the controller's factory-set service-port MAC address.

Step 2 Enter these commands to define the service-port interface:

- To configure the DHCP server, enter this command:

  config interface dhcp service-port enable

- To disable the DHCP server, enter this command:

  config interface dhcp service-port disable

- To configure the IPv4 address, enter this command:

  config interface address service-port *ip-addr ip-netmask*

The service port is used for out-of-band management of the controller. If the management workstation is in a remote subnet, you may need to add a IPv4 route on the controller in order to manage the controller from that remote workstation. To do so, enter this command:

config route add *network-ip-addr ip-netmask gateway*

To remove the IPv4 route on the controller, enter this command:

config route delete *ip_address*

Caution Communication through the management interface might not work as expected if subnet that is added to static route overlaps with other infrastructure or devices.

Step 3 Enter the **save config** command to save your changes.

Step 4 Enter the **show interface detailed service-port** command to verify that your changes have been saved.

Configuring Service-Port Interface Using IPv6 (GUI)

Step 1 Choose **Controller** > **Interfaces** to open the Interfaces page.

Step 2 Click the service-port link to open the Interfaces > Edit page.

Step 3 Enter the Service-Port Interface parameters:

Note The service-port interface uses the controller's factory-set service-port MAC address. Service Port can be statically assigned an address or select an address using SLAAC.

- SLACC(enabled)
- SLACC (disabled) and Primary Address and Prefix Length

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

Step 5 If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring Service-Port Interfaces Using IPv6 (CLI)

Step 1 To view the current service-port interface settings, enter this command:

show interface detailed service-port

Note The service-port interface uses the controller's factory-set service-port MAC address.

Step 2 Enter these commands to define the service-port interface:

- To configure the service port using SLACC , enter this command:

  config ipv6 interface slacc service-port enable

- To disable the service port from using SLACC, enter this command:

  config ipv6 interface slacc service-port disable

- To configure the IPv6 address, enter this command:

  config ipv6 interface address service-port *iipv6_address prefix-length*

Step 3 The service port is used for out-of-band management of the controller. If the management workstation is in a remote subnet, you may need to add a route on the controller in order to manage the controller from that remote workstation. To do so, enter this command:

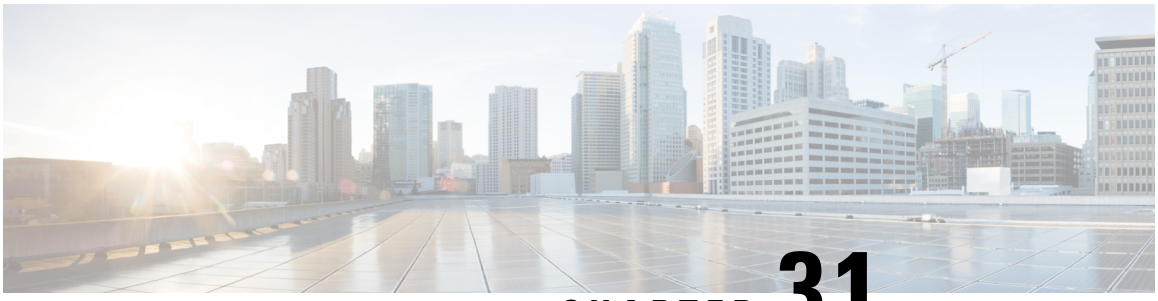
config ipv6 route add *network_ipv6_addr prefix-len ipv6_gw_addr*

Step 4 To remove the IPv6 route on the controller, enter this command:

config ipv6 route delete *network _ipv6 addr*

Step 5 Enter the **save config** command to save your changes.

Step 6 Enter the **show interface detailed service-port** command to verify that your changes have been saved.



CHAPTER 31

Configuring Dynamic Interfaces

- Dynamic Interface, on page 323
- Prerequisites for Configuring Dynamic Interfaces, on page 324
- Restrictions for Configuring Dynamic Interfaces, on page 324
- Configuring Dynamic Interfaces (GUI), on page 324
- Configuring Dynamic Interfaces (CLI), on page 325

Dynamic Interface

Dynamic interfaces are created by users and designed to be analogous to VLANs for wireless LAN clients. In a LAG setup, the dynamic interface on a controller is conceptually analogous to an SVI on a switch or router associated with a single VLAN and single subnet, although the controller does not have any routing capabilities. A controller can support up to 512 dynamic interfaces (VLANs). Each dynamic interface is individually configured and allows separate communication streams to exist on any or all of a controller's distribution system ports. A dynamic interface is a Layer 3 interface on the controller to map a WLAN to a particular VLAN and subnet. If DHCP relay is enabled on the controller, then the applicable dynamic interface is used as the relay address. The dynamic interface will also be the interface through which network communication to and from the controller will occur if the destination address is in the same subnet assigned to a dynamic interface. Alternatively, a dynamic interface can also be configured as an AP management interface as well, in place of the default management interface on a separate port in a non-LAG setup. You can assign dynamic interfaces to distribution system ports, WLANs, the Layer 2 management interface, and the Layer 3 AP-manager interface, and you can map the dynamic interface to a backup port.

Management traffic such as Telnet or SSH, HTTP or HTTPS, and so on, can use a dynamic interface as their destination address if management by dynamic interface option is enabled.

You can configure zero, one, or multiple dynamic interfaces on a distribution system port. However, all dynamic interfaces must be on a different VLAN or IP subnet from all other interfaces configured on the port. If the port is untagged, all dynamic interfaces must be on a different IP subnet from any other interface configured on the port.

For information about maximum number of VLANs supported on a controller platform, see the respective controller platform's datasheet.

Note You must not configure a dynamic interface in the same network as that of Local Mobility Anchor (LMA). If you do so, the GRE tunnel between the controller and LMA does not come up.

This section contains the following subsections:

Prerequisites for Configuring Dynamic Interfaces

While configuring on the dynamic interface of the controller, you must ensure the following:

- You must use tagged VLANs for dynamic interfaces.

Restrictions for Configuring Dynamic Interfaces

The following restrictions apply for configuring the dynamic interfaces on the controller:

- Wired clients cannot access management interface of the Cisco WLC 2500 series using the IP address of the AP Manager interface .
- For SNMP requests that come from a subnet that is configured as a dynamic interface, the controller responds but the response does not reach the device that initiated the conversation.
- If you are using DHCP proxy and/or a RADIUS source interface, ensure that the dynamic interface has a valid routable address. Duplicate or overlapping addresses across controller interfaces are not supported.
- You must not use **`ap-manager`** as the interface name while configuring dynamic interfaces as **`ap-manager`** is a reserved name.

Configuring Dynamic Interfaces (GUI)

Step 1 Choose **Controller > Interfaces** to open the Interfaces page.

Step 2 Perform one of the following:

- To create a new dynamic interface, click **New**. The **Interfaces > New page** appears. Go to *Step 3*.
- To modify the settings of an existing dynamic interface, click the name of the interface. The **Interfaces > Edit** page for that interface appears. Go to *Step 5*.
- To delete an existing dynamic interface, hover your cursor over the blue drop-down arrow for the desired interface and choose **Remove**.

Step 3 Enter an interface name and a VLAN ID.

Note You cannot enter **`ap-manager`** as the interface name while confiiguring a dynamic interface as **`ap-manager`** is a reserved name.

Step 4 Click **Apply** to commit your changes. The **Interfaces > Edit** page is displayed.

Step 5 Configure the following parameters:

- Guest LAN, if applicable
- Quarantine and quarantine VLAN ID, if applicable

Note Select the **Quarantine** check box if you want to configure this VLAN as unhealthy or you want to configure network access control (NAC) out-of-band integration. Doing so causes the data traffic of any client that is assigned to this VLAN to pass through the controller.

- Physical port assignment (for all controllers except the Cisco 5508 controller)
- NAT address (only for Cisco 5508 controllers configured for dynamic AP management)

  Note Check the **Enable NAT Address** check box and enter the external NAT IP address if you want to be able to deploy your controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

  The NAT parameters are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. The NAT parameters do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

- Dynamic AP management

  Note When you enable this feature, this dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

  Set the APs in a VLAN that is different than the dynamic interface configured on the controller. If the APs are in the same VLAN as the dynamic interface, the APs are not registered on the controller and the "LWAPP discovery rejected" and "Layer 3 discovery request not received on management VLAN" errors are logged on the controller.

- VLAN identifier
- Fixed IP address, IP netmask, and default gateway.

  Note Enter valid IP addresses in these fields.

- Primary and secondary DHCP servers
- Access control list (ACL) name, if required

  Note To ensure proper operation, you must set the Port Number and Primary DHCP Server parameters.

Step 6 Click **Save Configuration** to save your changes.

Step 7 Repeat this procedure for each dynamic interface that you want to create or edit.

Configuring Dynamic Interfaces (CLI)

Step 1 Enter the **show interface summary** command to view the current dynamic interfaces.

Step 2 View the details of a specific dynamic interface by entering this command:

show interface detailed *operator_defined_interface_name*.

Note Interface names that contain spaces must be enclosed in double quotes. For example: **config interface create** *"vlan 25"*

Step 3 Enter the **config wlan disable** *wlan_id* command to disable each WLAN that uses the dynamic interface for distribution system communication.

Step 4 Enter these commands to configure dynamic interfaces:

- **config interface create** *operator_defined_interface_name* {*vlan_id* | *x*}
- **config interface address interface** *ip_addr ip_netmask* [**gateway**]
- **config interface vlan** *operator_defined_interface_name* {*vlan_id* | *o*}
- **config interface port** *operator_defined_interface_name* physical_ds_port_number
- **config interface ap-manager** *operator_defined_interface_name* {**enable** | **disable**}

  Note Use the **config interface ap-manager operator_defined_interface_name** {**enable** | **disable}** command to enable or disable dynamic AP management. When you enable this feature, this dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface. You cannot use **ap-manager** as the **operator_defined_interface_name** while configuring a dynamic interface as **ap-manager** is a reserved name.

- **config interface dhcp** *operator_defined_interface_name ip_address_of_primary_dhcp_server* [*ip_address_of_secondary_dhcp_server*]
- **config interface quarantine vlan** *interface_name vlan_id*

  Note Use the **config interface quarantine vlan** *interface_name vlan_id* command to configure a quarantine VLAN on any interface.

- **config interface acl** *operator_defined_interface_name* access_control_list_name

Step 5 Enter these commands if you want to be able to deploy your controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT):

- **config interface nat-address dynamic-interface** *operator_defined_interface_name* {**enable** | **disable**}
- **config interface nat-address dynamic-interface** *operator_defined_interface_name* **set** *public_IP_address*

NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

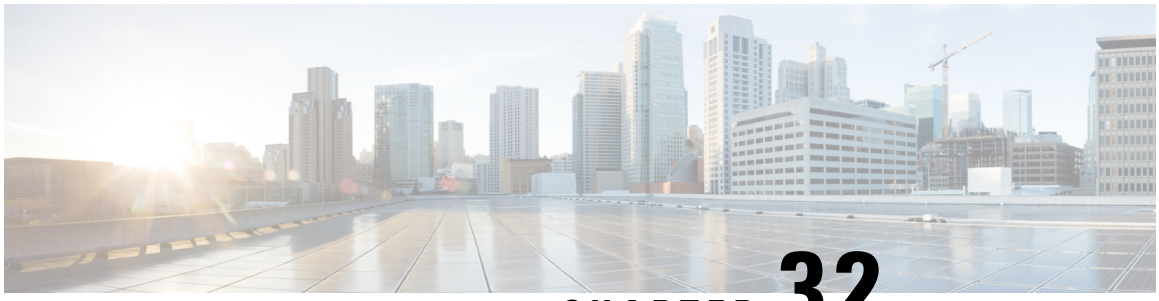
Note These commands are supported for use only with one-to-one-mapping NAT, whereby each private client has a direct and fixed mapping to a global address. These commands do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

Step 6 Enter the **config wlan enable** *wlan_id* command to reenable each WLAN that uses the dynamic interface for distribution system communication.

Step 7 Enter the **save config** command to save your changes.

Step 8 Enter the **show interface detailed** *operator_defined_interface_name* command and *show interface summary* command to verify that your changes have been saved.

Note If desired, you can enter the **config interface delete** *operator_defined_interface_name* command to delete a dynamic interface.



CHAPTER 32

Configuring Ports

• Configuring Ports (GUI), on page 329

Configuring Ports (GUI)

The controller's ports are configured with factory-default settings designed to make the controllers' ports operational without additional configuration. However, you can view the status of the controller's ports and edit their configuration parameters at any time.

Step 1 Choose **Controller** > **Ports** to open the Ports page.

This page shows the current configuration for each of the controller's ports.

If you want to change the settings of any port, click the number for that specific port. The **Port > Configure** page appears.

Note If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

Note The number of parameters available on the **Port > Configure** page depends on your controller type.

The following show the current status of the port:

- Port Number—Number of the current port.
- Admin Status—Current state of the port. Values: Enable or Disable
- Physical Mode—Configuration of the port physical interface. The mode varies by the controller type.
- Physical Status—The data rate being used by the port. The available data rates vary based on controller type.
  - Cisco 2504 WLC—1 Gbps full duplex
  - Cisco WiSM2—10 Gbps full duplex
  - Cisco 7510 WLC—10 Gbps full duplex
- Link Status—Link status of the port. Values: Link Up or Link Down
- Link Trap—Whether the port is set to send a trap when the link status changes. Values: Enable or Disable

- Power over Ethernet (PoE)—If the connecting device is equipped to receive power through the Ethernet cable and if so, provides –48 VDC. Values: Enable or Disable

  Note Some older Cisco access points do not draw PoE even if it is enabled on the controller port. In such cases, contact the Cisco Technical Assistance Center (TAC).

The following is a list of the port's configurable parameters.

a. **Admin Status**—Enables or disables the flow of traffic through the port. Options: Enable or Disable, with default option of Enable.

Note When a primary port link goes down, messages may get logged internally only and not be posted to a syslog server. It may take up to 40 seconds to restore logging to the syslog server.

b. **Physical Mode**—Determines whether the port's data rate is set automatically or specified by the user. The supported data rates vary based on the controller type. Default: Auto.

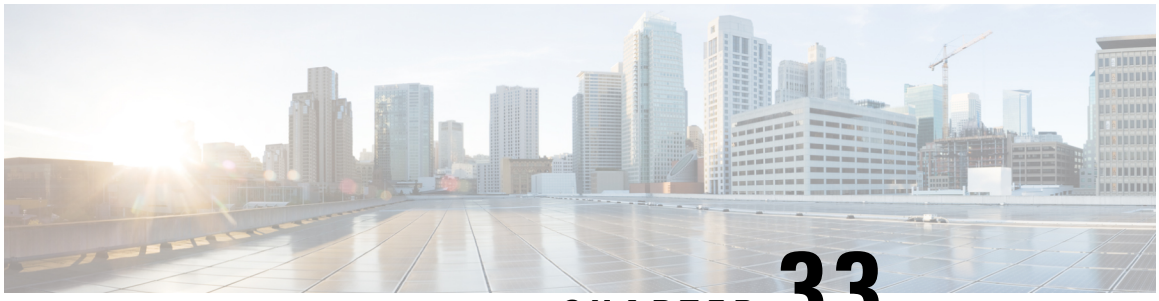
c. **Link Trap**—Causes the port to send a trap when the port's link status changes. Options: Enable or Disable, with default option of Enable.

Step 2 Click **Apply**.

Step 3 Click **Save Configuration**.

Step 4 Click **Back** to return to the Ports page and review your changes.

Step 5 Repeat this procedure for each additional port that you want to configure.



CHAPTER 33

Information About Using Cisco 5500 Series Controller USB Console Port

The USB console port on the Cisco 5500 Series Controllers connects directly to the USB connector of a PC using a USB Type A-to-5-pin mini Type B cable.

Note The 4-pin mini Type B connector is easily confused with the 5-pin mini Type B connector. They are not compatible. Only the 5-pin mini Type B connector can be used.

For operation with Microsoft Windows, the Cisco Windows USB console driver must be installed on any PC connected to the console port. With this driver, you can plug and unplug the USB cable into and from the console port without affecting Windows HyperTerminal operations.

Note Only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active.

- USB Console OS Compatibility, on page 331
- Changing the Cisco USB Systems Management Console COM Port to an Unused Port, on page 332

USB Console OS Compatibility

Before you begin

These operating systems are compatible with the USB console:

- Microsoft Windows 2000, Windows XP, Windows Vista, Windows 7 (Cisco Windows USB console driver required)
- Apple Mac OS X 10.5.2 (no driver required)
- Linux (no driver required)

Step 1 Download the USB_Console.inf driver file as follows:

a) Click this URL to go to the Software Center: http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243
b) Click **Wireless LAN Controllers**.
c) Click **Standalone Controllers**.
d) Click **Cisco 5500 Series Wireless LAN Controllers**.
e) Click **Cisco 5508 Wireless LAN Controller**.
f) Choose the USB driver file.
g) Save the file to your hard drive.

Step 2 Connect the Type A connector to a USB port on your PC.

Step 3 Connect the mini Type B connector to the USB console port on the controller.

Step 4 When prompted for a driver, browse to the USB_Console.inf file on your PC. Follow the prompts to install the USB driver.

Note Some systems might also require an additional system file. You can download the Usbser.sys file from Microsoft's Website.

Changing the Cisco USB Systems Management Console COM Port to an Unused Port

Before you begin

The USB driver is mapped to COM port 6. Some terminal emulation programs do not recognize a port higher than COM 4. If necessary, you must change the Cisco USB systems management console COM port to an unused port of COM 4 or lower.

Step 1 From your Windows desktop, right-click **My Computer** and choose **Manage**.

Step 2 From the list on the left side, choose **Device Manager**.

Step 3 From the device list on the right side, double-click **Ports (COM & LPT)**.

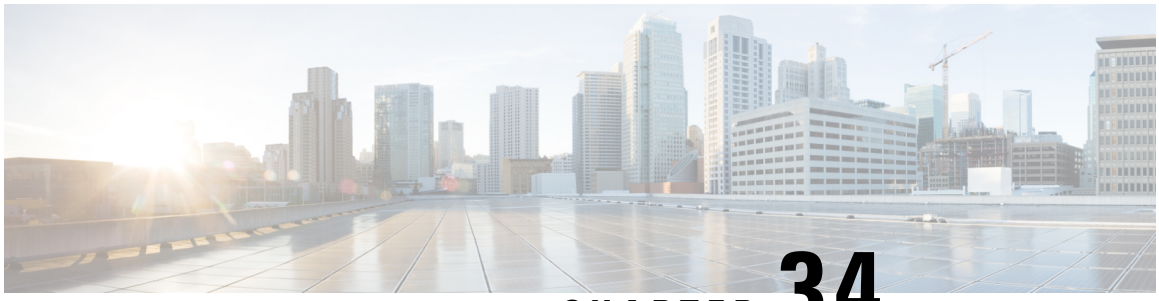
Step 4 Right-click **Cisco USB System Management Console 0108** and choose **Properties**.

Step 5 Click the **Port Settings** tab and click the **Advanced** button.

Step 6 From the COM Port Number drop-down list, choose an unused COM port of 4 or lower.

Step 7 Click **OK** to save and then close the Advanced Settings dialog box.

Step 8 Click **OK** to save and then close the Communications Port Properties dialog box.



CHAPTER 34

Configuring Link Aggregation

- Link Aggregation, on page 333
- Restrictions on Link Aggregation, on page 333
- Configuring Link Aggregation (GUI), on page 335
- Configuring Link Aggregation (CLI), on page 336
- Verifying Link Aggregation Settings (CLI), on page 336
- Configuring Neighbor Devices to Support Link Aggregation, on page 336
- Choosing Between Link Aggregation and Multiple AP-Manager Interfaces, on page 337

Link Aggregation

Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller's distribution system ports into a single 802.3ad port channel. This reduces the number of IP addresses required to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

LAG simplifies controller configuration because you no longer require to configure primary and secondary ports for each interface. If any of the controller ports fail, traffic is automatically migrated to one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

You can use fast restart for any LAG changes.

Controller does not send CDP advertisements on a LAG interface.

Note LAG is supported across switches.

This section contains the following subsections:

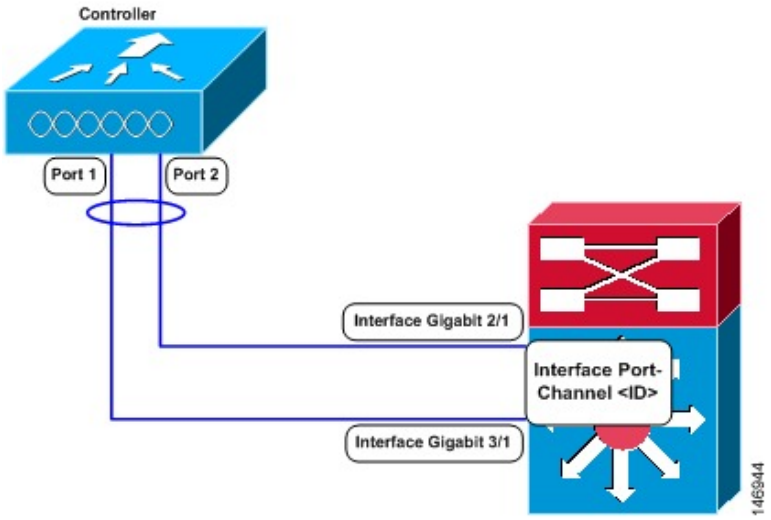
Restrictions on Link Aggregation

- You can bundle all eight ports on a Cisco 5508 Controller into a single link.
- Terminating on two different modules within a single Catalyst 6500 series switch provides redundancy and ensures that connectivity between the switch and the controller is maintained when one module fails.

The controller's port 1 is connected to Gigabit interface 3/1, and the controller's port 2 is connected to Gigabit interface 2/1 on the Catalyst 6500 series switch. Both switch ports are assigned to the same channel group.

- The controller relies on the switch for the load balancing decisions on traffic that come from the network, with "source-destination IP" as the typically recommended option. It is important to select a correct balancing configuration on the switch side, as some variations might have an impact on controller performance or cause packet drops on some scenarios, where traffic from different ports is split across different data planes internally.
- When using Link aggregation (LAG) make sure all ports of the controller have the same Layer 2 configuration on the switch side. For example, avoid filtering some VLANs in one port, and not the others.
- LAG requires the EtherChannel to be configured for 'mode on' on both the controller and the Catalyst switch.
- Once the EtherChannel is configured as on at both ends of the link, the Catalyst switch should not be configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP) but be set unconditionally to LAG. Because no channel negotiation is done between the controller and the switch, the controller does not answer to negotiation frames and the LAG is not formed if a dynamic form of LAG is set on the switch. Additionally, LACP and PAgP are not supported on the controller.
- If the recommended load-balancing method cannot be configured on the Catalyst switch, then configure the LAG connection as a single member link or disable LAG on the controller.

Figure 35: Link Aggregation with the Catalyst 6500 Series Neighbor Switch



- You cannot configure the controller's ports into separate LAG groups. Only one LAG group is supported per controller.
- When you enable LAG or make any changes to the LAG configuration, you must immediately reboot the controller.
- When you enable LAG, you can configure only one AP-manager interface because only one logical port is needed.

- When you enable LAG, all dynamic AP-manager interfaces and untagged interfaces are deleted, and all WLANs are disabled and mapped to the management interface. Also, the management, static AP-manager, and VLAN-tagged dynamic interfaces are moved to the LAG port.
- Multiple untagged interfaces to the same port are not allowed.
- When you enable LAG, all ports participate in LAG by default. You must configure LAG for all of the connected ports in the neighbor switch.
- When you enable LAG, if any single link goes down, traffic migrates to the other links.
- When you enable LAG, only one functional physical port is needed for the controller to pass client traffic.
- When you enable LAG, access points remain connected to the controller until you reboot the controller, which is needed to activate the LAG mode change, and data service for users continues uninterrupted.
- When you enable LAG, you eliminate the need to configure primary and secondary ports for each interface.
- When you enable LAG, the controller sends packets out on the same port on which it received them. If a CAPWAP packet from an access point enters the controller on physical port 1, the controller removes the CAPWAP wrapper, processes the packet, and forwards it to the network on physical port 1. This may not be the case if you disable LAG.
- When you disable LAG, the management, static AP-manager, and dynamic interfaces are moved to port 1.
- When you disable LAG, you must configure primary and secondary ports for all interfaces.
- When you enable LAG on Cisco 2504 WLC to which the direct-connect access point is associated, the direct connect access point is disconnected since LAG enabling is still in the transition state. You must reboot the controller immediately after enabling LAG.
- In Cisco 8510 WLCs, when more than 1000 APs join the controller, flapping occurs. To avoid this, we recommend that you do not add more than 1000 APs on a single Cisco Catalyst switch for CAPWAP IPv6.
- If you have configured a port-channel on the switch and you have not configured the AP for LAG, the AP moves to standalone mode.
- We recommend that you configure LAG with HA-SSO in disabled state. Therefore, you must enable LAG before placing the controllers in HA-SSO pair or schedule a maintenance window to break the HA-SSO (requires controller reboot) and then enable LG and re enable HA-SSO thereafter (incurs multiple controller reboots in the process).

Configuring Link Aggregation (GUI)

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

Step 2 Set the **LAG Mode on next reboot** parameter to **Enabled**.

Step 3 Save the configuration.

Step 4 Reboot the controller.

Configuring Link Aggregation (CLI)

Step 1 Enter the **config lag enable** command to enable LAG.

Note Enter the **config lag disable** command if you want to disable LAG.

Step 2 Enter the **save config** command to save your settings.

Step 3 Reboot controller.

Verifying Link Aggregation Settings (CLI)

Verify your LAG settings by entering this command:

show lag summary

Information similar to the following appears:

```
LAG Enabled
```

Configuring Neighbor Devices to Support Link Aggregation

The controller's neighbor devices must also be properly configured to support LAG.

- Each neighbor port to which the controller is connected should be configured as follows:

```
interface GigabitEthernet <interface id>
 switchport
 channel-group <id> mode on
 no shutdown
```

- The port channel on the neighbor switch should be configured as follows:

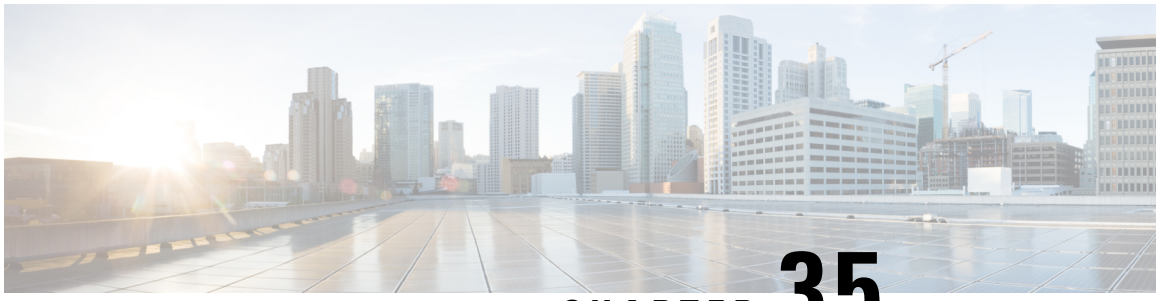
```
interface port-channel <id>
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan <native vlan id>
 switchport trunk allowed vlan <allowed vlans>
 switchport mode trunk
 no shutdown
```

Choosing Between Link Aggregation and Multiple AP-Manager Interfaces

controllers have no restrictions on the number of access points per port, but we recommend that you use link aggregation (LAG) or multiple AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load.

The following factors should help you decide which method to use if your controller is set for Layer 3 operation:

- With LAG, all of the controller ports need to connect to the same neighbor switch. If the neighbor switch goes down, the controller loses connectivity.
- With multiple AP-manager interfaces, you can connect your ports to different neighbor devices. If one of the neighbor switches goes down, the controller still has connectivity. However, using multiple AP-manager interfaces presents certain challenges when port redundancy is a concern.



CHAPTER 35

Configuring Multiple AP-Manager Interfaces

- Information About Multiple AP-Manager Interfaces, on page 339
- Restrictions on Configuring Multiple AP Manager Interfaces, on page 339
- Creating Multiple AP-Manager Interfaces (GUI), on page 340
- Creating Multiple AP-Manager Interfaces (CLI), on page 340

Information About Multiple AP-Manager Interfaces

When you create two or more AP-manager interfaces, each one is mapped to a different port. We recommend that you configure the ports in sequential order so that AP-manager interface 2 is on port 2, AP-manager interface 3 is on port 3, and AP-manager interface 4 is on port 4.

Before an access point joins a controller, it sends out a discovery request. From the discovery response that it receives, the access point can tell the number of AP-manager interfaces on the controller and the number of access points on each AP-manager interface. The access point generally joins the AP-manager with the least number of access points. In this way, the access point load is dynamically distributed across the multiple AP-manager interfaces.

Note Access points may not be distributed completely evenly across all of the AP-manager interfaces, but a certain level of load balancing occurs.

Multiple AP-Manager interfaces are also supported in non-LAG setups, only if you are not going to configure the controller for either LAG or IPv6.

Restrictions on Configuring Multiple AP Manager Interfaces

The following restrictions apply while configuring the multiple AP manager interfaces in the controller:

- You must assign an AP-manager interface to each port on the controller.
- Before implementing multiple AP-manager interfaces, you should consider how they would impact your controller's port redundancy.

- AP-manager interfaces do not need to be on the same VLAN or IP subnet, and they may or may not be on the same VLAN or IP subnet as the management interface. However, we recommend that you configure all AP-manager interfaces on the same VLAN or IP subnet.
- If the port of one of the AP-manager interfaces fails, the controller clears the state of the access points, and the access points must reboot to reestablish communication with the controller using the normal controller join process. The controller no longer includes the failed AP-manager interface in the CAPWAP or LWAPP discovery responses. The access points then rejoin the controller and are load balanced among the available AP-manager interfaces.

  In the case of management interface, because there is support for backup port, APs already connected to management interface continue to be in connected state (falling to backup port) rather than dropping off. However, AP-Mgr will get disabled any new APs will associate with the current AP-Mgr.

Creating Multiple AP-Manager Interfaces (GUI)

Step 1 Choose **Controller > Interfaces** to open the Interfaces page.

Step 2 Click **New**.

The Interfaces > New page appears.

Step 3 Enter an AP-manager interface name and a VLAN identifier.

Step 4 Click **Apply** to commit your changes. The Interfaces > Edit page appears.

Step 5 Enter the appropriate interface parameters.

Note Every interface supports primary and backup port with the following exceptions:

- Dynamic interface is converted to AP manager which does not support backup of port configuration.
- If AP manager is enabled on management interface and when management interface moves to backup port because of primary port failure, the AP manager will be disabled.

Step 6 To make this interface an AP-manager interface, check the **Enable Dynamic AP Management** check box.

Note Only one AP-manager interface is allowed per physical port. A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

Step 7 Click **Save Configuration** to save your settings.

Step 8 Repeat this procedure for each additional AP-manager interface that you want to create.

Creating Multiple AP-Manager Interfaces (CLI)

Step 1 Enter these commands to create a new interface:

- **config interface create** *operator_defined_interface_name* {*vlan_id* | *x*}

- **config interface address** *operator_defined_interface_name ip_addr ip_netmask* [*gateway*]
- **config interface vlan** *operator_defined_interface_name vlan_id*
- **config interface port** *operator_defined_interface_name physical_ds_port_number*
- **config interface dhcp** *operator_defined_interface_name ip_address_of_primary_dhcp_server* [*ip_address_of_secondary_dhcp_server*]
- (Optional) **config interface quarantine vlan** *interface_name vlan_id*

  Note Use this command to configure a quarantine VLAN on any interface.

- (Optional) **config interface acl** *operator_defined_interface_name access_control_list_name*

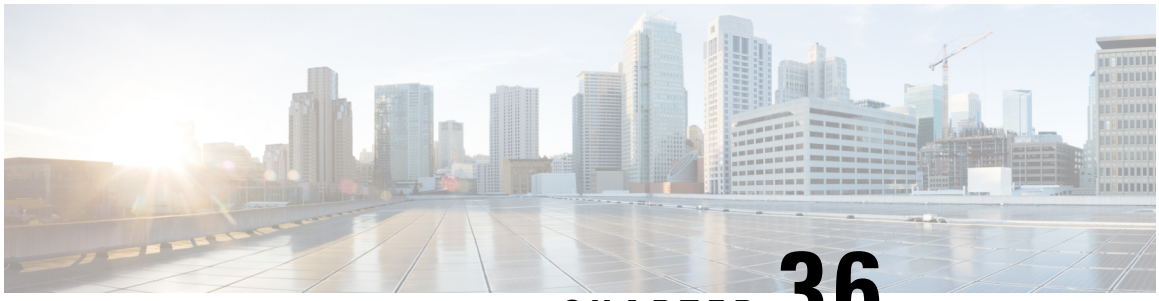
Step 2 To make this interface an AP-manager interface, enter this command:

{**config interface ap-manager** *operator_defined_interface_name* **enable | disable**}

Note Only one AP-manager interface is allowed per physical port. A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

Step 3 Enter **save config** command to save your changes.

Step 4 Repeat this procedure for each additional AP-manager interface that you want to create.



CHAPTER 36

Configuring VLAN Select

- Information About VLAN Select, on page 343
- Restrictions for Configuring VLAN Select, on page 344
- Configuring Interface Groups, on page 344

Information About VLAN Select

Whenever a wireless client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the WLAN. In a large venue such as an auditorium, a stadium, or a conference where there may be numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN select feature enables you to use a single WLAN that can support multiple VLANs. Clients can get assigned to one of the configured VLANs. This feature enables you to map a WLAN to a single or multiple interface VLANs using interface groups. Wireless clients that associate to the WLAN get an IP address from a pool of subnets identified by the interfaces. The IP address is derived by an algorithm based on the MAC address of the wireless client. This feature also extends the current AP group architecture where AP groups can override an interface or interface group to which the WLAN is mapped to, with multiple interfaces using the interface groups. This feature also provides the solution to auto anchor restrictions where a wireless guest user on a foreign location can get an IP address from multiple subnets based on their foreign locations or foreign controllers from the same anchor controller.

When a client roams from one controller to another, the foreign controller sends the VLAN information as part of the mobility announce message. Based on the VLAN information received, the anchor decides whether the tunnel should be created between the anchor controller and the foreign controller. If the same VLAN is available on the foreign controller, the client context is completely deleted from the anchor and the foreign controller becomes the new anchor controller for the client.

If an interface (int-1) in a subnet is untagged in one controller (Vlan ID 0) and the interface (int-2) in the same subnet is tagged to another controller (Vlan ID 1), then with the VLAN select, client joining the first controller over this interface may not undergo an L2 roam while it moves to the second controller. Hence, for L2 roaming to happen between two controllers with VLAN select, all the interfaces in the same subnet should be either tagged or untagged.

As part of the VLAN select feature, the mobility announce message carries an additional vendor payload that contains the list of VLAN interfaces in an interface group mapped to a foreign controller's WLAN. This VLAN list enables the anchor to differentiate from a local to local or local to foreign handoff.

Restrictions for Configuring VLAN Select

- The VLAN select feature enables you to use a single WLAN that can support multiple VLANs.

Configuring Interface Groups

Interface Groups

Interface groups are logical groups of interfaces. Interface groups facilitate user configuration where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface group can exclusively contain either quarantine or nonquarantine interfaces. An interface can be part of multiple interface groups.

A WLAN can be associated with an interface or interface group. The interface group name and the interface name cannot be the same.

This feature also enables you to associate a client to specific subnets based on the foreign controller that they are connected to. The anchor controller WLAN can be configured to maintain a mapping between foreign controller MAC and a specific interface or interface group (Foreign maps) as needed. If this mapping is not configured, clients on that foreign controller gets VLANs associated in a round robin fashion from interface group configured on WLAN.

You can also configure AAA override for interface groups. This feature extends the current access point group and AAA override architecture where access point groups and AAA override can be configured to override the interface group WLAN that the interface is mapped to. This is done with multiple interfaces using interface groups.

Controller marks VLAN as dirty when the clients are unable to receive IP address using DHCP. The VLAN interface is marked as dirty based on two methods:

Aggressive Method—When only one failure is counted per association per client and controller marks VLAN as dirty interface when a failure occurs three times for a client or for three different clients.

Non-Aggressive Method—When only one failure is counted per association per client and controller marks VLAN as a dirty interface only when three or more clients fail.

This section contains the following subsections:

Restrictions on Configuring Interface Groups

- The priority order for configuring interface groups for WLAN is:
  - AAA override
  - AP group
  - Interface group

Note AP group interface mapping for a WLAN is not supported in an anchor-foreign scenario.

- While you configure VLAN-ACL mapping using the native VLAN identifier as part of Flex group configuration, the ACL mapping does not take place. However, if you use the same VLAN to configure ACL mapping at the access point level, the configuration is allowed.
- Dual stack clients with a static-IPv4 address is not supported.

Creating Interface Groups (GUI)

Step 1 Choose **Controller** > **Interface Groups**.

The Interface Groups page appears with the list of interface groups already created.

Note To remove an interface group, hover your mouse pointer over the blue drop-down icon and choose **Remove**.

Step 2 Click **Add Group**.

The Add New Interface Group page appears.

Step 3 Enter the details of the interface group:

- **Interface Group Name**—Specify the name of the interface group.
- **Description**—Add a brief description of the interface group.

Step 4 Click **Add**.

Creating Interface Groups (CLI)

Step 1 **config interface group** {**create** | **delete**} *interface_group_name*—Creates or deletes an interface group

Step 2 **config interface group description** *interface_group_name description*—Adds a description to the interface group

Adding Interfaces to Interface Groups (GUI)

Step 1 Choose **Controller** > **Interface Groups**.

The **Interface Groups** page appears with a list of all interface groups.

Step 2 Click the name of the interface group to which you want to add interfaces.

The **Interface Groups > Edit** page appears.

Step 3 Choose the interface name that you want to add to this interface group from the **Interface Name** drop-down list.

Step 4 Click **Add Interface** to add the interface to the Interface group.

Step 5 Repeat Steps 2 and 3 if you want to add multiple interfaces to this interface group.

Note To remove an interface from the interface group, hover your mouse pointer over the blue drop-down arrow and choose **Remove**.

Adding Interfaces to Interface Groups (CLI)

Add interfaces to interface groups by entering this command:

config interface group interface add *interface_group interface_name*

Viewing VLANs in Interface Groups (CLI)

View a list of VLANs in the interface groups by entering this command:

show interface group detailed *interface-group-name*

Adding an Interface Group to a WLAN (GUI)

Step 1 Choose the **WLAN** tab.

The WLANs page appears listing the available WLANs.

Step 2 Click the WLAN ID of the WLAN to which you want to add the interface group.

Step 3 In the **General** tab, choose the interface group from the Interface/Interface Group (G) drop-down list.

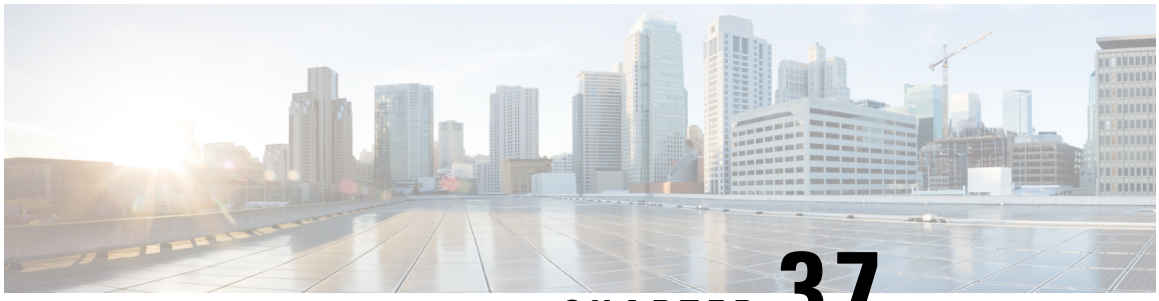
Step 4 Click **Apply**.

Note Suppose that the interface group that you add to a WLAN has RADIUS Server Overwrite interface enabled. In this case, when a client requests for authentication, the controller selects the first IP address from the interface group as the RADIUS server.

Adding an Interface Group to a WLAN (CLI)

Add an interface group to a WLAN by entering this command:

config wlan interface *wlan_id interface_group_name*



CHAPTER 37

Configuring Multicast Optimization

- Multicast Optimization, on page 349
- Configuring a Multicast VLAN (GUI), on page 349
- Configuring a Multicast VLAN (CLI), on page 350

Multicast Optimization

Prior to the 7.0.116.0 release, multicast was based on the grouping of the multicast address and the VLAN as one entity, MGID. With VLAN select and VLAN pooling, there is a possibility that you might increase duplicate packets. With the VLAN select feature, every client listens to the multicast stream on a different VLAN. As a result, the controller creates different MGIDs for each multicast address and VLAN. Therefore, the upstream router sends one copy for each VLAN, which results, in the worst case, in as many copies as there are VLANs in the pool. Since the WLAN is still the same for all clients, multiple copies of the multicast packet are sent over the air. To suppress the duplication of a multicast stream on the wireless medium and between the controller and access points, you can use the multicast optimization feature.

Multicast optimization enables you to create a multicast VLAN which you can use for multicast traffic. You can configure one of the VLANs of the WLAN as a multicast VLAN where multicast groups are registered. Clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using mulicast VLAN and multicast IP addresses. If multiple clients on the VLAN pool of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The controller makes sure that all multicast streams from the clients on this VLAN pool always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN pool. Only one multicast stream hits the VLAN pool even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the air is just one stream.

This section contains the following subsections:

Configuring a Multicast VLAN (GUI)

Step 1 Choose **WLANs** > **WLAN ID**. The WLAN > Edit page appears.

Step 2 In the **General** tab, select the **Multicast VLAN feature** check box to enable multicast VLAN for the WLAN.

The Multicast Interface drop-down list appears.

Step 3 Choose the VLAN from the Multicast Interface drop-down list.

Step 4 Click **Apply**.

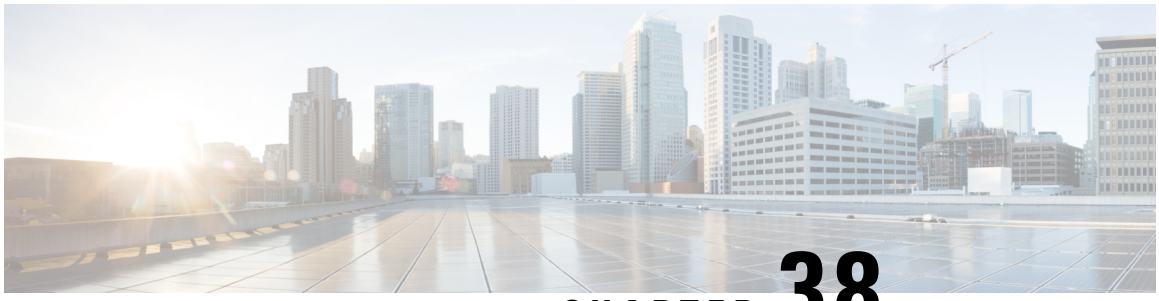
Configuring a Multicast VLAN (CLI)

Use the **config wlan multicast interface** *wlan_id* **enable** *interface_name* command to configure the multicast VLAN feature.

PART III

VideoStream

- VideoStream, on page 353



CHAPTER 38

VideoStream

- Information about Media Stream, on page 353
- Prerequisites for Media Stream, on page 353
- Restrictions for Configuring VideoStream, on page 353
- Configuring Media Stream (GUI), on page 354
- Configuring Media Stream (CLI), on page 357
- Viewing and Debugging Media Stream, on page 358

Information about Media Stream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. 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.

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

Prerequisites for Media Stream

- Make sure that the Multicast feature is enabled. We recommend that you configure IP multicast on the controller in 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 .
- Make sure that the clients are able to associate to the configured WLAN at 802.11n speed.

Restrictions for Configuring VideoStream

VideoStream is supported in the 7.0.98.0 and later controller software releases.

The Cisco OEAP-600 does not support VideoStream. All other access points support VideoStream.

Configuring Media Stream (GUI)

Step 1 Configure the multicast feature by following these steps:

a) Choose **Wireless** > **MediaStream** > **General**.

b) Select or unselect the **Multicast Direct feature** check box. The default value is disabled.

Note Enabling the multicast direct feature does not automatically reset the existing client state. The wireless clients must rejoin the multicast stream after enabling the multicast direct feature on the controller.

c) In the **Session Message Config** area, select **Session announcement State** check box to enable the session announcement mechanism. If the session announcement state is enabled, clients are informed each time a controller is not able to serve the multicast direct data to the client.

d) In the **Session announcement URL** text box, enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.

e) In the **Session announcement e-mail** text box, enter the e-mail address of the person who can be contacted.

f) In the **Session announcement Phone** text box, enter the phone number of the person who can be contacted.

g) In the **Session announcement Note** text box, enter a reason as to why a particular client cannot be served with a multicast media.

h) Click **Apply**.

Step 2 Add a media stream by following these steps:

a) Choose **Wireless** > **Media Stream** > **Streams** to open the Media Stream page.

b) Click **Add New** to configure a new media stream. The **Media Stream > New** page appears.

Note The Stream Name, Multicast Destination Start IP Address (IPv4 or IPv6), and Multicast Destination End IP Address (IPv4 or IPv6) text boxes are mandatory. You must enter information in these text boxes.

c) In the **Stream Name** text box, enter the media stream name. The stream name can be up to 64 characters.

d) In the **Multicast Destination Start IP Address (IPv4 or IPv6)** text box, enter the start (IPv4 or IPv6) address of the multicast media stream.

e) In the **Multicast Destination End IP Address (IPv4 or IPv6)** text box, enter the end (IPv4 or IPv6) address of the multicast media stream.

Note Ensure that the Multicast Destination Start and End IP addresses are of the same type, that is both addresses should be of either IPv4 or IPv6 type.

f) In the **Maximum Expected Bandwidth** text box, enter the maximum expected bandwidth that you want to assign to the media stream. The values can range between 1 to 35000 kbps.

Note We recommend that you use a template to add a media stream to the controller.

g) From the **Select from Predefined Templates** drop-down list under Resource Reservation Control (RRC) Parameters, choose one of the following options to specify the details about the resource reservation control:

- Very Coarse (below 300 kbps)
- Coarse (below 500 kbps)
- Ordinary (below 750 kbps)

- Low (below 1 Mbps)
- Medium (below 3 Mbps)
- High (below 5 Mbps)

Note When you select a predefined template from the drop-down list, the following text boxes under the Resource Reservation Control (RRC) Parameters list their default values that are assigned with the template.

- Average Packet Size (100-1500 bytes)—Specifies the average packet size. The value can be in the range of 100 to 1500 bytes. The default value is 1200.
- RRC Periodic update—Enables the RRC (Resource Reservation Control Check) Periodic update. By default, this option is enabled. RRC periodically updates the admission decision on the admitted stream according to the correct channel load. As a result, it may deny certain low priority admitted stream requests.
- RRC Priority (1-8)—Specifies the priority bit set in the media stream. The priority can be any number between 1 and 8. The larger the value means the higher the priority is. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
- Traffic Profile Violation—Specifies the action to perform in case of a violation after a re-RRC. Choose an action from the drop-down list. The possible values are as follows:

  Drop—Specifies that a stream is dropped on periodic revaluation.

  Fallback—Specifies that a stream is demoted to Best Effort class on periodic reevaluation.

  The default value is **drop**.

h) Click **Apply**.

Step 3 Enable the media stream for multicast-direct by following these steps:

a) Choose **WLANs** > WLAN ID to open the WLANs > Edit page.
b) Click the **QoS** tab and select Gold (Video) from the Quality of Service (QoS) drop-down list.
c) Click **Apply**.

Step 4 Set the EDCA parameters to voice and video optimized (optional) by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **EDCA Parameters**.
b) From the **EDCA Profile** drop-down list, choose the Voice and Video Optimized option.
c) Click **Apply**.

Step 5 Enable the admission control on a band for video (optional) by following these steps:

Note Keep the voice bandwidth allocation to a minimum for better performance.

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the **802.11a (5 GHZ) or 802.11b** > **Media** page.
b) Click the **Video** tab.
c) Select the **Admission Control (ACM)** check box to enable static CAC for this radio band. The default value is disabled.
d) Click **Apply**.

Step 6 Configure the video bandwidth by following these steps:

Note The template bandwidth that is configured for a media stream should be more than the bandwidth for the source media stream.

Note The voice configuration is optional. Keep the voice bandwidth allocation to a minimum for better performance.

a) Disable all WMM WLANs.
b) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the **802.11a (5 GHZ) or 802.11b** > **Media** page.
c) Click the **Video** tab.
d) Select the **Admission Control (ACM)** check box to enable the video CAC for this radio band. The default value is disabled.
e) In the Max RF Bandwidth field, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band.
f) The range is 5 to 85%.
g) The default value is 9%.
h) Click **Apply**.
i) Reenable all WMM WLANs and click **Apply**.

Step 7 Configure the media bandwidth by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media** to open the 802.11a (or 802.11b) > Media > Parameters page.
b) Click the **Media** tab to open the Media page.
c) Select the **Unicast Video Redirect** check box to enable Unicast Video Redirect. The default value is disabled.
d) In the **Maximum Media Bandwidth (0-85%)** text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches a specified value, the access point rejects new calls on this radio band.
e) The default value is 85%; valid values are from 0% to 85%.
f) In the **Client Minimum Phy Rate** text box, enter the minimum transmission data rate to the client. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
g) In the **Maximum Retry Percent (0-100%)** text box, enter the percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
h) Select the **Multicast Direct Enable** check box to enable the Multicast Direct Enable field. The default value is enabled.
i) From the **Max Streams per Radio** drop-down list, choose the maximum number of streams allowed per radio from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.
j) From the **Max Streams per Client** drop-down list, choose the maximum number of streams allowed per client from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.
k) Select the **Best Effort QoS Admission** check box to enable best-effort QoS admission.
l) Click **Apply**.

Step 8 Enable a WLAN by following these steps:

a) Choose **WLANs** > **WLAN ID**.

The **WLANs** > **Edit** page appears.

b) Select the **Status** check box.
c) Click **Apply**.

Step 9 Enable the 802.11 a/n/ac or 802.11 b/g/n network by following these steps:

a) Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network**.
b) Select the **802.11a** or **802.11b/g Network Status** check box to enable the network status.
c) Click **Apply**.

Step 10 Verify that the clients are associated with the multicast groups and group IDs by following these steps:

a) Choose **Monitor** > **Clients**.

The **Clients** page appears.

b) Check if the 802.11a/n/ac or 802.11b/g/n network clients have the associated access points.
c) Choose **Monitor > Multicast**. The Multicast Groups page appears.
d) Select the **MGID** check box for the Media Stream to the clients.
e) Click **MGID**. The Multicast Group Detail page appears. Check the Multicast Status details.

Configuring Media Stream (CLI)

Step 1 Configure the multicast-direct feature on WLANs media stream by entering this command:

config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

Step 2 Enable or disable the multicast feature by entering this command:

config media-stream multicast-direct {**enable** | **disable**}

Step 3 Configure various message configuration parameters by entering this command:

config media-stream message {**state** [**enable** | **disable**] | **url** *url* | **email** *email* | **phone** *phone _number* | **note** *note*}

Step 4 Save your changes by entering this command:

save config

Step 5 Configure various global media-stream configurations by entering this command:

config media-stream add multicast-direct stream-name *media_stream_name start_IP end_IP* [**template** {**very-coarse** | **coarse** | **ordinary** | **low-resolution** | **med-resolution** | **high-resolution**} | **detail** {**Max_bandwidth** *bandwidth* | **packet size** *packet_size* | **Re-evaluation** *re-evaluation* {*periodic* | *initial*}} **video** *video* **priority** {**drop** | **fallback**}

- The Resource Reservation Control (RRC) parameters are assigned with the predefined values based on the values assigned to the template.
- The following templates are used to assign RRC parameters to the media stream:
  - Very Coarse (below 3000 kbps)
  - Coarse (below 500 kbps)
  - Ordinary (below 750 kbps)
  - Low Resolution (below 1 mbps)
  - Medium Resolution (below 3 mbps)
  - High Resolution (below 5 mbps)

Step 6 Delete a media stream by entering this command:

config media-stream delete *media_stream_name*

Step 7 Enable a specific enhanced distributed channel access (EDC) profile by entering this command:

config advanced { **801.11a** | **802.11b**} **edca-parameters optimized-video-voice**

Step 8 Enable the admission control on the desired bandwidth by entering the following commands:

- Enable bandwidth-based voice CAC for 802.11a or 802.11b/g network by entering this command:

  config {**802.11a** | **802.11b**} **cac voice acm enable**

- Set the percentage of the maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network by entering this command:

  config {**802.11a** | **802.11b**} **cac voice max-bandwidth** *bandwidth*

- Configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the 802.11a or 802.11b/g network by entering this command:

  config {**802.11a** | **802.11b**} **cac voice roam-bandwidth** *bandwidth*

Note For TSpec and SIP based CAC for video calls, only Static method is supported.

Step 9 Set the maximum number of streams per radio and/or per client by entering these commands:

- Set the maximum limit to the number multicast streams per radio by entering this command:

  config {**802.11a** | **802.11b**} **media-stream multicast-direct radio-maximum** [*value* | **no-limit**]

- Set the maximum number of multicast streams per client by entering this command:

  config {**802.11a** | **802.11b**} **media-stream multicast-direct client-maximum** [*value* | **no-limit**]

Step 10 Save your changes by entering this command:

save config

Viewing and Debugging Media Stream

SUMMARY STEPS

1. See the configured media streams by entering this command:
2. See the details of the media stream name by entering this command:
3. See the clients for a media stream by entering this command:
4. See a summary of the media stream and client information by entering this command:
5. See details about a particular media stream group by entering this command:
6. See details of the 802.11a or 802.11b media resource reservation configuration by entering this command:
7. Enable debugging of the media stream history by entering this command:

DETAILED STEPS

Step 1 See the configured media streams by entering this command:

show wlan *wlan_id*

Step 2 See the details of the media stream name by entering this command:

show 802.11{a | b | h} media-stream *media-stream_name*

Step 3 See the clients for a media stream by entering this command:

show 802.11a media-stream client *media-stream-name*

Step 4 See a summary of the media stream and client information by entering this command:

show media-stream group summary

Step 5 See details about a particular media stream group by entering this command:

show media-stream group detail *media_stream_name*

Step 6 See details of the 802.11a or 802.11b media resource reservation configuration by entering this command:

show {802.11a | 802.11b} media-stream rrc

Step 7 Enable debugging of the media stream history by entering this command:

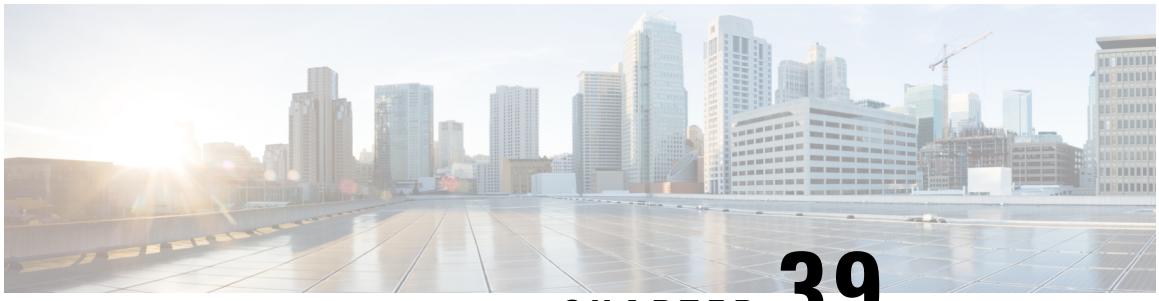
debug media-stream history {enable | disable}

PART IV

Security Solutions

- Cisco Unified Wireless Network Solution Security, on page 363
- Configuring RADIUS, on page 365
- Configuring TACACS+, on page 387
- Configuring Maximum Local Database Entries, on page 397
- Configuring Local Network Users on the Controller, on page 399
- Configuring Password Policies, on page 403
- Configuring LDAP, on page 407
- Configuring Local EAP, on page 413
- Configuring the System for SpectraLink NetLink Telephones, on page 423
- Configuring RADIUS NAC Support, on page 427
- Using Management Over Wireless, on page 431
- Using Dynamic Interfaces for Management, on page 433
- Configuring DHCP Option 82, on page 435
- Configuring and Applying Access Control Lists, on page 439
- Configuring Management Frame Protection, on page 449
- Configuring Client Exclusion Policies, on page 455
- Configuring Identity Networking, on page 459
- Configuring AAA Override, on page 465
- Managing Rogue Devices, on page 469
- Classifying Rogue Access Points, on page 481
- Configuring Cisco TrustSec SXP, on page 497
- Configuring Local Policies, on page 503
- Configuring Cisco Intrusion Detection System, on page 509
- Configuring IDS Signatures, on page 515

• Configuring wIPS, on page 523
• Configuring the Wi-Fi Direct Client Policy, on page 533
• Configuring Web Auth Proxy, on page 537
• Detecting Active Exploits, on page 541



CHAPTER 39

Cisco Unified Wireless Network Solution Security

- Security Overview, on page 363
- Layer 1 Solutions, on page 363
- Layer 2 Solutions, on page 363
- Layer 3 Solutions, on page 364
- Integrated Security Solutions, on page 364

Security Overview

The Cisco Unified Wireless Network (UWN) security solution bundles potentially complicated Layer 1, Layer 2, and Layer 3 802.11 Access Point security components into a simple policy manager that customizes system-wide security policies on a per-WLAN basis. The Cisco UWN security solution provides simple, unified, and systematic security management tools.

One of the biggest hurdles to WLAN deployment in the enterprise is WEP encryption, which is a weak standalone encryption method. A newer problem is the availability of low-cost access points, which can be connected to the enterprise network and used to mount man-in-the-middle and denial-of-service attacks.

Layer 1 Solutions

The Cisco UWN security solution ensures that all clients gain access within a user-set number of attempts. If a client fails to gain access within that limit, it is automatically excluded (blocked from access) until the user-set timer expires. The operating system can also disable SSID broadcasts on a per-WLAN basis.

Layer 2 Solutions

If a higher level of security and encryption is required, you can also implement industry-standard security solutions such as Extensible Authentication Protocol (EAP), Wi-Fi Protected Access (WPA), and WPA2. The Cisco UWN solution WPA implementation includes AES (Advanced Encryption Standard), TKIP and Michael (temporal key integrity protocol and message integrity code checksum) dynamic keys, or WEP (Wired Equivalent Privacy) static keys. Disabling is also used to automatically block Layer 2 access after a user-set number of failed authentication attempts.

Regardless of the wireless security solution selected, all Layer 2 wired communications between controllers and lightweight access points are secured by passing data through CAPWAP tunnels.

Restrictions for Layer 2 Solutions

Cisco Aironet client adapter version 4.2 does not authenticate if WPA/WPA2 is used with CCKM as auth key management and a 2 second latency between the controller and AP.

Layer 3 Solutions

The WEP problem can be further solved using industry-standard Layer 3 security solutions such as passthrough VPNs (virtual private networks).

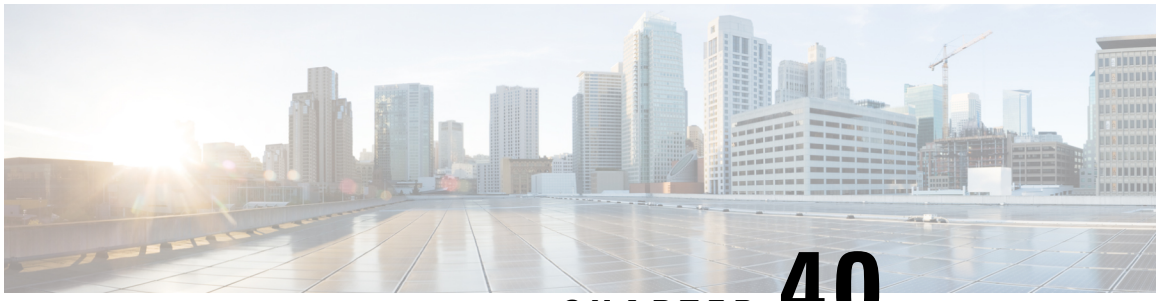
The Cisco UWN solution supports local and RADIUS MAC (media access control) filtering. This filtering is best suited to smaller client groups with a known list of 802.11 access card MAC addresses.

The Cisco UWN solution supports local and RADIUS user/password authentication. This authentication is best suited to small to medium client groups.

Integrated Security Solutions

The integrated security solutions are as follows:

- Cisco Unified Wireless Network (UWN) solution operating system security is built around a 802.1X AAA (authorization, authentication and accounting) engine, which allows users to rapidly configure and enforce a variety of security policies across the Cisco UWN solution.
- The controllers and lightweight access points are equipped with system-wide authentication and authorization protocols across all ports and interfaces, maximizing system security.
- Operating system security policies are assigned to individual WLANs, and lightweight access points simultaneously broadcast all (up to 16) configured WLANs, which can eliminate the need for additional access points, which can increase interference and degrade system throughput.
- Operating system security uses the RRM function to continually monitor the air space for interference and security breaches and to notify the user when they are detected.
- Operating system security works with industry-standard authorization, authentication, and accounting (AAA) servers.



CHAPTER 40

Configuring RADIUS

- Setting up RADIUS, on page 365
- Configuring RADIUS (GUI), on page 367
- Configuring RADIUS (CLI), on page 372
- RADIUS Authentication Attributes Sent by the Controller, on page 376
- Authentication Attributes Honored in Access-Accept Packets (Airespace), on page 378
- RADIUS Accounting Attributes, on page 384

Setting up RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol that provides centralized security for users attempting to gain management access to a network. It serves as a backend database similar to local and TACACS+ and provides authentication and accounting services:

- **Authentication**—The process of verifying users when they attempt to log into the controller.

  Users must enter a valid username and password in order for the controller to authenticate users to the RADIUS server. If multiple databases are configured, you can specify the sequence in which the backend database must be tired.

  Note Clients using Microsoft Windows 10 with default (zero-touch config) supplicant fail to connect to controller when there is no CA certificate to validate the server certificate. This is because the supplicant does not pop up a window to accept the server certificate and silently rejects the 802.1X authentication. Therefore, we recommend that you do either of the following:

  - Manually install a third-party CA certificate on the AAA server, which the clients using Microsoft Windows 10 can trust.
  - Use any other supplicant, such as Cisco AnyConnect, which pops up a window to trust or not trust the server certificate. If you accept the trust certificate, then the client is authenticated.

- **Accounting**—The process of recording user actions and changes.

Whenever a user successfully executes an action, the RADIUS accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided. If the RADIUS accounting server becomes unreachable, users are able to continue their sessions uninterrupted.

RADIUS uses User Datagram Protocol (UDP) for its transport. It maintains a database and listens on UDP port 1812 for incoming authentication requests and UDP port 1813 for incoming accounting requests. The controller, which requires access control, acts as the client and requests AAA services from the server. The traffic between the controller and the server is encrypted by an algorithm defined in the protocol and a shared secret key configured on both devices.

You can configure multiple RADIUS accounting and authentication servers. For example, you may want to have one central RADIUS authentication server but several RADIUS accounting servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one, then the third one if necessary, and so on.

When a management user is authenticated using a RADIUS server, only the PAP protocol is used. For web authentication users, PAP, MSCHAPv2 and MD5 security mechanisms are supported.

RADIUS Server Support

- You can configure up to 17 RADIUS authentication and accounting servers each.
- If multiple RADIUS servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.
- One Time Passwords (OTPs) are supported on the controller using RADIUS. In this configuration, the controller acts as a transparent passthrough device. The controller forwards all client requests to the RADIUS server without inspecting the client behavior. When using OTP, the client must establish a single connection to the controller to function properly. The controller currently does not have any intelligence or checks to correct a client that is trying to establish multiple connections.
- To create a read-only controller user on the RADIUS sever, you must set the service type to NAS prompt instead of Callback NAS prompt. If you set the service type to Callback NAS Prompt, the user authentication fails while setting it to NAS prompt gives the user read-only access to the controller.

  Also, the Callback Administrative service type gives the user the lobby ambassador privileges to the controller.
- If RADIUS servers are mapped per WLAN, then controller do not use RADIUS server from the global list on that WLAN.
- To configure the RADIUS server:
  - Using Access Control Server (ACS)—See the latest Cisco Secure Access Control System guide at https://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html.
  - Using Identity Services Engine (ISE)—See the Configuring External RADIUS Servers section in the Cisco Identity Services Engine Administrator Guide at https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html.

Primary and Fallback RADIUS Servers

The primary RADIUS server (the server with the lowest server index) is assumed to be the most preferable server for the controller. If the primary server becomes unresponsive, the controller switches to the next active backup server (the server with the next lowest server index). The controller continues to use this backup server, unless you configure the controller to fall back to the primary RADIUS server when it recovers and becomes responsive or to a more preferable server from the available backup servers.

Note **Functionality change introduced in Release 8.5.140.0**:

When RADIUS aggressive failover for controller is disabled: Packet is retried for six times unless there is a termination from clients. The RADIUS server (both AUTH and ACCT) is marked unreachable after three timeout events (18 consecutive retries) from multiple clients (previously, from exactly three clients).

When RADIUS aggressive failover for controller is enabled: Packet is retried for six times unless there is a termination from clients. The RADIUS server (both AUTH and ACCT) is marked unreachable after one timeout event (6 consecutive retries) from multiple clients (previously, from exactly one client).

It means 18 consecutive retries per RADIUS server (both AUTH and ACCT) can be from multiple clients. Therefore, it is not always guaranteed that each packet will be retried for six times.

RADIUS DNS

You can use a fully qualified domain name (FQDN) that enables you to change the IP address when needed, for example, for load balancing updates. A submenu, DNS, is added to the **Security > AAA > RADIUS** menu, which you can use to get RADIUS IP information from a DNS. The DNS query is disabled by default.

This section contains the following subsections:

Configuring RADIUS (GUI)

Step 1 Choose **Security** > **AAA** > **RADIUS**.

Step 2 Perform one of the following:

- If you want to configure a RADIUS server for authentication, choose **Authentication**.
- If you want to configure a RADIUS server for accounting, choose **Accounting**.

Note The pages used to configure authentication and accounting contain mostly the same text boxes. Therefore, these instructions walk through the configuration only once, using the Authentication pages as examples. You would follow the same steps to configure multiple services and/or multiple servers.

The RADIUS Authentication (or Accounting) Servers page appears.

This page lists any RADIUS servers that have already been configured.

- If you want to delete an existing server, hover your cursor over the blue drop-down arrow for that server and choose **Remove**.
- If you want to make sure that the controller can reach a particular server, hover your cursor over the blue drop-down arrow for that server and choose **Ping**.

Step 3 From the **Call Station ID Type** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The following options are available:

- IP Address
- System MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID
- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID

Note The AP Name:SSID, AP Name, AP Group, Flex Group, AP Location, and VLAN ID options are added in the 7.4 release.

Step 4 Enable RADIUS-to-controller key transport using AES key wrap protection by checking the **Use AES Key Wrap** check box. The default value is unchecked. This feature is required for FIPS customers.

Step 5 From the **MAC Delimiter** drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The following options are available:

- Colon
- Hyphen
- Single-hyphen
- None

Step 6 Click **Apply**. Perform one of the following:

- To edit an existing RADIUS server, click the server index number for that server. The **RADIUS Authentication (or Accounting) Servers > Edit** page appears.
- To add a RADIUS server, click **New**. The **RADIUS Authentication (or Accounting) Servers > New** page appears.

Step 7 If you are adding a new server, choose a number from the **Server Index (Priority)** drop-down list to specify the priority order of this server in relation to any other configured RADIUS servers providing the same service.

Step 8 If you are adding a new server, enter the IP address of the RADIUS server in the **Server IP Address** text box.

Note Auto IPv6 is not supported on RADIUS server. The RADIUS server must not be configured with Auto IPv6 address. Use fixed IPv6 address instead.

Step 9 From the **Shared Secret Format** drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret key to be used between the controller and the RADIUS server. The default value is ASCII.

Step 10 In the **Shared Secret** and **Confirm Shared Secret** text boxes, enter the shared secret key to be used for authentication between the controller and the server.

Note The shared secret key must be the same on both the server and the controller.

Step 11 If you are configuring a new RADIUS authentication server and want to enable AES key wrap, which makes the shared secret between the controller and the RADIUS server more secure, follow these steps:

Note AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.

a) Check the **Key Wrap** check box.
b) From the **Key Wrap Format** drop-down list, choose **ASCII** or **HEX** to specify the format of the AES key wrap keys: Key Encryption Key (KEK) and Message Authentication Code Key (MACK).
c) In the **Key Encryption Key (KEK)** text box, enter the 16-byte KEK.
d) In the **Message Authentication Code Key (MACK)** text box, enter the 20-byte KEK.

Step 12 If you are adding a new server, enter the RADIUS server's UDP port number for the interface protocols in the **Port Number** text box. The valid range is 1 to 65535, and the default value is 1812 for authentication and 1813 for accounting.

Step 13 From the **Server Status** text box, choose **Enabled** to enable this RADIUS server or choose **Disabled** to disable it. The default value is enabled.

Step 14 If you are configuring a new RADIUS authentication server, from the **Support for RFC 3576** drop-down list, choose **Enabled** to enable change of authorization, which is an extension to the RADIUS protocol that allows dynamic changes to a user session, or choose **Disabled** to disable this feature. By default, this is set to Disabled state. Support for RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session and supports disconnect and change of authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately where CoA messages modify session authorization attributes such as data filters.

Step 15 In the **Server Timeout** text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Check the **Key Wrap** check box.

Note We recommend that you increase the timeout value if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable.

Step 16 Check the **Network User** check box to enable network user authentication (or accounting), or uncheck it to disable this feature. The default value is unchecked. If you enable this feature, this entry is considered the RADIUS authentication (or accounting) server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.

Step 17 If you are configuring a RADIUS authentication server, check the **Management** check box to enable management authentication, or uncheck the check box to disable this feature. The default value is checked. If you enable this feature, this entry is considered the RADIUS authentication server for management users, and authentication requests go to the RADIUS server.

Step 18 Enter the **Management Retransmit Timeout** value, which denotes the network login retransmission timeout for the server.

Step 19 Check the **IPSec** check box to enable the IP security mechanism, or uncheck the check box to disable this feature. The default value is unchecked.

Note IPSec is not supported for IPv6. Use this only if you have used IPv4 for Server IP Address.

Step 20 If you enabled IPsec, follow these steps to configure additional IPsec parameters:

a) From the IPSec drop-down list, choose one of the following options as the authentication protocol to be used for IP security: **HMAC MD5** or **HMAC SHA1**. The default value is HMAC SHA1.

A message authentication code (MAC) is used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is based on cryptographic hash functions. It can be used in combination with any iterated cryptographic hash function. HMAC MD5 and HMAC SHA1 are two constructs of the HMAC using the MD5 hash function and the SHA1 hash function. HMAC also uses a secret key for calculation and verification of the message authentication values.

b) From the IPSec Encryption drop-down list, choose one of the following options to specify the IP security encryption mechanism:

- **DES**—Data Encryption Standard that is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
- **3DES**—Data Encryption Standard that applies three keys in succession. This is the default value.
- **AES CBC**—Advanced Encryption Standard that uses keys with a length of 128, 192, or 256 bits to encrypt data blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Block Chaining (CBC) mode.
- **256-AES**—Advanced Encryption Standard that uses keys with a length of 256 bits.

c) From the IKE Phase 1 drop-down list, choose one of the following options to specify the Internet Key Exchange (IKE) protocol: **Aggressive** or **Main**. The default value is Aggressive.

IKE Phase 1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets with the benefit of slightly faster connection establishment at the cost of transmitting the identities of the security gateways in the clear.

d) In the Lifetime text box, enter a value (in seconds) to specify the timeout interval for the session. The valid range is 1800 to 57600 seconds, and the default value is 1800 seconds.

e) From the IKE Diffie Hellman Group drop-down list, choose one of the following options to specify the IKE Diffie Hellman group: **Group 1 (768 bits)**, **Group 2 (1024 bits)**, or **Group 5 (1536 bits)**. The default value is Group 1 (768 bits).

Diffie-Hellman techniques are used by two devices to generate a symmetric key through which they can publicly exchange values and generate the same symmetric key. Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size.

Note If the shared secret for IPSec is not configured, the default radius shared secret is used. If the authentication method is PSK, WLANCC should be enabled to use the IPSec shared secret, default value is used otherwise. You can view the status for the WLANCC and UCAPL prerequisite modes in **Controller** > **Inventory**.

Step 21 Click **Apply**.

Step 22 Click **Save Configuration**.

Step 23 Repeat the previous steps if you want to configure any additional services on the same server or any additional RADIUS servers.

Step 24 Specify the RADIUS server fallback behavior, as follows:

a) Choose **Security** > **AAA** > **RADIUS > Fallback to open the RADIUS > Fallback Parameters** to open the fallback parameters page.

b) From the **Fallback Mode** drop-down list, choose one of the following options:

- **Off**—Disables RADIUS server fallback. This is the default value.
- **Passive**—Causes the controller to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
- **Active**—Causes the controller to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.

c) If you enabled Active fallback mode in *Step b*, enter the name to be sent in the inactive server probes in the **Username** text box. You can enter up to 16 alphanumeric characters. The default value is "cisco-probe."

d) If you enabled Active fallback mode in *Step b*, enter the probe interval value (in seconds) in the Interval in **Sec** text box. The interval serves as inactive time in passive mode and probe interval in active mode. The valid range is 180 to 3600 seconds, and the default value is 300 seconds.

Step 25 Specify the RADIUS DNS parameters as follows:

Note IPv6 is not supported for RADIUS DNS.

a) Choose **Security** > **AAA** > **RADIUS** > **DNS**. The **RADIUS DNS Parameters** page appears.

b) Check or uncheck the **DNS Query** check box.

c) In the **Port Number** text box, enter the authentication port number. The valid range is 1 to 65535.

The accounting port number is an increment of 1 of the authentication port number. For example, if you define the authentication port number as 1812, the accounting port number is 1813. The accounting port number is always derived from the authentication port number.

d) From the **Secret Format** drop-down list, choose the format in which you want to configure the secret. Valid options are ASCII and Hex.

e) Depending on the format selected, enter and confirm the secret.

Note All servers are expected to use the same authentication port and the same secret.

f) In the **DNS Timeout** text box, enter the number of days after which the DNS query is refreshed to get the latest update from the DNS server.

g) In the **URL** text box, enter the fully qualified domain name or the absolute domain name of the RADIUS server.

h) In the **Server IP Address** text box, enter the IP address of the DNS server.

i) Click **Apply**.

Step 26 Specify the order of authentication when multiple databases are configured by choosing **Security** > **Priority Order** > **Management User**. The Priority Order > Management User page appears.

Step 27 In the Order Used for Authentication text box, specify which servers have priority when the controller attempts to authenticate management users. Use the **>** and **<** buttons to move servers between the Not Used and Order Used for Authentication text boxes. After the desired servers appear in the Order Used for **Authentication** text box, use the **Up** and **Down** buttons to move the priority server to the top of the list.

By default, the local database is always queried first. If the username is not found, the controller switches to the RADIUS server if configured for RADIUS or to the TACACS+ server if configured for TACACS+. The default setting is local and then RADIUS.

Step 28 Click **Apply**.

Step 29 Click **Save Configuration**.

Related Topics

Configuring TACACS+ (GUI), on page 390

Configuring RADIUS (CLI)

Procedure

- Specify whether the IP address, system MAC address, AP MAC address, AP Ethernet MAC address of the originator will be sent to the RADIUS server in the Access-Request message by entering this command:

  config radius callStationIdType {**ipaddr** | **macaddr** | **ap-macaddr-only** | **ap-macaddr-ssid** | | | **ap-group-name** | **ap-location** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **vlan-id**}

Note The default is System MAC Address.

Caution Do not use Called Station ID Type for IPv6-only clients.

- Specify the delimiter to be used in the MAC addresses that are sent to the RADIUS authentication or accounting server in Access-Request messages by entering this command:

  config radius {**auth** | **acct**} **mac-delimiter** {**colon** | **hyphen** | **single-hyphen** | **none**}

  where

  - **colon** sets the delimiter to a colon (the format is xx:xx:xx:xx:xx:xx).
  - **hyphen** sets the delimiter to a hyphen (the format is xx-xx-xx-xx-xx-xx). This is the default value.
  - **single-hyphen** sets the delimiter to a single hyphen (the format is xxxxxx-xxxxxx).
  - **none** disables delimiters (the format is xxxxxxxxxxxx).

- Configure a RADIUS authentication server by entering these commands:
  - **config radius auth add** *index server_ip_address port_number* {**ascii** | **hex**} **shared_secret**—Adds a RADIUS authentication server.
  - **config radius auth keywrap** {**enable** | **disable**}—Enables AES key wrap, which makes the shared secret between the controller and the RADIUS server more secure. AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.
  - **config radius auth keywrap add {ascii** | **hex**} *kek mack index*—Configures the AES key wrap attributes

    where

    - *kek* specifies the 16-byte Key Encryption Key (KEK).
    - *mack* specifies the 20-byte Message Authentication Code Key (MACK).
    - *index* specifies the index of the RADIUS authentication server on which to configure the AES key wrap.

- **config radius auth rfc3576 {enable | disable}** *index*—Enables or disables RFC 3576, which is an extension to the RADIUS protocol that allows dynamic changes to a user session. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session and supports disconnect and change-of-authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately where CoA messages modify session authorization attributes such as data filters.
- **config radius auth retransmit-timeout** *index timeout*—Configures the retransmission timeout value for a RADIUS authentication server.
- **config radius auth mgmt-retransmit-timeout** *index timeout*—Configures the default management login retransmission timeout for a RADIUS authentication server.
- **config radius auth network** *index* **{enable | disable}**—Enables or disables network user authentication. If you enable this feature, this entry is considered the RADIUS authentication server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.
- **config radius auth management** *index* **{enable | disable}**—Enables or disables management authentication. If you enable this feature, this entry is considered the RADIUS authentication server for management users, and authentication requests go to the RADIUS server.
- **config radius auth ipsec** {**enable** | **disable**} *index*—Enables or disables the IP security mechanism.
- **config radius auth ipsec authentication** {**hmac-md5** | **hmac-sha1**} *index*—Configures the authentication protocol to be used for IP security.
- **config radius auth ipsec encryption** {**3des** | **aes** | **des** | **none**} *index*—Configures the IP security encryption mechanism.
- **config radius auth ipsec ike dh-group** {**group-1** | **group-2** | **group-5** | **2048bit-group-14**} *index*—Configures the IKE Diffie-Hellman group.
- **config radius auth ipsec ike lifetime** *interval index*—Configures the timeout interval for the session.
- **config radius auth ipsec ike phase1** {**aggressive** | **main**} *index*—Configures the Internet Key Exchange (IKE) protocol.
- **config radius auth ipsec ike auth-method** {**PSK** | **certificate**} *index*—Configures the IKE authentication methods. By default PSK is be used for IPSEC sessions.
- **config radius auth ipsec ike auth-mode pre-shared-key** *index hex/asciisecret*—Configures the IPSEC pre-shared key.
- **config radius auth ipsec ike auth-mode** {**pre-shared-key** *index hex-ascii-index shared-secret* | **certificate** *index*} —Configures the IKE authentication method. By default, preshared key is used for IPSEC sessions.
- **config radius auth** {**enable** | **disable**} *index*—Enables or disables a RADIUS authentication server.
- **config radius auth delete** *index*—Deletes a previously added RADIUS authentication server.

• Configure a RADIUS accounting server by entering these commands:

- **config radius acct add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*—Adds a RADIUS accounting server.

- **config radius acct server-timeout** *index timeout*—Configures the retransmission timeout value for a RADIUS accounting server.
- **config radius acct network** *index* {**enable** | **disable**}—Enables or disables network user accounting. If you enable this feature, this entry is considered the RADIUS accounting server for network users. If you did not configure a RADIUS server entry on the WLAN, you must enable this option for network users.
- **config radius acct ipsec** {**enable** | **disable**} *index*—Enables or disables the IP security mechanism.
- **config radius acct ipsec authentication** {**hmac-md5** | **hmac-sha1**} *index*—Configures the authentication protocol to be used for IP security.
- **config radius acct ipsec encryption** { **3des** | **aes** | **des** | **none**} *index*—Configures the IP security encryption mechanism.
- **config radius acct ipsec ike dh-group** {**group-1** | **group-2** | **group-5**} *index*—Configures the IKE Diffie Hellman group.
- **config radius acct ipsec ike lifetime** *interval index*—Configures the timeout interval for the session.
- **config radius acct ipsec ike phase1**{**aggressive** | **main**} *index*—Configures the Internet Key Exchange (IKE) protocol.
- **config radius acct** {**enable** | **disable**} index—Enables or disables a RADIUS accounting server.
- **config radius acct delete index**—Deletes a previously added RADIUS accounting server.
- **config radius auth callStationIdType ap-group-name** —Sets the Called Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
- **config radius auth callStationIdType ap-location**—Sets the Called Station ID to the AP Location.
- **config radius auth callStationIdType** {**ap-macaddr-only** | **ap-macaddr-ssid**}—Sets the Called Station ID type to be AP's radio MAC address or AP's radio MAC address with SSID in the <AP radio MAC address>:<SSID> format.
- **config radius auth callStationIdType** {**ap-name** | **ap-name-ssid**}—Sets the Called Station ID type to be AP name or AP name with SSID in the <AP name>:<SSID> format.
- **config radius auth callStationIdType flex-group-name**—Sets the Called Station ID type to the FlexConnect group name.
- **config radius auth callStationIdType** {**ipaddr** | **macaddr**}—Sets the Called Station ID type to use the IP address (only Layer 3) or system's MAC address.
- **config radius auth callStationIdType vlan-id**—Sets the Called Station ID type to the system's VLAN ID.

- Configure the RADIUS server fallback behavior by entering this command:

  config radius fallback-test mode {off | passive | active}

  where

  - **off** disables RADIUS server fallback.

- **passive** causes the controller to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The controller simply ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
- **active** Causes the controller to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.

- If you enabled Active mode in *Step 5*, enter these commands to configure additional fallback parameters:
  - **config radius fallback-test username** *username*—Specifies the name to be sent in the inactive server probes. You can enter up to 16 alphanumeric characters for the *username parameter*.
  - **config radius fallback-test interval** *interval*—Specifies the probe interval value (in seconds).
- Configure RADIUS DNS parameters by entering these commands:
  - **config radius dns global** *port-num* {*ascii* | *hex*} *secret*—Adds global port number and secret information for the RADIUS DNS.
  - **config radius dns query** *url timeout-in-days*—Configures the FQDN of the RADIUS server and timeout after which a refresh is performed to get the latest update from the DNS server.
  - **config radius dns serverip** *ip-addr*—Configures the IP address of the DNS server.
  - **config radius dns** {**enable** | **disable**}—Enables or disables the DNS query.
- Save your changes by entering this command:

  save config
- Configure the order of authentication when multiple databases are configured by entering this command:

  config aaa auth mgmt *AAA_server_type AAA_server_type*

  where *AAA_server_type is* local, RADIUS, or TACACS+.

  To see the current management authentication server order, enter the **show aaa auth** command.
- See RADIUS statistics by entering these commands:
  - **show radius summary**—Shows a summary of RADIUS servers and statistics with AP Ethernet MAC configurations.
  - **show radius auth statistics**—Shows the RADIUS authentication server statistics.
  - **show radius acct statistics**—Shows the RADIUS accounting server statistics.
  - **show radius rfc3576 statistics**—Shows a summary of the RADIUS RFC-3576 server.
- See active security associations by entering these commands:
  - **show ike {brief | detailed}** *ip_or_mac_addr*—Shows a brief or detailed summary of active IKE security associations.

- **show ipsec {brief | detailed}** *ip_or_mac_addr*—Shows a brief or detailed summary of active IPSec security associations.

- Clear the statistics for one or more RADIUS servers by entering this command:

  clear stats radius {**auth** | **acct**} {*index* | **all**}

- Make sure that the controller can reach the RADIUS server by entering this command:

  ping *server_ip_address*

Related Topics

Configuring TACACS+ (CLI), on page 392

RADIUS Authentication Attributes Sent by the Controller

The following tables identify the RADIUS authentication attributes sent between the controller and the RADIUS server in access-request and access-accept packets.

Table 9: Authentication Attributes Sent in Access-Request Packets

Attribute ID	Description
1	User-Name
2	Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
12	Framed-MTU
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier
33	Proxy-State
60	CHAP-Challenge
61	NAS-Port-Type
79	EAP-Message

[4] To specify read-only or read-write access to controllers through RADIUS authentication, you must set the Service-Type attribute (6) on the RADIUS server to **Callback NAS Prompt** for read-only access or to **Administrative** for read-write privileges.

Table 10: Authentication Attributes Honored in Access-Accept Packets (Cisco)

Attribute ID	Description
1	Cisco-LEAP-Session-Key
2	Cisco-Keywrap-Msg-Auth-Code
3	Cisco-Keywrap-NonCE
4	Cisco-Keywrap-Key
5	Cisco-URL-Redirect
6	Cisco-URL-Redirect-ACL

Note These Cisco-specific attributes are not supported: Auth-Algo-Type and SSID.

Table 11: Authentication Attributes Honored in Access-Accept Packets (Standard)

Attribute ID	Description
6	Service-Type. To specify read-only or read-write access to controllers through RADIUS authentication, you must set the Service-Type attribute (6) on the RADIUS server to Callback NAS Prompt for read-only access or to Administrative for read-write privileges.
8	Framed-IP-Address
25	Class
26	Vendor-Specific
27	Timeout
29	Termination-Action
40	Acct-Status-Type
64	Tunnel-Type
79	EAP-Message
81	Tunnel-Group-ID

Note Message authentication is not supported.

Table 12: Authentication Attributes Honored in Access-Accept Packets (Microsoft)

Attribute ID	Description
11	MS-CHAP-Challenge
16	MS-MPPE-Send-Key

Attribute ID	Description
17	MS-MPPE-Receive-Key
25	MS-MSCHAP2-Response
26	MS-MSCHAP2-Success

Table 13: Authentication Attributes Honored in Access-Accept Packets (Airespace)

Attribute ID	Description
1	VAP-ID
3	DSCP
4	8021P-Type
5	VLAN-Interface-Name
6	ACL-Name
7	Data-Bandwidth-Average-Contract
8	Real-Time-Bandwidth-Average-Contract
9	Data-Bandwidth-Burst-Contract
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name **Note** Guest-Role-Name is honored only on L3 security web authentication with AAA over-ride enabled on the controller.
13	Data-Bandwidth-Average-Contract-US
14	Real-Time-Bandwidth-Average-Contract-US
15	Data-Bandwidth-Burst-Contract-US
16	Real-Time-Bandwidth-Burst-Contract-US

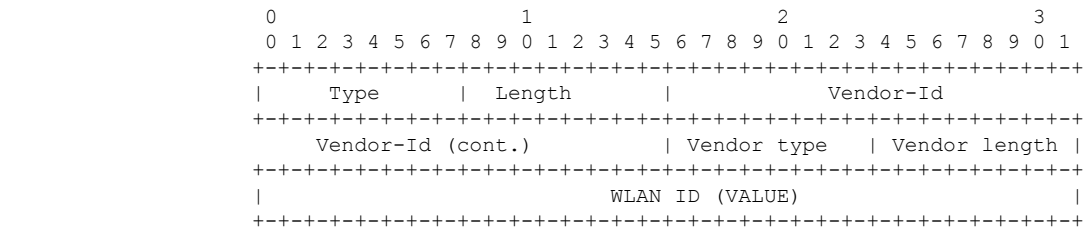
Authentication Attributes Honored in Access-Accept Packets (Airespace)

This section lists the RADIUS authentication Airespace attributes currently supported on the controller.

VAP ID

This attribute indicates the WLAN ID of the WLAN to which the client should belong. When the WLAN-ID attribute is present in the RADIUS Access Accept, the system applies the WLAN-ID (SSID) to the client station after it authenticates. The WLAN ID is sent by the controller in all instances of authentication except IPsec. In case of web authentication, if the controller receives a WLAN-ID attribute in the authentication response from the AAA server, and it does not match the ID of the WLAN, authentication is rejected. The

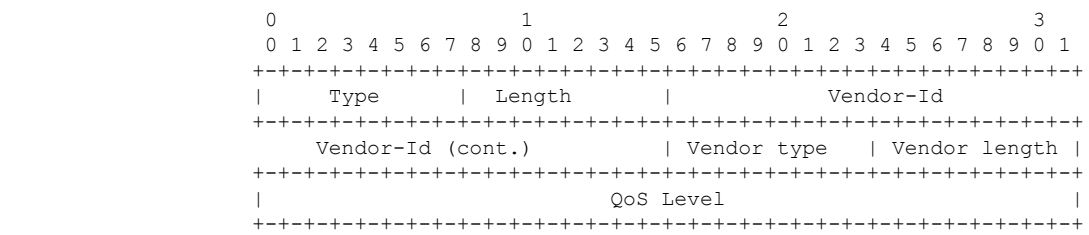
802.1X/MAC filtering is also rejected. The rejection, based on the response from the AAA server, is because of the SSID Cisco AVPair support. The fields are transmitted from left to right.



- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 1
- Vendor length – 4
- Value – ID of the WLAN to which the client should belong.

QoS-Level

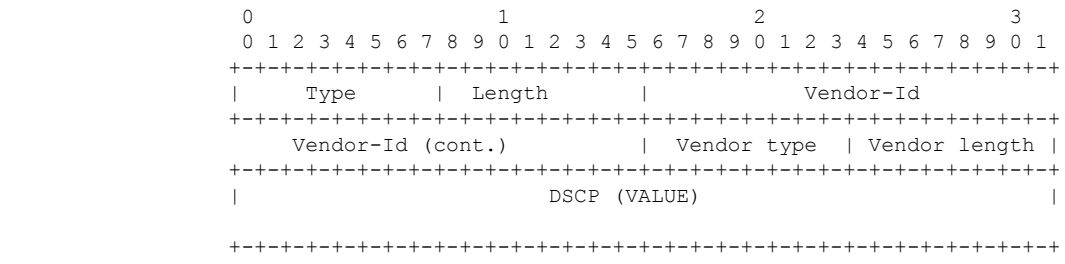
This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The fields are transmitted from left to right.



- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – Three octets:
  - 3 – Bronze (Background)
  - 0 – Silver (Best Effort)
  - 1 – Gold (Video)
  - 2 – Platinum (Voice)

Differentiated Services Code Point (DSCP)

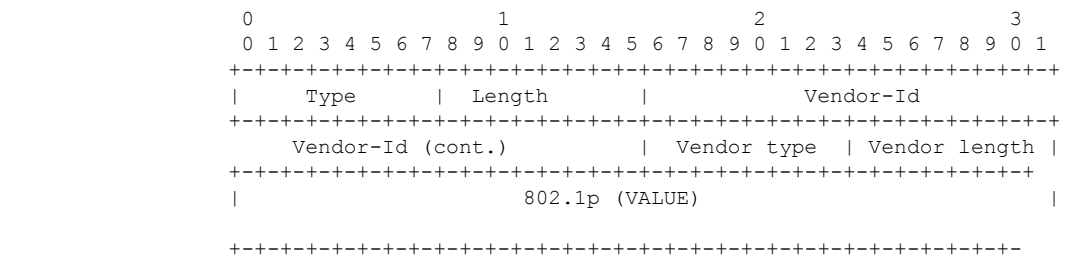
DSCP is a packet header code that can be used to provide differentiated services based on the QoS levels. This attribute defines the DSCP value to be applied to a client. When present in a RADIUS Access Accept, the DSCP value overrides the DSCP value specified in the WLAN profile. The fields are transmitted from left to right.



- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 3
- Vendor length – 4
- Value – DSCP value to be applied for the client.

802.1p Tag Type

802.1p VLAN tag received from the client, defining the access priority. This tag maps to the QoS Level for client-to-network packets. This attribute defines the 802.1p priority to be applied to the client. When present in a RADIUS Access Accept, the 802.1p value overrides the default specified in the WLAN profile. The fields are transmitted from left to right.



- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 4
- Vendor length – 3

- Value – 802.1p priority to be applied to a client.

VLAN Interface Name

This attribute indicates the VLAN interface a client is to be associated to. A summary of the Interface-Name Attribute format is shown below. The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 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 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          |  Vendor type  | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Interface Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value – A string that includes the name of the interface the client is to be assigned to.

Note This attribute only works when MAC filtering is enabled or if 802.1X or WPA is used as the security policy.

ACL-Name

This attribute indicates the ACL name to be applied to the client. A summary of the ACL-Name Attribute format is shown below. The fields are transmitted from left to right.

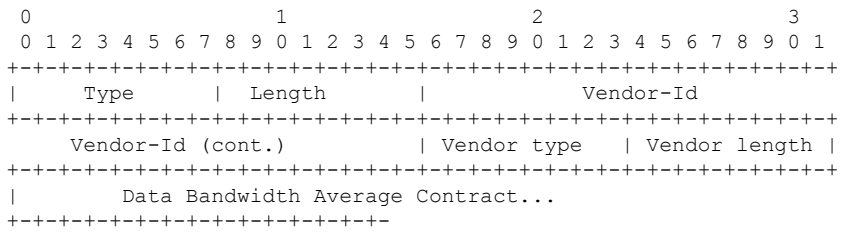
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0

- Value – A string that includes the name of the ACL to use for the client

Data Bandwidth Average Contract

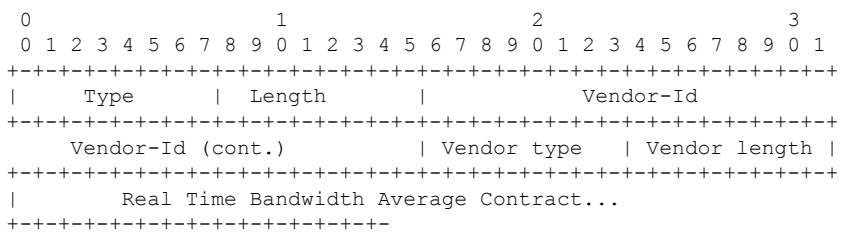
This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied for a client for non-realtime traffic such as TCP. This value is specific for downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Data Bandwidth Average Contract value overrides the Average Data Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.



- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 7
- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Average Contract

This attribute is a rate limiting value. It indicates the Data Bandwidth Average Contract that will be applied to a client for realtime traffic such as UDP. This value is specific for downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Real Time Bandwidth Average Contract value overrides the Average Real-Time Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

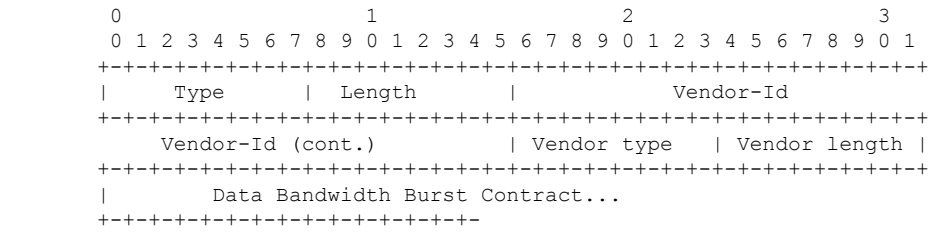


- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 8

- Vendor length – 4
- Value – A value in kbps

Data Bandwidth Burst Contract

This attribute is a rate limiting value. It indicates the Data Bandwidth Burst Contract that will be applied to a client for non-realtime traffic such as TCP. This value is specific to downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Data Bandwidth Burst Contract value overrides the Burst Data Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

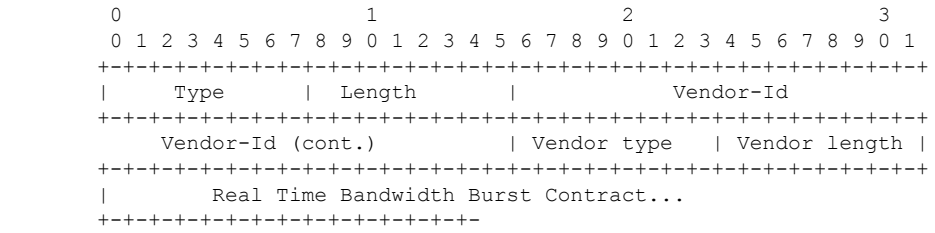


- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 9
- Vendor length – 4
- Value – A value in kbps

Real Time Bandwidth Burst Contract

This attribute is a rate limiting value. It indicates the Data Bandwidth Burst Contract that will be applied to a client for realtime traffic such as UDP. This value is specific to downstream direction from wired to wireless. When present in a RADIUS Access Accept, the Real Time Bandwidth Burst Contract value overrides the Burst Real-Time Rate value present in the WLAN or QoS Profile. The fields are transmitted from left to right.

Note If you try to implement Average Data Rate and Burst Data Rate as AAA override parameters to be pushed from a AAA server, both Average Data Rate and Burst Data Rate have to be sent from ISE.

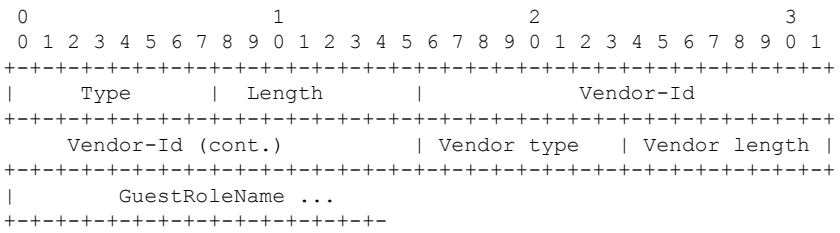


- Type – 26 for Vendor-Specific

- Length – 10
- Vendor-Id – 14179
- Vendor type – 10
- Vendor length – 4
- Value – A value in kbps

Guest Role Name

This attribute provides the bandwidth contract values to be applied for an authenticating user. When present in a RADIUS Access Accept, the bandwidth contract values defined for the Guest Role overrides the bandwidth contract values (based on QOS value) specified for the WLAN. The fields are transmitted from left to right.



- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 11
- Vendor length – Variable based on the Guest Role Name length
- Value – A string of alphanumeric characters

RADIUS Accounting Attributes

This table identifies the RADIUS accounting attributes for accounting requests sent from a controller to the RADIUS server.

Table 14: Accounting Attributes for Accounting Requests

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
8	Framed-IP-Address
25	Class

Attribute ID	Description
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier
40	Accounting-Status-Type
41	Accounting-Delay-Time (Stop and interim messages only)
42	Accounting-Input-Octets (Stop and interim messages only)
43	Accounting-Output-Octets (Stop and interim messages only)
44	Accounting-Session-ID
45	Accounting-Authentic
46	Accounting-Session-Time (Stop and interim messages only)
47	Accounting-Input-Packets (Stop and interim messages only)
48	Accounting-Output-Packets (Stop and interim messages only)
49	Accounting-Terminate-Cause (Stop messages only)
52	Accounting-Input-Gigawords
53	Accounting-Output-Gigawords
55	Event-Timestamp
64	Tunnel-Type
65	Tunnel-Medium-Type
81	Tunnel-Group-ID
	IPv6-Framed-Prefix
190	IPv6-Framed-Address

This table lists the different values for the Accounting-Status-Type attribute (40).

Table 15: Accounting-Status-Type Attribute Values

Attribute ID	Description
1	Start
2	Stop
3	Interim-Update **Note** RADIUS Accounting Interim updates are sent upon each client authentication, even if the RADIUS Server Accounting - Interim Update feature is not enabled on the client's WLAN. Interim updates can also be triggered by events such as mobility events, every time clients receive IPv4 addresses, PEM state changes, and so on.

Attribute ID	Description
7	Accounting-On
8	Accounting-Off
9-14	Reserved for Tunneling Accounting
15	Reserved for Failed

CHAPTER 41

Configuring TACACS+

- Setting up TACACS+, on page 387
- Configuring TACACS+ (GUI), on page 390
- Configuring TACACS+ (CLI), on page 392
- Viewing the TACACS+ Administration Server Logs, on page 393

Setting up TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) is a client/server protocol that provides centralized security for users attempting to gain management access to a controller. It serves as a backend database similar to local and RADIUS. However, local and RADIUS provide only authentication support and limited authorization support while TACACS+ provides three services:

- **Authentication**—The process of verifying users when they attempt to log into the controller.

  Users must enter a valid username and password in order for the controller to authenticate users to the TACACS+ server. The authentication and authorization services are tied to one another. For example, if authentication is performed using the local or RADIUS database, then authorization would use the permissions that are associated with the user in the local or RADIUS database (which are read-only, read-write, and lobby-admin) and not use TACACS+. Similarly, when authentication is performed using TACACS+, authorization is tied to TACACS+.

  Note When multiple databases are configured, you can use the controller GUI or CLI to specify the sequence in which the backend databases should be tried.

- **Authorization**—The process of determining the actions that users are allowed to take on the controller based on their level of access.

  For TACACS+, authorization is based on privilege (or role) rather than specific actions. The available roles correspond to the seven menu options on the controller GUI: MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. An additional role, LOBBY, is available for users who require only lobby ambassador privileges. The roles to which users are assigned are configured on the TACACS+ server. Users can be authorized for one or more roles.

- The minimum authorization is MONITOR only, and the maximum is ALL, which authorizes the user to execute the functionality associated with all seven menu options. For example, a user who is assigned the role of SECURITY can make changes to any items appearing on the Security menu (or designated

as security commands in the case of the CLI). If users are not authorized for a particular role (such as WLAN), they can still access that menu option in read-only mode (or the associated CLI **show** commands). If the TACACS+ authorization server becomes unreachable or unable to authorize, users are unable to log into the controller.

Note If users attempt to make changes on a controller GUI page that are not permitted for their assigned role, a message appears indicating that they do not have sufficient privilege. If users enter a controller CLI command that is not permitted for their assigned role, a message may appear indicating that the command was successfully executed although it was not. In this case, the following additional message appears to inform users that they lack sufficient privileges to successfully execute the command: "Insufficient Privilege! Cannot execute command!"

- **Accounting**—The process of recording user actions and changes.

  Whenever a user successfully executes an action, the TACACS+ accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided. If the TACACS+ accounting server becomes unreachable, users are able to continue their sessions uninterrupted.

  Note The logs under TACACS+ records the configurations as user readable statements.

TACACS+ uses Transmission Control Protocol (TCP) for its transport, unlike RADIUS which uses User Datagram Protocol (UDP). It maintains a database and listens on TCP port 49 for incoming requests. The controller, which requires access control, acts as the client and requests AAA services from the server. The traffic between the controller and the server is encrypted by an algorithm that is defined in the protocol and a shared secret key that is configured on both devices.

You can configure up to three TACACS+ authentication, authorization, and accounting servers each. For example, you may want to have one central TACACS+ authentication server but several TACACS+ authorization servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one and then the third one if necessary.

Note If multiple TACACS+ servers are configured for redundancy, the user database must be identical in all the servers for the backup to work properly.

The following are some guidelines about TACACS+:

- You must configure TACACS+ on both your CiscoSecure Access Control Server (ACS) and your controller. You can configure the controller through either the GUI or the CLI.
- TACACS+ is supported on CiscoSecure ACS version 3.2 and later releases. See the CiscoSecure ACS documentation for the version that you are running.

- One Time Passwords (OTPs) are supported on the controller using TACACS. In this configuration, the controller acts as a transparent passthrough device. The controller forwards all client requests to the TACACS server without inspecting the client behavior. When using OTP, the client must establish a single connection to the controller to function properly. The controller currently does not have any intelligence or checks to correct a client that is trying to establish multiple connections.
- We recommend that you increase the retransmit timeout value for TACACS+ authentication, authorization, and accounting servers if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable. The default retransmit timeout value is 2 seconds and you can increase the retransmit timeout value to a maximum of 30 seconds.
- If you want to migrate your configuration from a Cisco 5508 WLC to a Cisco 5520 WLC, the RADIUS or TACACS+ configuration present in Cisco 5508 WLC does not work in Cisco 5520 WLC. We recommend that you configure the RADIUS or TACACS+ configuration again after migration.
- To configure the TACACS+ server:
  - Using Access Control Server (ACS)—See the latest Cisco Secure Access Control System guide at http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html.
  - Using Identity Services Engine (ISE)—See the *ISE TACACS+ Configuration Guide for Wireless LAN Controllers* at http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-TACACS_for_WLC.pdf.

TACACS+ DNS

You can use a fully qualified domain name (FQDN) that enables you to change the IP address when needed, for example, for load-balancing updates. A submenu, DNS, is added to the **Security > AAA > TACACS+** menu, which you can use to get TACACS+ IP information from a DNS. The DNS query is disabled by default.

Note IPv6 is not supported for TACAS+ DNS.

It is not possible to use both the static list and the DNS list at the same time. The addresses that are returned by the DNS override the static entries.

DNS AAA is valid for FlexConnect AP clients that use central authentication.

DNS AAA is not supported to define a RADIUS for FlexConnect AP groups. For FlexConnect clients with local switching, you have to manually define AAA.

Rogue, 802.1X, web authentication, MAC filtering, mesh, and other features that use the global list also use the DNS-defined servers.

This section contains the following subsections:

TACACS+ VSA

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the TACACS+ server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use.

The Cisco TACACS+ implementation supports one vendor-specific option using the format recommended in the IETF specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named cisco-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Cisco attribute for a particular type of authorization, the separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

Configuring TACACS+ (GUI)

Step 1 Choose **Security** > **AAA** > **TACACS+**.

Step 2 Perform one of the following:

- If you want to configure a TACACS+ server for authentication, choose **Authentication**.
- If you want to configure a TACACS+ server for authorization, choose **Authorization**.
- If you want to configure a TACACS+ server for accounting, choose **Accounting**.

Note The pages used to configure authentication, authorization, and accounting all contain the same text boxes. Therefore, these instructions walk through the configuration only once, using the Authentication pages as examples. You would follow the same steps to configure multiple services and/or multiple servers.

For basic management authentication via TACACS+ to succeed, it is required to configure authentication and authorization servers on the WLC. Accounting configuration is optional.

The TACACS+ (Authentication, Authorization, or Accounting) Servers page appears. This page lists any TACACS+ servers that have already been configured.

- If you want to delete an existing server, hover your cursor over the blue drop-down arrow for that server and choose **Remove**.
- If you want to make sure that the controller can reach a particular server, hover your cursor over the blue drop-down arrow for that server and choose **Ping**.

Step 3 Perform one of the following:

- To edit an existing TACACS+ server, click the server index number for that server. The **TACACS+ (Authentication, Authorization, or Accounting) Servers > Edit** page appears.
- To add a TACACS+ server, click **New**. The **TACACS+ (Authentication, Authorization, or Accounting) Servers > New** page appears.

Step 4 If you are adding a new server, choose a number from the Server Index (Priority) drop-down list to specify the priority order of this server in relation to any other configured TACACS+ servers providing the same service. You can configure up to three servers. If the controller cannot reach the first server, it tries the second one in the list and then the third if necessary.

Step 5 If you are adding a new server, enter the IP address of the TACACS+ server in the **Server IP Address** text box.

Step 6 From the **Shared Secret Format** drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret key to be used between the controller and the TACACS+ server. The default value is ASCII.

Step 7 In the **Shared Secret** and **Confirm Shared Secret** text boxes, enter the shared secret key to be used for authentication between the controller and the server.

Note The shared secret key must be the same on both the server and the controller.

Step 8 If you are adding a new server, enter the TACACS+ server's TCP port number for the interface protocols in the **Port Number** text box. The valid range is 1 to 65535, and the default value is 49.

Step 9 In the **Server Status** text box, choose **Enabled** to enable this TACACS+ server or choose **Disabled** to disable it. The default value is Enabled.

Step 10 In the **Server Timeout** text box, enter the number of seconds between retransmissions. The valid range is 5 to 30 seconds, and the default value is 5 seconds.

Note We recommend that you increase the timeout value if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable.

Step 11 Click **Apply**.

Step 12 Specify the TACACS+ DNS parameters as follows:

a) Choose **Security** > **AAA** > **TACACS+** > **DNS**. The **TACACS DNS Parameters** page appears.
b) Select or unselect the **DNS Query** check box.
c) In the **Interval in sec** text box, enter the authentication port number. The valid range is 1 to 65535.

The accounting port number is an increment of 1 of the authentication port number. For example, if you define the authentication port number as 1812, the accounting port number is 1813. The accounting port number is always derived from the authentication port number.

d) From the **Secret Format** drop-down list, choose the format in which you want to configure the secret. Valid options are ASCII and Hex.
e) Depending on the format selected, enter and confirm the secret.

Note All servers are expected to use the same authentication port and the same secret.

f) In the **DNS Timeout** text box, enter the number of days after which the DNS query is refreshed to get the latest update from the DNS server.
g) In the **URL** text box, enter the fully qualified domain name or the absolute domain name of the TACACS+ server.
h) In the **Server IP Address** text box, enter the IPv4 address of the DNS server.

Note IPv6 is not supported for TACACS+ DNS.

i) Click **Apply**.

Step 13 Click **Save Configuration**.

Step 14 Repeat the previous steps if you want to configure any additional services on the same server or any additional TACACS+ servers.

Step 15 Specify the order of authentication when multiple databases are configured by choosing **Security** > **Priority Order** > **Management User**. The Priority Order > Management User page appears.

Step 16 In the **Order Used for Authentication** text box, specify which servers have priority when the controller attempts to authenticate management users.

Use the **>** and **<** buttons to move servers between the **Not Used** and **Order Used for Authentication** text boxes. After the desired servers appear in the Order Used for Authentication text box, use the **Up** and **Down** buttons to move the priority server to the top of the list. By default, the local database is always queried first. If the username is not found, the controller switches to the RADIUS server if configured for RADIUS or to the TACACS+ server if configured for TACACS+. The default setting is local and then RADIUS.

Step 17 Click **Apply**.

Step 18 Click **Save Configuration**.

Related Topics

Configuring RADIUS (GUI), on page 367

Configuring TACACS+ (CLI)

Procedure

- Configure a TACACS+ authentication server by entering these commands:
  - **config tacacs auth add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*—Adds a TACACS+ authentication server.
  - **config tacacs auth delete** *index*—Deletes a previously added TACACS+ authentication server.
  - **config tacacs auth** {**enable** | **disable**} *index*—Enables or disables a TACACS+ authentication server.
  - **config tacacs auth server-timeout** *index timeout*—Configures the retransmission timeout value for a TACACS+ authentication server.
- Configure a TACACS+ authorization server by entering these commands:
  - **config tacacs athr add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*—Adds a TACACS+ authorization server.
  - **config tacacs athr delete** *index*—Deletes a previously added TACACS+ authorization server.
  - **config tacacs athr** {**enable** | **disable**} *index*—Enables or disables a TACACS+ authorization server.
  - **config tacacs athr server-timeout** *index timeout*—Configures the retransmission timeout value for a TACACS+ authorization server.
- Configure a TACACS+ accounting server by entering these commands:
  - **config tacacs acct add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*—Adds a TACACS+ accounting server.
  - **config tacacs acct delete** *index*—Deletes a previously added TACACS+ accounting server.
  - **config tacacs acct** {**enable** | **disable**} *index*—Enables or disables a TACACS+ accounting server.
  - **config tacacs acct server-timeout** *index timeout*—Configures the retransmission timeout value for a TACACS+ accounting server.
- See TACACS+ statistics by entering these commands:
  - **show tacacs summary**—Shows a summary of TACACS+ servers and statistics.
  - **show tacacs auth stats**—Shows the TACACS+ authentication server statistics.
  - **show tacacs athr stats**—Shows the TACACS+ authorization server statistics.

- **show tacacs acct stats**—Shows the TACACS+ accounting server statistics.

- Clear the statistics for one or more TACACS+ servers by entering this command:

  clear stats tacacs [**auth** | **athr** | **acct**] {*index* | *all*}

- Configure the order of authentication when multiple databases are configured by entering this command. The default setting is local and then radius.

  config aaa auth mgmt [**radius** | **tacacs**]

  See the current management authentication server order by entering the **show aaa auth** command.

- Make sure the controller can reach the TACACS+ server by entering this command:

  ping *server_ip_address*

- Configure TACACS+ DNS parameters by entering these commands:

  - **config tacacs dns global** *port-num* {*ascii* | *hex*} *secret*—Adds global port number and secret information for the TACACS+ DNS.
  - **config tacacs dns query** *url timeout-in-days*—Configures the FQDN of the TACACS+ server and timeout after which a refresh is performed to get the latest update from the DNS server.
  - **config tacacs dns serverip** *ip-addr*—Configures the IP address of the DNS server.
  - **config tacacs dns** {**enable** | **disable**}—Enables or disables the DNS query.

- Enable or disable TACACS+ debugging by entering this command:

  debug aaa tacacs {**enable** | **disable**}

- Save your changes by entering this command:

  save config

Related Topics

Configuring RADIUS (CLI), on page 372

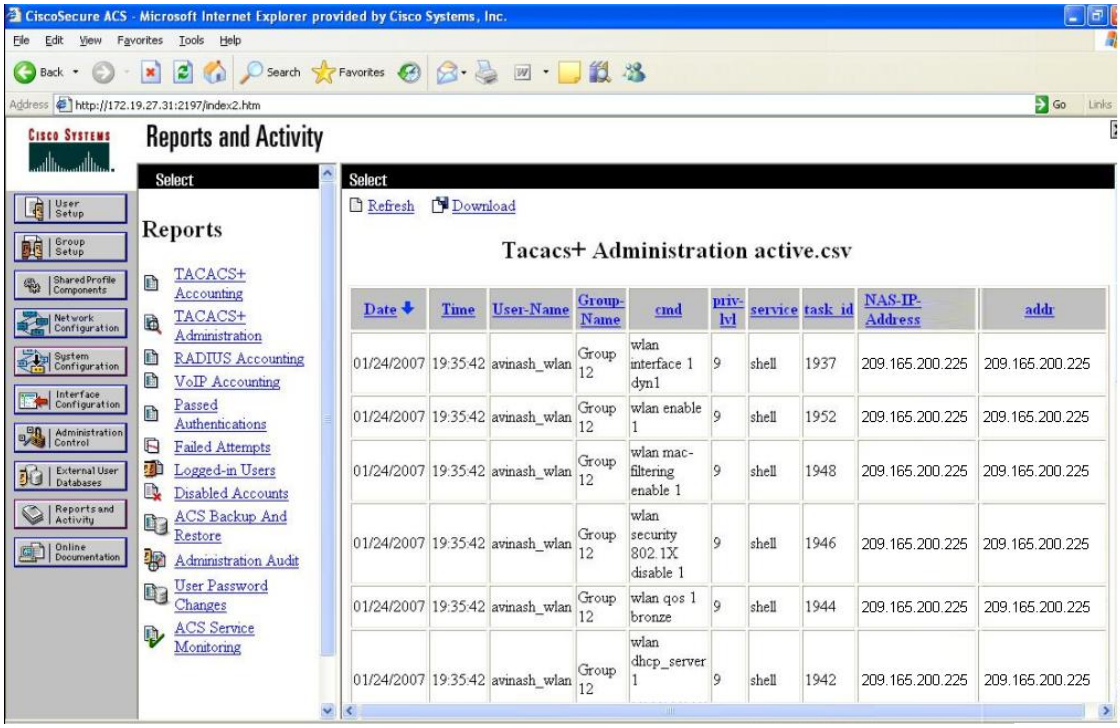
Viewing the TACACS+ Administration Server Logs

Step 1 On the ACS main page, in the left navigation pane, choose **Reports and Activity**.

Step 2 Under Reports, choose **TACACS+ Administration**.

Click the .csv file corresponding to the date of the logs you want to view. The TACACS+ Administration .csv page appears.

Figure 36: TACACS+ Administration .csv Page on CiscoSecure ACS

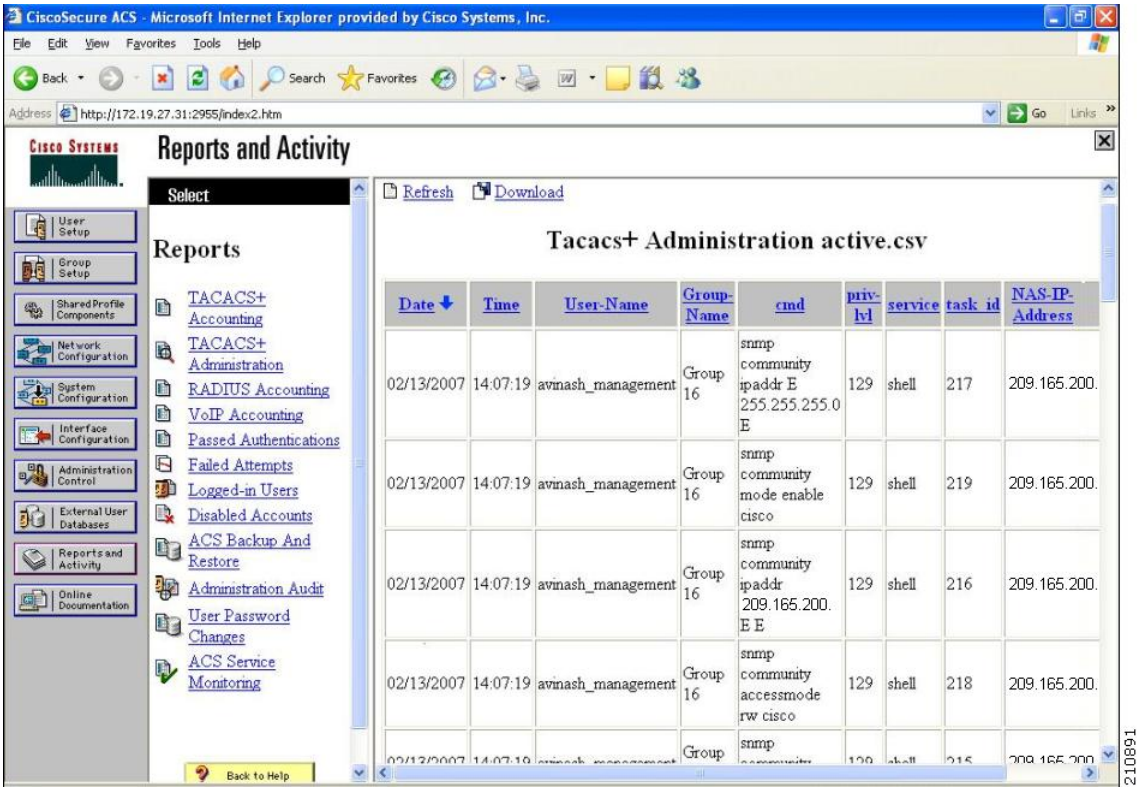


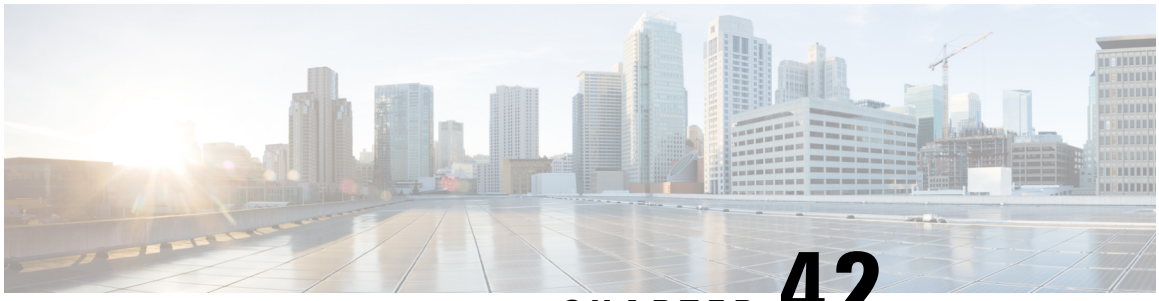
This page displays the following information:

- Date and time the action was taken
- Name and assigned role of the user who took the action
- Group to which the user belongs
- Specific action that the user took
- Privilege level of the user who executed the action
- IP address of the controller
- IP address of the laptop or workstation from which the action was executed

Sometimes a single action (or command) is logged multiple times, once for each parameter in the command. For example, if you enter the **snmp community ipaddr** *ip_address subnet_mask community_name* command, the IP address may be logged on one line while the subnet mask and community name are logged as "E." On another line, the subnet mask maybe logged while the IP address and community name are logged as "E." See the first and third lines in the example in this figure.

Figure 37: TACACS+ Administration .csv Page on CiscoSecure ACS





CHAPTER 42

Configuring Maximum Local Database Entries

- Maximum Local Database Entries, on page 397
- Configuring Maximum Local Database Entries (GUI), on page 397
- Configuring Maximum Local Database Entries (CLI), on page 397

Maximum Local Database Entries

You can configure the controller to specify the maximum number of local database entries that are used for storing user authentication information. The database entries include local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries, and access point authorization list entries. Together they cannot exceed the configured maximum value.

This section contains the following subsections:

Configuring Maximum Local Database Entries (GUI)

Step 1 Choose **Security** > **AAA** > **General** to open the General page.

Step 2 In the Maximum Local Database Entries text box, enter a value for the maximum number of entries that can be added to the local database the next time the controller reboots. The currently configured value appears in parentheses to the right of the text box. The valid range is 512 to 2048, and the default setting is 2048.

The **Number of Entries, Already Used** text box shows the number of entries currently in the database.

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

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

Configuring Maximum Local Database Entries (CLI)

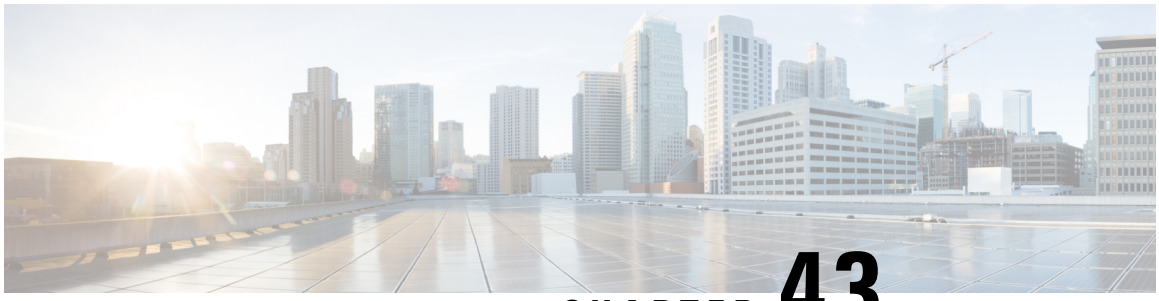
Step 1 Specify the maximum number of entries that can be added to the local database the next time the controller reboots by entering this command:

config database size *max_entries*

Step 2 Save your changes by entering this command:

save config

Step 3 View the maximum number of database entries and the current database contents by entering this command:
show database summary



CHAPTER 43

Configuring Local Network Users on the Controller

- Local Network Users on Controller, on page 399
- Configuring Local Network Users for the Controller (GUI), on page 399
- Configuring Local Network Users for the Controller (CLI), on page 400

Local Network Users on Controller

You can add local network users to the local user database on the controller. The local user database stores the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP may use the local user database as its backend database to retrieve user credentials.

Note The controller passes client information to the RADIUS authentication server first. If the client information does not match a RADIUS database entry, the RADIUS authentication server replies with an authentication failure message. If the RADIUS authentication server does not reply, then the local user database is queried. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

This section contains the following subsections:

Configuring Local Network Users for the Controller (GUI)

Step 1 Choose **Security** > **AAA** > **Local Net Users** to open the Local Net Users page.

Note If you want to delete an existing user, hover your cursor over the blue drop-down arrow for that user and choose **Remove**.

Step 2 Perform one of the following:

- To edit an existing local network user, click the username for that user. The **Local Net Users > Edit** page appears.

- To add a local network user, click **New**. The **Local Net Users > New** page appears.

Step 3 If you are adding a new user, enter a username for the local user in the **User Name** text box. You can enter up to 49 alphanumeric characters.

Note Local network usernames must be unique because they are all stored in the same database.

Step 4 In the **Password** and **Confirm Password** text boxes, enter a password for the local user. You can enter up to 49 alphanumeric characters.

Step 5 If you are adding a new user, select the **Guest User** check box if you want to limit the amount of time that the user has access to the local network. The default setting is unselected.

Step 6 If you are adding a new user and you selected the **Guest User** check box, enter the amount of time (in seconds) that the guest user account is to remain active in the Lifetime text box. The valid range is 60 to 2,592,000 seconds (30 days) inclusive, and the default setting is 86,400 seconds.

Step 7 If you are adding a new user, you selected the **Guest User** check box, and you want to assign a QoS role to this guest user, select the **Guest User Role** check box. The default setting is unselected.

Note If you do not assign a QoS role to a guest user, the bandwidth contracts for this user are defined in the QoS profile for the WLAN.

Step 8 If you are adding a new user and you selected the **Guest User Role** check box, choose the QoS role that you want to assign to this guest user from the Role drop-down list.

Step 9 From the WLAN Profile drop-down list, choose the name of the WLAN that is to be accessed by the local user. If you choose **Any WLAN**, which is the default setting, the user can access any of the configured WLANs.

Step 10 In the **Description** text box, enter a descriptive title for the local user (such as "User 1").

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Configuring Local Network Users for the Controller (CLI)

Procedure

- Configure a local network user by entering these commands:
  - **config netuser add** *username password* **wlan** *wlan_id userType* **permanent description** *description*—Adds a permanent user to the local user database on the controller.
  - **config netuser add** *username password* {**wlan | guestlan**} {*wlan_id | guest_lan_id}* **userType guestlifetime** *seconds* **description** *description*—Adds a guest user on a WLAN or wired guest LAN to the local user database on the controller.

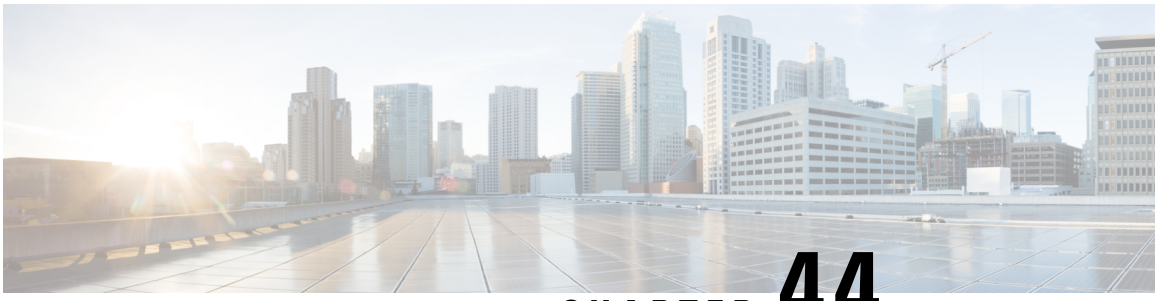
Note Instead of adding a permanent user or a guest user to the local user database from the controller, you can choose to create an entry on the RADIUS server for the user and enable RADIUS authentication for the WLAN on which web authentication is performed.

- **config netuser delete** *username*
  - *username*—Deletes a user from the local user database on the controller.

Note Local network usernames must be unique because they are all stored in the same database.

- See information related to the local network users configured on the controller by entering these commands:
  - **show netuser detail** *username*—Shows the configuration of a particular user in the local user database.
  - **show netuser summary**—Lists all the users in the local user database.
- Save your changes by entering this command:

  save config



CHAPTER 44

Configuring Password Policies

- Password Policies, on page 403
- Configuring Password Policies (GUI), on page 404
- Configuring Password Policies (CLI), on page 404

Password Policies

The password policies allows you to enforce strong password checks on newly created passwords for additional management users of controller and access point. The following are the requirements enforced on the new password:

- When the controller is upgraded from old version, all the old passwords are maintained as it is, even though the passwords are weak. After the system upgrade, if strong password checks are enabled, the same is enforced from that time and the strength of previously added passwords will not be checked or altered.
- Depending on the settings done in the Password Policy page, the local management and access point user configuration is affected.

Restrictions on Password Policies

- Strong password requirement based on WLAN-CC requirement is applicable only to WLAN admin login passwords and is not applicable to AP Management user passwords.
- The valid length of AP Management user passwords is minimum of 3 characters and maximum of 32 characters. Also, it is not possible to change the AP Management user password. Therefore, the restrictions of local net users for strong password does not apply to AP Management user passwords.
- Strong password: lockout feature is not applied if you try to access the controller through a serial connection or a terminal server connection and it has unlimited attempts.

This section contains the following subsections:

Configuring Password Policies (GUI)

Step 1 Choose **Security** > **AAA** > **Password Policies** to open the Password Policies page.

Step 2 Select the **Password must contain characters from at least 3 different classes** check box if you want your password to contain characters from at least three of the following classes: lower case letters, upper case letters, digits, and special characters.

Step 3 Select the **No character can be repeated more than 3 times consecutively** check box if you do not want character in the new password to repeat more than three times consecutively.

Step 4 Select the **Password cannot be the default words like cisco, admin** check box if you do not want the password to contain words such as Cisco, ocsic, admin, nimda, or any variant obtained by changing the capitalization of letters or by substituting 1, |, or! or substituting 0 for o or substituting $ for s.

Step 5 Select the **Password cannot contain username or reverse of username** check box if you do not want the password to contain a username or the reverse letters of a username.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Configuring Password Policies (CLI)

Procedure

- Enable or disable strong password check for AP and WLC by entering this command:

  config switchconfig strong-pwd {**case-check** | **consecutive-check** | **default-check** | **username-check** | **all-checks** | **position-check** | **case-digit-check**} {**enable** | **disable**}

  where

  - **case-check**—Checks the occurrence of same character thrice consecutively
  - **consecutive-check**—Checks the default values or its variants are being used.
  - **default-check**—Checks either username or its reverse is being used.
  - **all-checks**—Enables/disables all the strong password checks.
  - **position-check**—Checks four-character range from old password.
  - **case-digit-check**—Checks all four combinations to be present: lower, upper, digits, and special characters.

- Configure minimum number of upper, lower, digit, and special characters in a password by entering this command:

  config switchconfig strong-pwd minimum {**upper-case** | **lower-case** | **digits** | **special-chars**} *num-of-chars*

- Configure minimum length for a password by entering this command:

  config switchconfig strong-pwd min-length *pwd-length*

- Configure lockout for management or SNMPv3 users by entering this command:

config switchconfig strong-pwd lockout {**mgmtuser** | **snmpv3user**} {**enable** | **disable**}

- Configure lockout time for management or SNMPv3 users by entering this command:

  config switchconfig strong-pwd lockout time {**mgmtuser** | **snmpv3user**} *timeout-in-mins*

- Configure the number of consecutive failure attempts for management or SNMPv3 users by entering this command:

  config switchconfig strong-pwd lockout attempts {**mgmtuser** | **snmpv3user**} *num-of-failure-attempts*

- Configure lifetime for management or SNMPv3 users by entering this command:

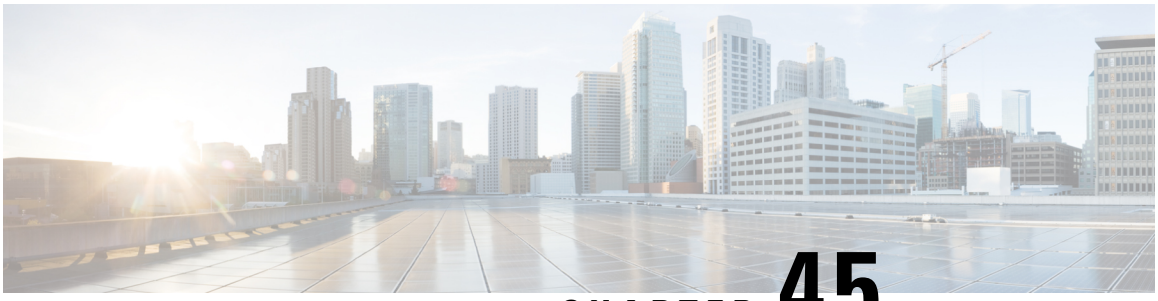
  config switchconfig strong-pwd lifetime {**mgmtuser** | **snmpv3user**} *lifetime-in-days*

- See the configured options for strong password check by entering this command:

  show switchconfig

  Information similar to the following appears:

```
802.3x Flow Control Mode..................... Disabled
FIPS prerequisite features................... Disabled
secret obfuscation........................... Enabled
Strong Password Check Features:

         case-check ...........Enabled
         consecutive-check ....Enabled
         default-check .......Enabled
         username-check ......Enabled
```



CHAPTER 45

Configuring LDAP

- LDAP, on page 407
- Configuring LDAP (GUI), on page 408
- Configuring LDAP (CLI), on page 410

LDAP

An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP may use an LDAP server as its backend database to retrieve user credentials.

Note From Release 8.0, IPv6 can also be used to configure the LDAP server on the controller.

Fallback LDAP Servers

The LDAP servers are configured on a WLAN for authentication. You require at least two LDAP servers to configure them for fallback behavior. A maximum of three LDAP servers can be configured for the fallback behavior per WLAN. The servers are listed in the priority order for authentication. If the first LDAP server becomes irresponsive, then the controller switches to the next LDAP server. If the second LDAP server becomes irresponsive, then the controller switches again to the third LDAP server.

The LDAP backend database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, EAP-FAST/EAP-GTC and PEAPv0/MSCHAPv2 are also supported, but only if the LDAP server is set up to return a clear-text password.

Controllers support Local EAP authentication against external LDAP databases such as Microsoft Active Directory and Novell's eDirectory. For more information about configuring the controller for Local EAP authentication against Novell's eDirectory, see the Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database whitepaper at http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112137-novell-edirectory-00.html

This section contains the following subsections:

Configuring LDAP (GUI)

Step 1 Choose **Security** > **AAA** > **LDAP** to open the LDAP Servers page.

- If you want to delete an existing LDAP server, hover your cursor over the blue drop-down arrow for that server and choose **Remove**.
- If you want to make sure that the controller can reach a particular server, hover your cursor over the blue drop-down arrow for that server and choose **Ping**.

Step 2 Perform one of the following:

- To edit an existing LDAP server, click the index number for that server. The **LDAP Servers > Edit** page appears.
- To add an LDAP server, click **New**. The **LDAP Servers > New** page appears. If you are adding a new server, choose a number from the Server Index (Priority) drop-down list to specify the priority order of this server in relation to any other configured LDAP servers. You can configure up to 17 servers. If the controller cannot reach the first server, it tries the second one in the list and so on.

Step 3 If you are adding a new server, enter the IP address of the LDAP server in the **Server IP Address** text box.

Note From Release 8.0, IPv6 can also be used to configure the LDAP server on the controller.

Step 4 If you are adding a new server, enter the LDAP server's TCP port number in the **Port Number** text box. The valid range is 1 to 65535, and the default value is 389.

Note Only LDAP port 389 is supported on Cisco WLC. No other ports are supported for LDAP.

Step 5 From the **Server Mode** drop-down list, choose **None**.

Step 6 Select the **Enable Server Status** check box to enable this LDAP server or unselect it to disable it. The default value is disabled.

Step 7 From the Simple Bind drop-down list, choose **Anonymous** or **Authenticated** to specify the local authentication bind method for the LDAP server. The Anonymous method allows anonymous access to the LDAP server. The Authenticated method requires that a username and password be entered to secure access. The default value is Anonymous.

Step 8 If you chose **Authenticated** in the previous step, follow these steps:

a) In the Bind Username text box, enter a username to be used for local authentication to the LDAP server. The username can contain up to 80 characters.

Note If the username starts with "cn=" (in lowercase letters), the controller assumes that the username includes the entire LDAP database path and does not append the user base DN. This designation allows the authenticated bind user to be outside the user base DN.

b) In the Bind Username text box, enter a username to be used for local authentication to the LDAP server. The username can contain up to 80 characters.

Step 9 In the User Base DN text box, enter the distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit, .ou=next organizational unit, and o=corporation.com. If the tree containing users is the base DN, type.

o=*corporation*.com

or

dc=*corporation***,dc=com**

Step 10 In the User Attribute text box, enter the name of the attribute in the user record that contains the username. You can obtain this attribute from your directory server.

Step 11 In the User Object Type text box, enter the value of the LDAP objectType attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user and some of which are shared with other object types.

Step 12 In the Server Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Step 13 Click **Apply** to commit your changes.

Step 14 Click **Save Configuration** to save your changes.

Step 15 Specify LDAP as the priority backend database server for local EAP authentication as follows:

a) Choose **Security** > **Local EAP** > **Authentication Priority** to open the Priority Order > Local-Auth page.
b) Highlight **LOCAL** and click **<** to move it to the left User Credentials box.
c) Highlight **LDAP** and click **>** to move it to the right User Credentials box. The database that appears at the top of the right User Credentials box is used when retrieving user credentials.

Note If both LDAP and LOCAL appear in the right User Credentials box with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If LOCAL is on the top, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

d) Click **Apply** to commit your changes.
e) Click **Save Configuration** to save your changes.

Step 16 (Optional) Assign specific LDAP servers to a WLAN as follows:

a) Choose **WLANs** to open the WLANs page.
b) Click the ID number of the desired WLAN.
c) When the WLANs > Edit page appears, choose the **Security** > **AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page.
d) From the LDAP Servers drop-down lists, choose the LDAP server(s) that you want to use with this WLAN. You can choose up to three LDAP servers, which are tried in priority order.

Note These LDAP servers apply only to WLANs with web authentication enabled. They are not used by local EAP.

e) Click **Apply** to commit your changes.
f) Click **Save Configuration** to save your changes.

Step 17 Specify the LDAP server fallback behavior, as follows:

a) Choose **WLAN** > **AAA Server** to open the Fallback Parameters page.
b) From the LDAP Servers drop-down list, choose the LDAP server in the order of priority when the controller attempts to authenticate management users. The order of authentication is from server.
c) Choose **Security** > **AAA** > **LDAP** to view the list of global LDAP servers configured for the controller.

Configuring LDAP (CLI)

Procedure

- Configure an LDAP server by entering these commands:
  - **config ldap add** *index server_ip_address port# user_base user_attr user_type* — Adds an LDAP server.
  - **config ldap delete** *index*—Deletes a previously added LDAP server.
  - **config ldap** {**enable** | **disable**} *index*—Enables or disables an LDAP server.
  - **config ldap simple-bind** {**anonymous** *index* | **authenticated** *index* **username** *username* **password** *password*}—Specifies the local authentication bind method for the LDAP server. The anonymous method allows anonymous access to the LDAP server whereas the authenticated method requires that a username and password be entered to secure access. The default value is anonymous. The username can contain up to 80 characters.

    If the username starts with "cn=" (in lowercase letters), the controller assumes that the username includes the entire LDAP database path and does not append the user base DN. This designation allows the authenticated bind user to be outside the user base DN.
  - **config ldap retransmit-timeout** *index timeout*—Configures the number of seconds between retransmissions for an LDAP server.
- Specify LDAP as the priority backend database server by entering this command:

  config local-auth user-credentials ldap

  If you enter the **config local-auth user-credentials ldap local command**, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If you enter the **config local-auth user-credentials local ldap command**, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.
- (Optional) Assign specific LDAP servers to a WLAN by entering these commands:
  - **config wlan ldap add** *wlan_id server_index*—Links a configured LDAP server to a WLAN.

    The LDAP servers specified in this command apply only to WLANs with web authentication enabled. They are not used by local EAP.
  - **config wlan ldap delete** *wlan_id* {*all* | *index*}—Deletes a specific or all configured LDAP server(s) from a WLAN.
- View information pertaining to configured LDAP servers by entering these commands:
  - **show ldap summary**—Shows a summary of the configured LDAP servers.

    ```
    Idx  Server Address   Port  Enabled
    ---  ---------------  ----  -------
    1    2.3.1.4           389     No
    2    10.10.20.22       389     Yes
    ```
  - **show ldap** *index*—Shows detailed LDAP server information. Information like the following appears:

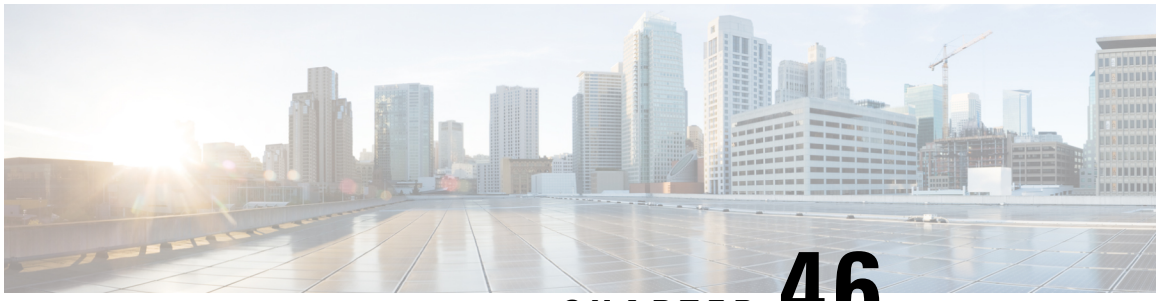
```
Server Index..................................... 2
Address.......................................... 10.10.20.22
Port............................................. 389
Enabled.......................................... Yes
User DN.......................................... ou=active,ou=employees,ou=people,

            o=cisco.com
User Attribute................................... uid
User Type........................................ Person
Retransmit Timeout............................... 2 seconds
Bind Method ..................................... Authenticated
Bind Username.................................... user1
```

- **show ldap statistics**—Shows LDAP server statistics.

```
Server Index..................................... 1
Server statistics:
  Initialized OK................................. 0
  Initialization failed.......................... 0
  Initialization retries......................... 0
  Closed OK...................................... 0
Request statistics:
  Received....................................... 0
  Sent........................................... 0
  OK............................................. 0
  Success........................................ 0
  Authentication failed.......................... 0
  Server not found............................... 0
  No received attributes......................... 0
  No passed username............................. 0
  Not connected to server........................ 0
  Internal error................................. 0
  Retries........................................ 0

Server Index..................................... 2
..
```

- **show wlan** *wlan_id*—Shows the LDAP servers that are applied to a WLAN.

- Make sure the controller can reach the LDAP server by entering this command:
  ping *server_ip_address*
- Save your changes by entering this command:
  save config
- Enable or disable debugging for LDAP by entering this command:
  debug aaa ldap {**enable** | **disable**}



CHAPTER 46

Configuring Local EAP

- Local EAP, on page 413
- Restrictions for Local EAP, on page 414
- Configuring Local EAP (GUI), on page 415
- Configuring Local EAP (CLI), on page 418

Local EAP

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, which removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the controller and wireless clients.

Note The LDAP backend database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are also supported but only if the LDAP server is set up to return a clear-text password.

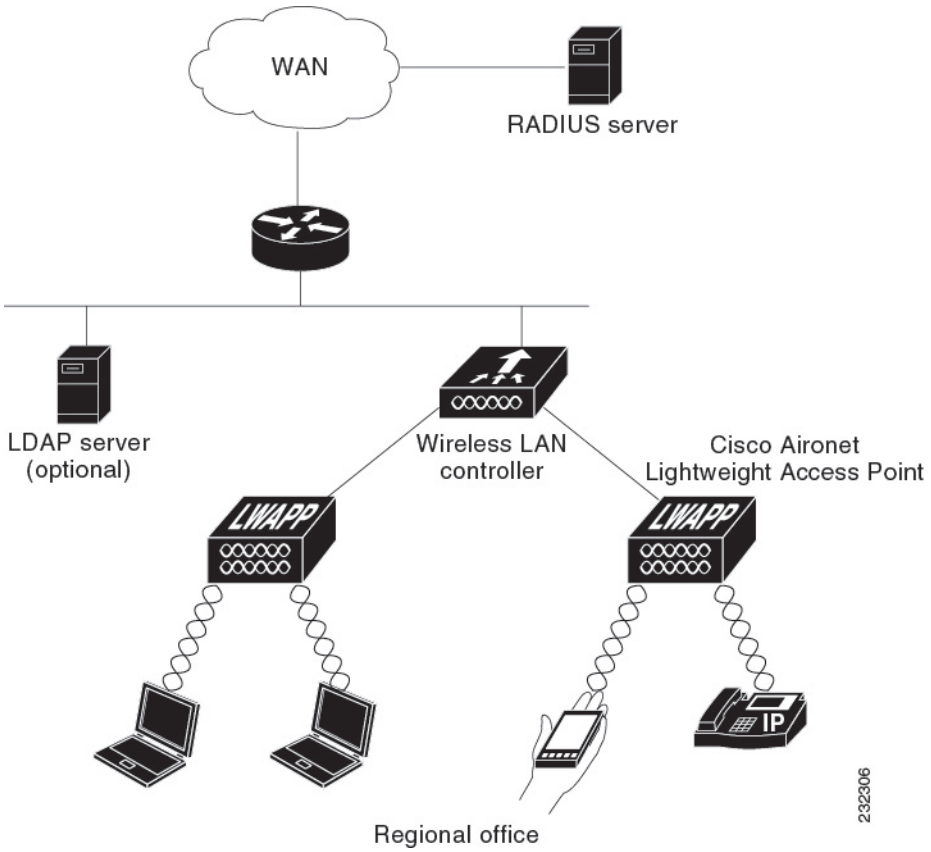
Note Cisco wireless LAN controllers support Local EAP authentication against external LDAP databases such as Microsoft Active Directory and Novell's eDirectory. For more information about configuring the controller for Local EAP authentication against Novell's eDirectory, see the Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database whitepaper at http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112137-novell-edirectory-00.html

Note Local authentication with certificates of second level hierarchy (CA + intermediate CA + device) is not supported.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP. If you never want the controller to try to authenticate clients using an external RADIUS server, enter these CLI commands in this order:

- **config wlan disable** *wlan_id*
- **config wlan radius_server auth disable** *wlan_id*
- **config wlan enable** *wlan_id*

Figure 38: Local EAP Example



This section contains the following subsections:

Restrictions for Local EAP

- In Release 8.6 and later releases, legacy clients that require RC4 or 3DES encryption types are not supported in Local EAP authentication.

Configuring Local EAP (GUI)

Before you begin

Note EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC use certificates for authentication, and EAP-FAST uses either certificates or PACs. The controller is shipped with Cisco-installed device and Certificate Authority (CA) certificates. However, if you want to use your own vendor-specific certificates, they must be imported on the controller.

Step 1 If you are configuring local EAP to use one of the EAP types listed in the note above, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller.

Step 2 If you want the controller to retrieve user credentials from the local user database, make sure that you have properly configured the local network users on the controller.

Step 3 If you want the controller to retrieve user credentials from an LDAP backend database, make sure that you have properly configured an LDAP server on the controller.

Step 4 Specify the order in which user credentials are retrieved from the backend database servers as follows:

a) Choose **Security** > **Local EAP** > **Authentication Priority** to open the **Priority Order > Local-Auth** page.

b) Determine the priority order in which user credentials are to be retrieved from the local and/or LDAP databases. For example, you may want the LDAP database to be given priority over the local user database, or you may not want the LDAP database to be considered at all.

c) When you have decided on a priority order, highlight the desired database. Then use the left and right arrows and the Up and Down buttons to move the desired database to the top of the right User Credentials box.

Note If both LDAP and LOCAL appear in the right User Credentials box with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If LOCAL is on the top, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

d) Click **Apply** to commit your changes.

Step 5 Specify values for the local EAP timers as follows:

a) Choose **Security** > **Local EAP** > **General** to open the General page.

b) In the **Local Auth Active Timeout** text box, enter the amount of time (in seconds) in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails. The valid range is 1 to 3600 seconds, and the default setting is 300 seconds.

Step 6 Specify values for the Advanced EAP parameters as follows:

a) Choose **Security**> **Advanced EAP**.

b) In the **Identity Request Timeout** text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.

c) In the **Identity Request Max Retries** text box, enter the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.

d) In the **Dynamic WEP Key Index** text box, enter the key index used for dynamic wired equivalent privacy (WEP). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).

e) In the **Request Timeout** text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.

f) In the **Request Max Retries** text box, enter the maximum number of times that the controller attempts to retransmit the EAP request to wireless clients using local EAP. The valid range is 1 to 120 retries, and the default setting is 2 retries.

g) From the **Max-Login Ignore Identity Response** drop-down list, choose **Enable** to limit the number of devices that can be connected to the controller with the same username. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same controller. The default value is enabled.

h) In the **EAPOL-Key Timeout** text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 1 to 5 seconds, and the default setting is 1 second.

Note If the controller and access point are separated by a WAN link, the default timeout of 1 second may not be sufficient.

i) In the **EAPOL-Key Max** Retries text box, enter the maximum number of times that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.

j) In the **EAP-Broadcast Key Interval** text box, enter the interval between the Group Temporal Key (GTK) key rotation for all the stations on a BSSID that is using WPA protocol. The default interval is 3600 seconds.

k) Click **Apply** to commit your changes.

Step 7 Create a local EAP profile, which specifies the EAP authentication types that are supported on the wireless clients as follows:

a) Choose **Security** > **Local EAP** > **Profiles** to open the Local EAP Profiles page.

This page lists any local EAP profiles that have already been configured and specifies their EAP types. You can create up to 16 local EAP profiles.

Note If you want to delete an existing profile, hover your cursor over the blue drop-down arrow for that profile and choose **Remove**.

b) Click **New** to open the **Local EAP Profiles > New** page.

c) In the Profile Name text box, enter a name for your new profile and then click **Apply**.

Note You can enter up to 63 alphanumeric characters for the profile name. Make sure not to include spaces.

d) When the Local EAP Profiles page reappears, click the name of your new profile. The **Local EAP Profiles > Edit** page appears.

e) Select the **LEAP**, **EAP-FAST**, **EAP-TLS,** and/or **PEAP** check boxes to specify the EAP type that can be used for local authentication.

Note You can specify more than one EAP type per profile. However, if you choose multiple EAP types that use certificates (such as EAP-FAST with certificates, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC), all the EAP types must use the same certificate (from either Cisco or another vendor).

Note If you select the **PEAP** check box, both PEAPv0/MSCHAPv2 or PEAPv1/GTC are enabled on the controller.

f) If you chose EAP-FAST and want the device certificate on the controller to be used for authentication, select the **Local Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected, which is the default setting.

Note This option applies only to EAP-FAST because device certificates are not used with LEAP and are mandatory for EAP-TLS and PEAP.

g) If you chose EAP-FAST and want the wireless clients to send their device certificates to the controller in order to authenticate, select the **Client Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected, which is the default setting.

Note This option applies only to EAP-FAST because client certificates are not used with LEAP or PEAP and are mandatory for EAP-TLS.

h) If you chose EAP-FAST with certificates, EAP-TLS, or PEAP, choose which certificates will be sent to the client, the ones from **Cisco** or the ones from another **Vendor**, from the Certificate Issuer drop-down list. The default setting is Cisco.

i) If you chose EAP-FAST with certificates or EAP-TLS and want the incoming certificate from the client to be validated against the CA certificates on the controller, select the **Check against CA certificates** check box. The default setting is enabled.

j) If you chose EAP-FAST with certificates or EAP-TLS and want the common name (CN) in the incoming certificate to be validated against the Local Net Users configured on the controller, select the **Verify Certificate CN Identity** check box. The default setting is disabled.

k) If you chose EAP-FAST with certificates or EAP-TLS and want the controller to verify that the incoming device certificate is still valid and has not expired, select the **Check Certificate Date Validity** check box. The default setting is enabled.

Note Certificate date validity is checked against the current UTC (GMT) time that is configured on the controller. Timezone offset will be ignored.

l) Click **Apply** to commit your changes.

Step 8 If you created an EAP-FAST profile, follow these steps to configure the EAP-FAST parameters:

a) Choose **Security** > **Local EAP** > **EAP-FAST Parameters** to open the EAP-FAST Method Parameters page.

b) In the Server Key and Confirm Server Key text boxes, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.

c) In the Time to Live for the PAC text box, enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.

d) In the Authority ID text box, enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.

e) In the Authority ID Information text box, enter the authority identifier of the local EAP-FAST server in text format.

f) If you want to enable anonymous provisioning, select the **Anonymous Provision** check box. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACS must be manually provisioned. The default setting is enabled.

Note If the local and/or client certificates are required and you want to force all EAP-FAST clients to use certificates, unselect the **Anonymous Provision** check box.

g) Click **Apply** to commit your changes.

Step 9 Enable local EAP on a WLAN as follows:

a) Choose **WLANs** to open the WLANs page.

b) Click the ID number of the desired WLAN.

c) When the **WLANs > Edit** page appears, choose the **Security** > **AAA Servers** tabs to open the **WLANs > Edit (Security > AAA Servers)** page.

d) Unselect the **Enabled** check boxes for Radius Authentication Servers and Accounting Server to disable RADIUS accounting and authentication for this WLAN.

e) Select the **Local EAP Authentication** check box to enable local EAP for this WLAN.
f) From the EAP Profile Name drop-down list, choose the EAP profile that you want to use for this WLAN.
g) If desired, choose the LDAP server that you want to use with local EAP on this WLAN from the **LDAP Servers** drop-down lists.
h) Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring Local EAP (CLI)

Before you begin

Note EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC use certificates for authentication, and EAP-FAST uses either certificates or PACbs. The controller is shipped with Cisco-installed device and Certificate Authority (CA) certificates. However, if you want to use your own vendor-specific certificates, they must be imported on the controller.

Step 1 If you are configuring local EAP to use one of the EAP types listed in the note above, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller.

Step 2 If you want the controller to retrieve user credentials from the local user database, make sure that you have properly configured the local network users on the controller.

Step 3 If you want the controller to retrieve user credentials from an LDAP backend database, make sure that you have properly configured an LDAP server on the controller.

Step 4 Specify the order in which user credentials are retrieved from the local and/or LDAP databases by entering this command:

config local-auth user-credentials {*local* | *ldap*}

Note If you enter the **config local-auth user-credentials ldap local** command, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If you enter the **config local-auth user-credentials local ldap command**, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.

Step 5 Specify values for the local EAP timers by entering these commands:

- **config local-auth active-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails. The valid range is 1 to 3600 seconds, and the default setting is 100 seconds.
- **config advanced eap identity-request-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
- **config advanced eap identity-request-retries** *retries*—Specifies the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients using local EAP. The valid range is 1 to 20 retries, and the default setting is 20 retries.

- **config advanced eap key-index** *index*—Specifies the key index used for dynamic wired equivalent privacy (WEP). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).
- **config advanced eap request-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
- **config advanced eap request-retries** *retries*—Specifies the maximum number of times that the controller attempts to retransmit the EAP request to wireless clients using local EAP. The valid range is 1 to 120 retries, and the default setting is 20 retries.
- **config advanced eap eapol-key-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 1 to 5 seconds, and the default setting is 1 second.

  Note If the controller and access point are separated by a WAN link, the default timeout of 1 second may not be sufficient.

- **config advanced eap eapol-key-retries** *retries*—Specifies the maximum number of times that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.
- **config advanced eap max-login-ignore-identity-response** {**enable** | **disable**}—When enabled, this command ignores the limit set for the number of devices that can be connected to the controller with the same username through 802.1x authentication. When disabled, this command limits the number of devices that can be connected to the controller with the same username. This is not applicable for web authentication users. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same controller. The default value is enabled. Use the command **config netuser maxUserLogin** to set the limit of maximum number of devices per same username.

Step 6 Create a local EAP profile by entering this command:

config local-auth eap-profile add *profile_name*

Note Do not include spaces within the profile name.

Note To delete a local EAP profile, enter the **config local-auth eap-profile delete** *profile_name* command.

Step 7 Add an EAP method to a local EAP profile by entering this command:

config local-auth eap-profile method add *method profile_name*

The supported methods are leap, fast, tls, and peap.

Note If you choose peap, both P EAPv0/MSCHAPv2 or PEAPv1/GTC are enabled on the controller.

Note You can specify more than one EAP type per profile. However, if you create a profile with multiple EAP types that use certificates (such as EAP-FAST with certificates, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC), all of the EAP types must use the same certificate (from either Cisco or another vendor).

Note To delete an EAP method from a local EAP profile, enter the **config local-auth eap-profile method delete** *method profile_name* command.

Step 8 Configure EAP-FAST parameters if you created an EAP-FAST profile by entering this command:

config local-auth method fast *?*

where *?* is one of the following:

- **anon-prov** {**enable** | **disable**}—Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during PAC provisioning.

- **authority-id** *auth_id*—Specifies the authority identifier of the local EAP-FAST server.
- **pac-ttl** *days*—Specifies the number of days for the PAC to remain viable.
- **server-key** *key*—Specifies the server key used to encrypt and decrypt PACs.

Step 9 Configure certificate parameters per profile by entering these commands:

- **config local-auth eap-profile method fast local-cert** {**enable** | **disable**} *profile_name*— Specifies whether the device certificate on the controller is required for authentication.

  Note This command applies only to EAP-FAST because device certificates are not used with LEAP and are mandatory for EAP-TLS and PEAP.

- **config local-auth eap-profile method fast client-cert** {**enable** | **disable**} *profile_name*— Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.

  Note This command applies only to EAP-FAST because client certificates are not used with LEAP or PEAP and are mandatory for EAP-TLS.

- **config local-auth eap-profile cert-issuer** {**cisco** | **vendor**} *profile_name*—If you specified EAP-FAST with certificates, EAP-TLS, or PEAP, specifies whether the certificates that will be sent to the client are from Cisco or another vendor.
- **config local-auth eap-profile cert-verify ca-issuer** {**enable** | **disable**} *profile_name*—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the incoming certificate from the client is to be validated against the CA certificates on the controller.
- **config local-auth eap-profile cert-verify cn-verify** {**enable** | **disable**} *profile_name*—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
- **config local-auth eap-profile cert-verify date-valid** {**enable** | **disable**} *profile_name*—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

Step 10 Enable local EAP and attach an EAP profile to a WLAN by entering this command:

config wlan local-auth enable *profile_name wlan_id*

Note To disable local EAP for a WLAN, enter the **config wlan local-auth disable** *wlan_id command.*

Step 11 Save your changes by entering this command:

save config

Step 12 View information pertaining to local EAP by entering these commands:

- **show local-auth config—**Shows the local EAP configuration on the controller.

```
User credentials database search order:
   Primary ..................................... Local DB

Timer:
    Active timeout ............................. 300

Configured EAP profiles:
   Name ........................................ fast-cert
     Certificate issuer ....................... vendor
     Peer verification options:
```

```
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. Yes
        Client certificate required ............. Yes
      Enabled methods ........................... fast
      Configured on WLANs ....................... 1

   Name ..................................... tls
     Certificate issuer ....................... vendor
     Peer verification options:
       Check against CA certificates ........... Enabled
       Verify certificate CN identity .......... Disabled
       Check certificate date validity ......... Enabled
     EAP-FAST configuration:
       Local certificate required .............. No
       Client certificate required ............. No
     Enabled methods ........................... tls
     Configured on WLANs ....................... 2

EAP Method configuration:
   Low-Cipher Support(TLSv1.0 for local EAP)..... Enabled
   EAP-FAST:
     Server key ................................ <hidden>
     TTL for the PAC ........................... 10
     Anonymous provision allowed ............... Yes
     Accept client on auth prov ................ No
     Authority ID .............................. 436973636f00000000000000000000000000
     Authority Information ..................... Cisco A-ID
```

- **show local-auth statistics**—Shows the local EAP statistics.
- **show local-auth certificates**—Shows the certificates available for local EAP.
- **show local-auth user-credentials**—Shows the priority order that the controller uses when retrieving user credentials from the local and/or LDAP databases.
- **show advanced eap**—Shows the timer values for local EAP.

```
EAP-Identity-Request Timeout (seconds)........... 1
EAP-Identity-Request Max Retries................. 20
EAP Key-Index for Dynamic WEP.................... 0
EAP Max-Login Ignore Identity Response........... enable
EAP-Request Timeout (seconds).................... 20
EAP-Request Max Retries.......................... 20
EAPOL-Key Timeout (seconds)...................... 1
EAPOL-Key Max Retries........................... 2
```

- **show ap stats wlan** *Cisco_AP*—Shows the EAP timeout and failure counters for a specific access point for each WLAN.
- **show client detail** *client_mac*—Shows the EAP timeout and failure counters for a specific associated client. These statistics are useful in troubleshooting client association issues.

```
...
Client Statistics:
      Number of Bytes Received................... 10
      Number of Bytes Sent....................... 10
      Number of Packets Received................. 2
      Number of Packets Sent..................... 2
      Number of EAP Id Request Msg Timeouts...... 0
      Number of EAP Id Request Msg Failures...... 0
      Number of EAP Request Msg Timeouts......... 2
```

```
Number of EAP Request Msg Failures..... 1
Number of EAP Key Msg Timeouts............ 0
Number of EAP Key Msg Failures............ 0
Number of Policy Errors................... 0
Radio Signal Strength Indicator........... Unavailable
Signal to Noise Ratio..................... Unavailable
```

- **show wlan** *wlan_id*—Shows the status of local EAP on a particular WLAN.

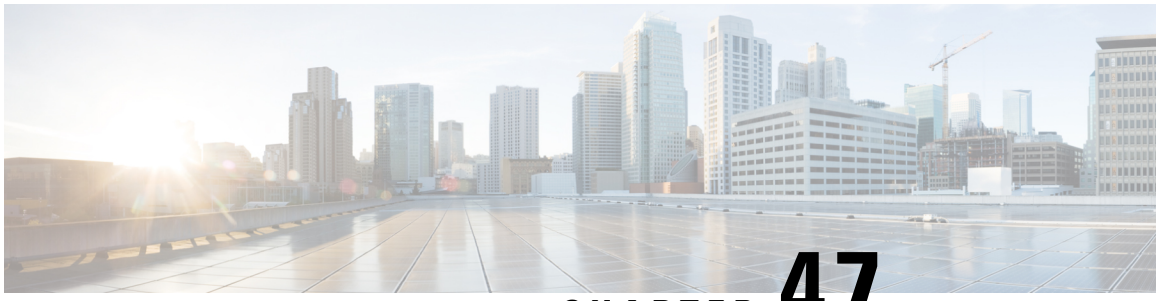
Step 13 (Optional) Troubleshoot local EAP sessions by entering these commands:

- **debug aaa local-auth eap method** {**all** | **errors** | **events** | **packets** | **sm**} {*enable* | *disable*}— Enables or disables debugging of local EAP methods.
- **debug aaa local-auth eap framework** {**all** | **errors** | **events** | **packets** | **sm**} {*enable* | *disable*}— Enables or disables debugging of the local EAP framework.

  Note In these two debug commands, **sm** is the state machine.

- **clear stats local-auth**—Clears the local EAP counters.
- **clear stats ap wlan** *Cisco_AP*—Clears the EAP timeout and failure counters for a specific access point for each WLAN.

```
WLAN      1
   EAP Id Request Msg Timeouts.................... 0
   EAP Id Request Msg Timeouts Failures.......... 0
   EAP Request Msg Timeouts....................... 2
   EAP Request Msg Timeouts Failures.............. 1
   EAP Key Msg Timeouts........................... 0
   EAP Key Msg Timeouts Failures.................. 0
WLAN      2
   EAP Id Request Msg Timeouts.................... 1
   EAP Id Request Msg Timeouts Failures.......... 0
   EAP Request Msg Timeouts....................... 0
   EAP Request Msg Timeouts Failures.............. 0
   EAP Key Msg Timeouts........................... 3
EAP Key Msg Timeouts Failures.............. 1
```



CHAPTER 47

Configuring the System for SpectraLink NetLink Telephones

- Information About SpectraLink NetLink Telephones, on page 423
- Configuring SpectraLink NetLink Phones, on page 423

Information About SpectraLink NetLink Telephones

For the best integration with the Cisco UWN solution, SpectraLink NetLink Telephones require an extra operating system configuration step: **enable long preambles**. The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

Configuring SpectraLink NetLink Phones

Enabling Long Preambles (GUI)

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

Step 2 If the **Short Preamble** check box is selected, continue with this procedure. However, if the Short Preamble check box is unselected (which means that long preambles are enabled), the controller is already optimized for SpectraLink NetLink phones and you do not need to continue this procedure.

Step 3 Unselect the **Short Preamble** check box to enable long preambles.

Step 4 Click **Apply** to update the controller configuration.

Note If you do not already have an active CLI session to the controller, we recommend that you start a CLI session to reboot the controller and watch the reboot process. A CLI session is also useful because the GUI loses its connection when the controller reboots.

Step 5 Choose **Commands** > **Reboot** > **Reboot > Save and Reboot to reboot the controller**. Click OK in response to this prompt:

```
Configuration will be saved and the controller will be rebooted. Click ok to confirm.
```

The controller reboots.

Step 6 Log back onto the controller GUI to verify that the controller is properly configured.

Step 7 Choose **Wireless** > **802.11b/g/n** > **Network** to open the 802.11b/g Global Parameters page. If the **Short Preamble** check box is unselected, the controller is optimized for SpectraLink NetLink phones.

Enabling Long Preambles (CLI)

Step 1 Log on to the controller CLI.

Step 2 Enter the show 802.11b command and select the Short preamble mandatory parameter. If the parameter indicates that short preambles are enabled, continue with this procedure. This example shows that short preambles are enabled:

```
Short Preamble mandatory..................... Enabled
```

However, if the parameter shows that short preambles are disabled (which means that long preambles are enabled), the controller is already optimized for SpectraLink NetLink phones and you do not need to continue this procedure.

Step 3 Disable the 802.11b/g network by entering this command:

config 802.11b disable *network*

You cannot enable long preambles on the 802.11a network.

Step 4 Enable long preambles by entering this command:

config 802.11b preamble *long*

Step 5 Reenable the 802.11b/g network by entering this command:

config 802.11b *enable network*

Step 6 Enter the reset system command to reboot the controller. Enter y when the prompt to save the system changes is displayed. The controller reboots.

Step 7 Verify that the controller is properly configured by logging back into the CLI and entering the show 802.11b command to view these parameters:

```
802.11b Network.............................. Enabled
Short Preamble mandatory..................... Disabled
```

These parameters show that the 802.11b/g network is enabled and that short preambles are disabled.

Configuring Enhanced Distributed Channel Access (CLI)

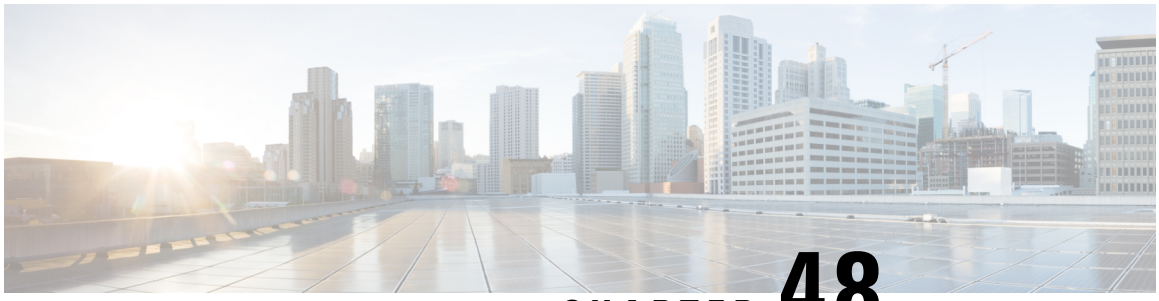
To configure 802.11 enhanced distributed channel access (EDCA) parameters to support SpectraLink phones, use the following CLI commands:

config advanced edca-parameter {**custom-voice** | **optimized-video-voice** | **optimized-voice** | **svp-voice** | **wmm-default**}

where

- **custom-voice** enables custom voice EDCA parameters
- **optimized-video-voice** enables combined video-voice-optimized parameters
- **optimized-voice** enables non-SpectraLink voice-optimized parameters
- **svp-voice** enables SpectraLink voice priority (SVP) parameters
- **wmm-default** enables wireless multimedia (WMM) default parameters

Note To propagate this command to all access points connected to the controller, make sure to disable and then reenable the 802.11b/g network after entering this command.



CHAPTER 48

Configuring RADIUS NAC Support

- ISE NAC Support, on page 427
- Guidelines and Restrictions on ISE NAC Support, on page 429
- Configuring ISE NAC Support (GUI), on page 430
- Configuring ISE NAC Support (CLI), on page 430

ISE NAC Support

The Cisco Identity Services Engine (ISE) is a next-generation, context-based access control solution that provides the functions of Cisco Secure Access Control System (ACS) and Cisco Network Admission Control (NAC) in one integrated platform.

Cisco ISE was introduced in Cisco Wireless Release 7.0.116.0. Cisco ISE can be used to provide advanced security for your deployed network. It is an authentication server that you can configure on your controller. When a client associates with a controller on a ISE NAC–enabled WLAN with OPEN/Layer 2 + MAC Filtering, the controller forwards the request to the Cisco ISE server without verifying in the local database.

Note ISE NAC was previously known as RADIUS NAC.

This section contains the following subsections:

Device Registration

Device registration enables you to authenticate and provision new devices on the WLAN with RADIUS NAC enabled. When a device is registered on the WLAN, it can use the network based on the configured ACL.

Central Web Authentication

In the case of Central Web Authentication (CWA), web authentication occurs on the Cisco ISE server. The web portal in the Cisco ISE server provides a login page to a client. After the credentials are verified on the Cisco ISE server, the client is provisioned. The client remains in the POSTURE_REQD state until a change of authorization (CoA) is reached. The credentials and ACLs are received from the Cisco ISE server.

Note In a CWA and MAC filtering configuration scenario, if a change in VLAN occurs during pre-authentication and post-authentication, dissociation request is sent to clients and the clients are forced to go through DHCP again.

For new clients, the RADIUS access accept message carries redirected URL for port 80 and pre-auth ACLs or quarantine VLAN. Definition of ACL is defined in the controller (IP addresses and ports).

Clients will be redirected to the URL provided in the access accept message and put into a new state until posture validation is done. Clients in this state validate themselves against ISE server and the policies configured on the ISE NAC server.

The NAC agent on the clients initiates posture validation (traffic to port 80): The agent sends HTTP discovery request to port 80, which the controller redirects to the URL provided in the access accept message. Cisco ISE knows that the client is trying to reach and responds directly to the client. This way, the client learns about the Cisco ISE IP address and from now on, the client talks directly with the Cisco ISE.

The controller allows this traffic because the ACL is configured to allow this traffic. In case of VLAN override, the traffic is bridged so that it reaches the Cisco ISE.

ISE NAC

After the client completes the assessment, a RADIUS CoA-Req with reauth service is sent to the controller. This initiates reauthentication of the client (by sending EAP-START). Once reauthentication succeeds, the Cisco ISE sends an access accept message with a new ACL (if any) and no URL redirect, or access VLAN.

The controller has support for CoA-Req and Disconnect-Req as per RFC 3576. The controller needs to support CoA-Req for re-auth service, as per RFC 5176.

Instead of downloadable ACLs, pre-configured ACLs are used on the controller. Cisco ISE sends the ACL name, which is already configured in the controller.

This design should work for both VLAN and ACL cases. In case of VLAN override, the port 80 is redirected and allows (bridge) rest of the traffic on the quarantine VLAN. For the ACL, the pre-auth ACL received in the access accept message is applied.

Here's the workflow:

1. The guest user associates with the controller.
2. The controller sends a MAB Request to ISE.
3. ISE matches the first authorization rules, and sends the redirect parameters (ACL and URL).
4. The controller redirects the GUEST to ISE.
5. After the guest is authenticated, ISE makes a second authorization, which is called RADIUS Change of Authorization (CoA). In this second authorization, a profile must be returned so that the guest is permitted access to the network. We can use usecase: guestflow to easily match this second authorization.

Local Web Authentication

Local web authentication is not supported for RADIUS NAC.

This table describes the possible combinations in a typical ISE deployment with Device Registration, CWA and LWA enabled:

Table 16: ISE Network Authentication Flow

WLAN Configuration	CWA	LWA	Device Registration
RADIUS NAC Enabled	Yes	No	Yes
L2 PSK	802.1X	PSK, Static WEP, CKIP	No
L3 None	N/A	Internal/External	N/A
MAC Filtering Enabled	Yes	No	Yes

Guidelines and Restrictions on ISE NAC Support

Guidelines

- When a client moves from one WLAN to another, the Cisco WLC retains the client's audit session ID if it returns to the WLAN before the idle timeout occurs. As a result, when the client associates with the Cisco WLC before the idle timeout session expires, it is immediately moved to Run state. The client is validated if it reassociates with the Cisco WLC after the session timeout.
- If you have two WLANs, and WLAN 1 is configured on a Cisco WLC (WLC1) and WLAN2 is configured on another Cisco WLC (WLC2) and both are ISE NAC enabled, the client first connects to WLC1 and moves to the RUN state after posture validation. Assume that the client now moves to WLC2. If the client connects back to WLC1 before the PMK expires for this client in WLC1, the posture validation is skipped for the client. The client directly moves to Run state by passing posture validation because the Cisco WLC retains the old audit session ID for the client that is already known to Cisco ISE.
- When deploying ISE NAC in your wireless network, do not configure a primary and secondary Cisco ISE server. Instead, we recommend that you configure High Availability (HA) between the two Cisco ISE servers. Having a primary and secondary ISE setup will require posture validation to occur before the clients move to the Run state. If HA is configured, the client is automatically moved to the Run state in the fallback Cisco ISE server.
- Do not swap AAA server indexes in a live network because clients might get disconnected and have to reconnect to the RADIUS server, which might result in log messages to be appended to the ISE server logs.
- Enable AAA override on the WLAN to use ISE NAC.
- ISE NAC is supported with open authentication/Layer 2 (PSK/802.1x) + MAC Filtering security types.
- During slow roaming, clients go through posture validation.
- If the AAA url-redirect-acl and url-redirect attributes are expected from the AAA server, the AAA override feature must be enabled on the controller.

Restrictions

- For ISE NAC WLANs, the MAC authentication request is always sent to the external RADIUS server. The MAC authentication is not validated against the local database. This functionality is applicable to Releases 8.5, 8.7, 8.8, and later releases via the fix for CSCvh85830.
- The ISE NAC functionality does not work if the configured accounting server is different from the authentication (Cisco ISE) server. You should configure the same server as the authentication and accounting server if Cisco ISE functionalities are used. If Cisco ISE is used only for Cisco ACS functionality, the accounting server can be flexible.
- The controller software configured with ISE NAC does not support a CoA on the service port.
- Guest tunneling mobility is supported only for ISE NAC–enabled WLANs.
- VLAN select is not supported.
- Workgroup bridges are not supported.
- The AP Group over NAC is not supported in ISE NAC.
- When ISE NAC is enabled, the RADIUS server overwrite interface is not supported.
- Audit session ID is not supported across mobility domains if the controller belongs to a different mobility domain.

Configuring ISE NAC Support (GUI)

Step 1 Choose **WLANs**.

Step 2 Click the WLAN ID.

The **WLANs > Edit** page appears.

Step 3 Click the **Advanced** tab.

Step 4 From the **NAC State** drop-down list, choose from the following options:

- **None**
- **SNMP NAC**—Uses SNMP NAC for the WLAN.
- **ISE NAC**—Uses ISE NAC for the WLAN.

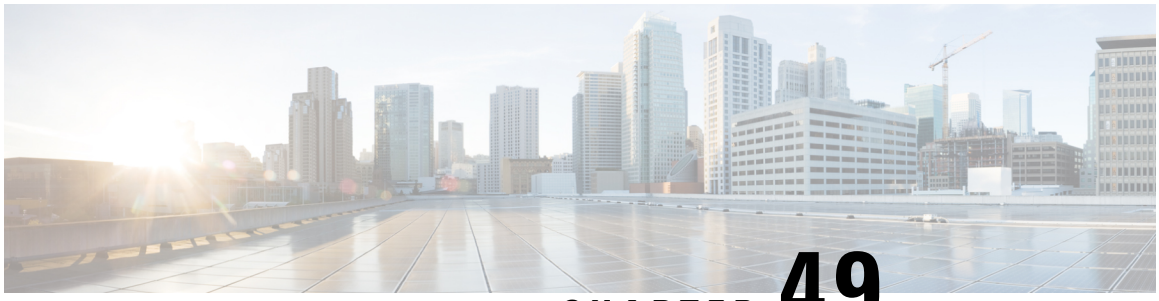
Note AAA override is automatically enabled when you use ISE NAC on a WLAN.

Step 5 Save the configuration.

Configuring ISE NAC Support (CLI)

Enter the following command:

config wlan nac radius {**enable** | **disable**} *wlan_id*



CHAPTER 49

Using Management Over Wireless

- Management over Wireless, on page 431
- Enabling Management over Wireless (GUI), on page 431
- Enabling Management over Wireless (CLI), on page 432

Management over Wireless

The management over wireless feature allows you to monitor and configure local controllers using a wireless client. This feature is supported for all management tasks except uploads to and downloads from (transfers to and from) the controller.

This feature blocks wireless management access to the same controller that the wireless client device is currently associated with. It does not prevent management access for a wireless client associated with another controller entirely. To completely block manabgement access to wireless clients based on VLAN and so on, we recommend that you use access control lists (ACLs) or similar mechanism.

Restrictions on Management over Wireless

- Management over Wireless can be disabled only if clients are on central switching.
- Management over Wireless is not supported for FlexConnect local switching clients. However, Management over Wireless works for non-web authentication clients if you have a route to the controller from the FlexConnect site.

This section contains the following subsections:

Enabling Management over Wireless (GUI)

Step 1 Choose **Management > Mgmt Via Wireless** to open the **Management Via Wireless** page.

Step 2 Check the **Enable Controller Management to be accessible from Wireless Clients** check box to enable management over wireless for the WLAN or unselect it to disable this feature. By default, it is in disabled state.

Step 3 Save the configuration.

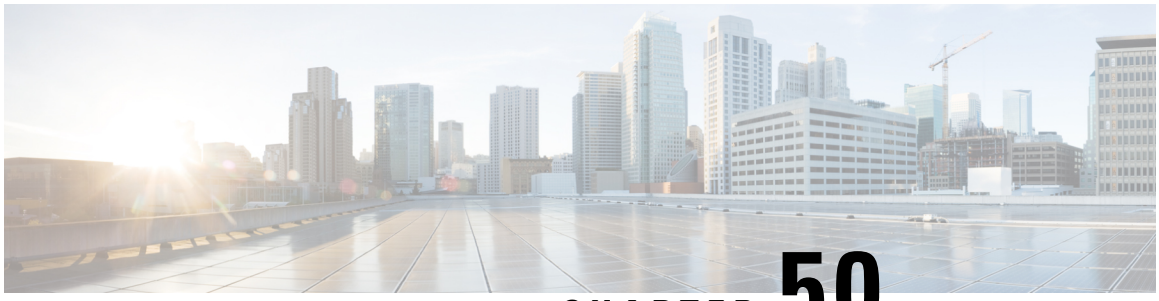
Enabling Management over Wireless (CLI)

Step 1 Verify whether the management over wireless interface is enabled or disabled by entering this command:

show network summary

- If disabled: Enable management over wireless by entering this command:**config network mgmt-via-wireless** *enable*
- Otherwise, use a wireless client to associate with an access point connected to the controller that you want to manage.

Step 2 Log into the CLI to verify that you can manage the WLAN using a wireless client by entering this command:
telnet *wlc-ip-addr CLI-command*



CHAPTER 50

Using Dynamic Interfaces for Management

- Using Dynamic Interfaces for Management, on page 433
- Configuring Management using Dynamic Interfaces (CLI), on page 434

Using Dynamic Interfaces for Management

You can access the controller with one of its dynamic interface IP addresses. Both the wired and wireless clients can access the dynamic interface of the controller using the CLI and GUI. To access the GUI of the controller enter the dynamic interface IP address of the controller in the address field of either Internet Explorer or Mozilla Firefox browser. For wired clients, you must enable management of dynamic interface and must ensure that the wired client is in the VLAN that is mapped to the dynamic interface.

A device, when the management using dynamic interfaces is disabled, can open an SSH connection, if the protocol is enabled. However, you are not prompted to log on. Additionally, the management address remains accessible from a dynamic interface VLAN, unless a CPU ACL is in place. When management using dynamic interface is enabled along with CPU ACL, the CPU ACL has more priority.

The following are some examples of management access and management access using dynamic interfaces, here the management VLAN IP address of the Cisco WLC is 209.165. 201.1 and dynamic VLAN IP address of the Cisco WLC is 209.165. 202.129:

- Source wired client from Cisco WLC's dynamic interface VLAN accesses the management interface VLAN and tries for management access.
- Source wired client from Cisco WLC's management interface VLAN accesses the dynamic interface VLAN and tries for management access.
- Source wired client from Cisco WLC's dynamic interface VLAN accesses the dynamic interface VLAN tries and tries for management access.
- Source wired client from Layer 3 VLAN interface accesses the dynamic interface or the management interface and tries for management access.

Here, management is not the management interface but the configuration access. If the Cisco WLC configuration is accessed from any other IP address on the Cisco WLC other than the management IP, it is management using dynamic interface.

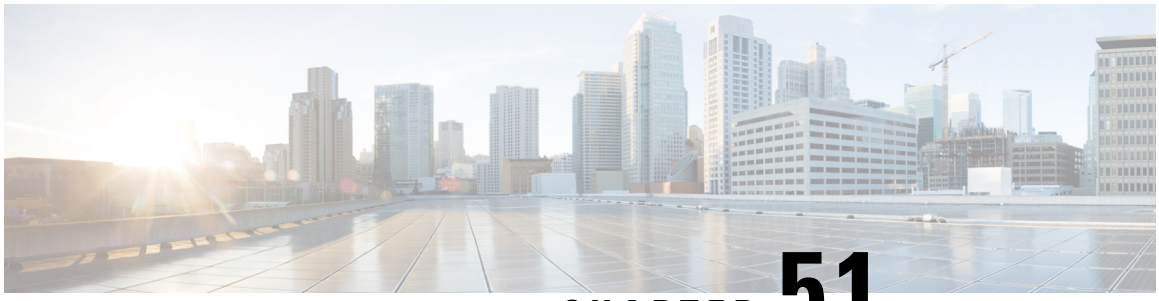
Configuring Management using Dynamic Interfaces (CLI)

Dynamic interface is disabled by default and can be enabled if needed to be also accessible for most or all of management functions. Once enabled, all dynamic interfaces are available for management access to controller. You can use access control lists (ACLs) to limit this access as required.

Procedure

- Enable or disable management using dynamic interfaces by entering this command:

  config network mgmt-via-dynamic-interface {**enable** | **disable**}



CHAPTER 51

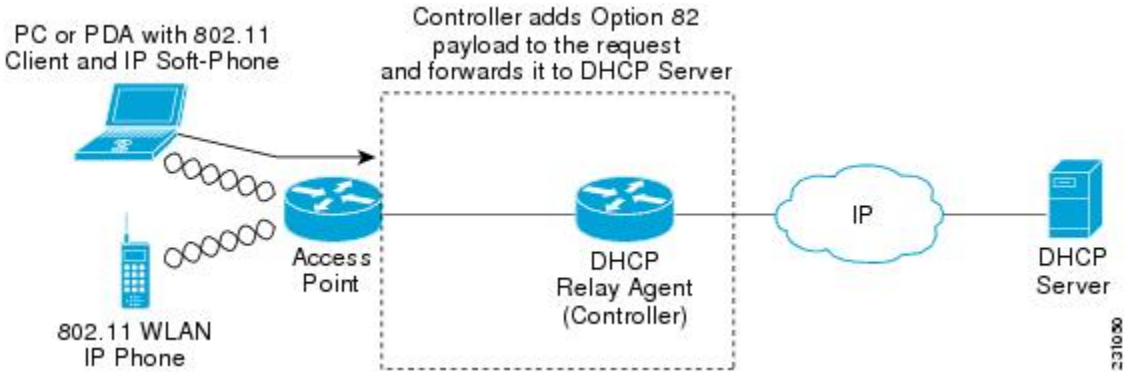
Configuring DHCP Option 82

- DHCP Option 82, on page 435
- Restrictions on DHCP Option 82, on page 436
- Configuring DHCP Option 82 (GUI), on page 436
- Configuring DHCP Option 82 (CLI), on page 436

DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can configure the controller to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.

Figure 39: DHCP Option 82



The access point forwards all DHCP requests from a client to the controller. The controller 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 controller.

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

This section contains the following subsections:

Restrictions on DHCP Option 82

- DHCP option 82 is not supported for use with auto-anchor mobility.

Configuring DHCP Option 82 (GUI)

Step 1 Choose **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page.

Step 2 Select the **Enable DHCP Proxy** check box to enable DHCP proxy.

Step 3 Choose a DHCP Option 82 format from the drop-down list. You can choose either binary or ascii to specify the format of the DHCP option 82 payload.

Step 4 Choose a DHCP Option 82 Remote ID field format from the drop-down list to specify the format of the DHCP option 82 payload.

For more information about the options available, see the Controller Online Help.

Step 5 Enter the DHCP timeout value in the DHCP Timeout field. The timeout value is globally applicable. You can specify the DHCP timeout value in range from 5 to 120 seconds.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration** .

What to do next

On the controller CLI, you can enable DHCP option 82 on the dynamic interface to which the WLAN is associated by entering this command:

config interface dhcp dynamic-interface *interface-name* **option-82 enable**

Configuring DHCP Option 82 (CLI)

Procedure

- Configure the format of the DHCP option 82 payload by entering one of these commands:
  - **config dhcp opt-82 remote-id** *ap_mac*—Adds the radio MAC address of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *ap_mac:ssid*—Adds the radio MAC address and SSID of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *ap-ethmac*—Adds the Ethernet MAC address of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *apname:ssid*—Adds the AP name and SSID of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *ap-group-name*—Adds the AP group name to the DHCP option 82 payload.

- **config dhcp opt-82 remote-id** *flex-group-name*—Adds the FlexConnect group name to the DHCP option 82 payload.
- **config dhcp opt-82 remote-id** *ap-location*—Adds the AP location to the DHCP option 82 payload.
- **config dhcp opt-82 remote-id** *apmac-vlan-id*—Adds the radio MAC address of the access point and the VLAN ID to the DHCP option 82 payload.
- **config dhcp opt-82 remote-id** *apname-vlan-id*—Adds the AP name and its VLAN ID to the DHCP option 82 payload.
- **config dhcp opt-82 remote-id** *ap-ethmac-ssid*—Adds the Ethernet MAC address of the access point and the SSID to the DHCP option 82 payload.

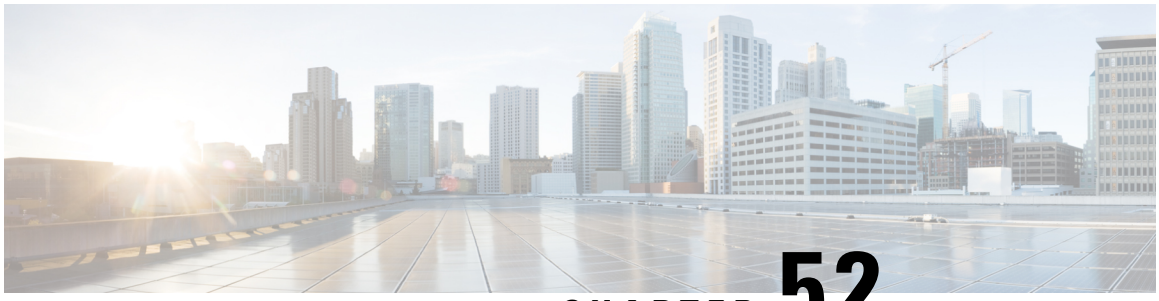
- Configure the format of the DHCP option 82 as binary or ASCII by entering this command:

  config dhcp opt-82 format {**binary** | **ascii**}

- Enable DHCP Option 82 on the dynamic interface to which the WLAN is associated by entering this command:

  config interface dhcp dynamic-interface *interface-name* **option-82 enable**

- See the status of DHCP option 82 on the dynamic interface by entering the **show interface detailed** *dynamic-interface-name*command.



CHAPTER 52

Configuring and Applying Access Control Lists

- Information about Access Control Lists, on page 439
- Guidelines and Restrictions on Access Control Lists, on page 439
- Configuring and Applying Access Control Lists (GUI), on page 440
- Configuring and Applying Access Control Lists (CLI), on page 444
- Configuring Layer 2 Access Control Lists, on page 446

Information about Access Control Lists

An Access Control List (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). After ACLs are configured on the controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU.

You may also want to create a preauthentication ACL for web authentication. Such an ACL could be used to allow certain types of traffic before authentication is complete.

Both IPv4 and IPv6 ACL are supported. IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.

Note You can enable only IPv4 traffic in your network by blocking IPv6 traffic. That is, you can configure an IPv6 ACL to deny all IPv6 traffic and apply it on specific or all WLANs.

Guidelines and Restrictions on Access Control Lists

- You can define up to 64 ACLs, each with up to 64 rules (or filters) for both IPv4 and IPv6. Each rule has parameters that affect its action. When a packet matches all of the parameters for a rule, the action set for that rule is applied to the packet.
- When you apply CPU ACLs on a Cisco 5508 WLC or a Cisco WiSM2, you must permit traffic towards the virtual interface IP address for web authentication.
- All ACLs have an implicit “deny all rule” as the last rule. If a packet does not match any of the rules, it is dropped by the controller.

- If you are using an external web server with a Cisco 5508 WLC or a WLC network module, you must configure a preauthentication ACL on the WLAN for the external web server.
- Multicast traffic received from wired networks that is destined to wireless clients is not processed by WLC ACLs. Multicast traffic initiated from wireless clients, destined to wired networks or other wireless clients on the same controller, is processed by WLC ACLs.
- ACLs are configured on the controller directly or configured through Cisco Prime Infrastructure templates. The ACL name must be unique.
- You can configure ACL per client (AAA overridden ACL) or on either an interface or a WLAN. The AAA overridden ACL has the highest priority. However, each interface, WLAN, or per client ACL configuration that you apply can override one another.
- If peer-to-peer blocking is enabled, traffic is blocked between peers even if the ACL allows traffic between them.
- When you create an ACL, it is recommended to perform the two actions (create an ACL or ACL ruleand apply the ACL or ACL rule) continuously either from CLI or GUI.
- Mobility pings on ports 16666 and 16667 are notable exemptions and these ports cannot be blocked by any ACL.
- When high priority for an ACL is enabled, two types of rules are possible as follows:
  - **Deny**: If you add the *Deny* rule, all the relevant services under the rule are blocked or disabled. This does not depend on the configuration status of the services.
  - **Permit**: If you add the *Permit* rule, all the relevant services might require more configuration that are based on the nature of the service, for the service to be functional. For example, Telnet/SSH do not require more configuration for their services to be functional, whereas HTTP/HTTPS do require more configuration for their services to be functional.
- ACLs do not affect the service ports of controllers.
- URL domain configuration for IPv6 ACLs is not supported. However, it is supported in the case of IPv4 ACLs.

Configuring and Applying Access Control Lists (GUI)

Configuring Access Control Lists (GUI)

Step 1 Choose **Security** > **Access Control Lists** > **Access Control Lists** to open the Access Control Lists page.

Step 2 If you want to see if packets are hitting any of the ACLs configured on your controller, select the **Enable Counters** check box and click **Apply**. Otherwise, leave the check box unselected, which is the default value. This feature is useful when troubleshooting your system.

Note If you want to clear the counters for an ACL, hover your cursor over the blue drop-down arrow for that ACL and choose **Clear Counters**.

Step 3 Add a new ACL by clicking **New**. The Access Control Lists > New page appears.

Step 4 In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 5 Choose the ACL type. There are two types of ACL supported, IPv4 and IPv6.

Step 6 Click **Apply**. When the Access Control Lists page reappears, click the name of the new ACL.

Step 7 When the Access Control Lists > Edit page appears, click **Add New Rule**. The Access Control Lists > Rules > New page appears.

Step 8 Configure a rule for this ACL as follows:

a) The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

Note If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number for a rule, the sequence numbers for other rules adjust to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

b) From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

- **Any**—Any source (this is the default value).
- **IP Address**—A specific source. If you choose this option, enter the IP address and netmask of the source in the text boxes. If you are configuring IPv6 ACL, enter the IPv6 address and prefix length of the destination in the text boxes.

c) From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- **Any**—Any destination (this is the default value).
- **IP Address**—A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes. If you are configuring IPv6 ACL, enter the IPv6 address and prefix length of the destination in the text boxes.

d) From the Protocol drop-down list, choose the protocol ID of the IP packets to be used for this ACL. These are the protocol options:

- **Any**—Any protocol (this is the default value)
- **TCP**—Transmission Control Protocol
- **UDP**—User Datagram Protocol
- **ICMP/ICMPv6**—Internet Control Message Protocol

Note ICMPv6 is only available for IPv6 ACL.

- **ESP**—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP in IP**—Internet Protocol (IP) in IP (permits or denies IP-in-IP packets)
- **Eth Over IP**—Ethernet-over-Internet Protocol

- **OSPF**—Open Shortest Path First
- **Other**—Any other Internet Assigned Numbers Authority (IANA) protocol

Note If you choose Other, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.

The controller can permit or deny only IP packets in an ACL. Other types of packets (such as ARP packets) cannot be specified.

e) If you chose TCP or UDP in the previous step, two additional parameters appear: Source Port and Destination Port. These parameters enable you to choose a specific source port and destination port or port ranges. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.

Note Source and Destination ports based on the ACL type.

f) From the DSCP drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet.

- **Any**—Any DSCP (this is the default value)
- **Specific**—A specific DSCP from 0 to 63, which you enter in the DSCP edit box

g) From the **Direction** drop-down list, choose one of these options to specify the direction of the traffic to which this ACL applies:

- **Any**—Any direction (this is the default value)
- **Inbound**—From the client
- **Outbound**—To the client

Note If you are planning to apply this ACL to the controller CPU, the packet direction does not have any significance, it is always 'Any'.

h) From the **Action** drop-down list, choose Deny to cause this ACL to block packets or Permit to cause this ACL to allow packets. The default value is Deny.

i) Click **Apply** to commit your changes. The **Access Control Lists > Edit** page reappears, showing the rules for this ACL.

The **Deny Counters** fields shows the number of times that packets have matched the explicit deny ACL rule. The **Number of Hits** field shows the number of times that packets have matched an ACL rule. You must enable ACL counters on the Access Control Lists page to enable these fields.

Note If you want to edit a rule, click the sequence number of the desired rule to open the **Access Control Lists > Rules > Edit** page. If you want to delete a rule, hover your cursor over the blue drop-down arrow for the desired rule and choose **Remove**.

j) Repeat this procedure to add any additional rules for this ACL.

Step 9 Click **Save Configuration** to save your changes.

Step 10 Repeat this procedure to add any additional ACLs.

Applying an Access Control List to an Interface (GUI)

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Click the name of the desired interface. The **Interfaces > Edit** page for that interface appears.

Step 3 Choose the desired ACL from the ACL Name drop-down list and click **Apply**. The default is None.

Note IPv6 ACLs are supported only on management interface.

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

Applying an Access Control List to the Controller CPU (GUI)

Before you begin

Before you apply ACL rules, ensure that you have explicitly set the following RRM ports to *allow* in the CPU ACL:

- 12124-12125
- 12134-12135

Also ensure that you add these ACL rules specifically at the top of the ACL list.

If you do not set these RRM ports to *allow*, the ports are blocked by default.

Step 1 Choose **Security** > **Access Control Lists** > **CPU Access Control Lists** to open the CPU Access Control Lists page.

Step 2 Select the **Enable CPU ACL** check box to enable a designated ACL to control the IPv4 traffic to the controller CPU or unselect the check box to disable the CPU ACL feature and remove any ACL that had been applied to the CPU. The default value is unselected.

Step 3 From the **ACL Name** drop-down list, choose the ACL that will control the IPv4 traffic to the controller CPU. *None* is the default value when the CPU ACL feature is disabled. If you choose *None* while the **Enable CPU ACL** check box is selected, an error message appears indicating that you must choose an ACL.

Note This parameter is available only if you have selected the **CPU ACL Enable** check box.

Note When CPU ACL is enabled, it is applicable to both wireless and wired traffic.

Step 4 Select the **Enable CPU IPv6 ACL** check box to enable a designated ACL to control the IPv6 traffic to the controller CPU or unselect the check box to disable the CPU ACL feature and remove any ACL that had been applied to the CPU. The default value is unselected.

Note For CPU IPv6 ACL, along with permit rules for HTTP/Telnet, you must add a rule to allow ICMPv6 (NA/ND uses ICMPv6) for the CPU IPv6 ACLs to work.

Step 5 From the **IPv6 ACL Name** drop-down list, choose the ACL that will control the IPv6 traffic to the controller CPU. *None* is the default value when the CPU ACL feature is disabled. If you choose *None* while the **Enable CPU IPv6 ACL** check box is selected, an error message appears indicating that you must choose an ACL.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Applying an Access Control List to a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4 From the **Override Interface ACL** drop-down list, choose the IPv4 or IPv6 ACL that you want to apply to this WLAN. The ACL that you choose overrides any ACL that is configured for the interface. None is the default value.

Note To support centralized access control through AAA server such as ISE or ACS, IPv6 ACL must be configured on the controller and the WLAN must be configured with AAA override enabled feature.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Applying a Preauthentication Access Control List to a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** page.

Step 3 Choose the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page.

Step 4 Select the **Web Policy** check box.

Step 5 From the **Preauthentication ACL** drop-down list, choose the desired ACL and click **Apply**. None is the default value.

Step 6 Save the configuration.

Configuring and Applying Access Control Lists (CLI)

Configuring Access Control Lists (CLI)

Step 1 See all of the ACLs that are configured on the controller by entering this command:

show [**ipv6**] **acl summary**

Step 2 See detailed information for a particular ACL by entering this command:

show [**ipv6**] **acl detailed** *acl_name*

The Counter text box increments each time a packet matches an ACL rule, and the DenyCounter text box increments each time a packet does not match any of the rules.

Note If a traffic/request is allowed from the controller by a permit rule, then the response to the traffic/request in the opposite direction also is allowed and cannot be blocked by a deny rule in the ACL.

Step 3 Enable or disable ACL counters for your controller by entering this command:

config acl counter {**start** | **stop**}

Note If you want to clear the current counters for an ACL, enter the **clear acl counters** *acl_name command.*

Step 4 Add a new ACL by entering this command:

config [ipv6] **acl create** *acl_name*.

You can enter up to 32 alphanumeric characters for the *acl_name* parameter.

Note When you try to create an interface name with space, the controller CLI does not create an interface. For example, if you want to create an interface name int 3, the CLI will not create this since there is a space between int and 3. If you want to use int 3 as the interface name, you need to enclose within single quotes like 'int 3'.

Step 5 Add a rule for an ACL by entering this command:

config [ipv6] acl rule add acl_name rule_index

Step 6 Configure an ACL rule by entering **config [ipv6] acl rule** command:

Step 7 Save your settings by entering this command:

save config

Note To delete an ACL, enter the **config** [**ipv6**] **acl delete** *acl_name* command. To delete an ACL rule, enter the **config** [**ipv6**] **acl rule delete** *acl_name rule_index* command.

Applying Access Control Lists (CLI)

Step 1 Perform the following to apply an IPv4 ACL:

- To apply an ACL to the IPv4 data path, enter this command:

  config acl apply acl_name

- To apply an ACL to the controller CPU to restrict the IPv4 type of traffic (wired, wireless, or both) reaching the CPU, enter this command:

  config acl cpu acl_name {wired | wireless | both}

  Note To see the ACL that is applied to the controller CPU, enter the **show acl cpu command**. To remove the ACL that is applied to the controller CPU, enter the **config acl cpu none** command.

  Note For 2504 and 4400 series WLC, the CPU ACL cannot be used to control the CAPWAP traffic. Use the access-list on the network to control CAPWAP traffic.

Step 2 Perform the following to apply an IPv6 ACL:

- To apply an ACL to an IPv6 data path, enter this command:

config ipv6 acl apply name

- To apply an ACL to the controller CPU to restrict the IPv6 type of traffic (wired, wireless, or both) reaching the CPU, enter this command:

  config ipv6 acl cpu {name|none}

Step 3 To apply an ACL to a WLAN, enter this command:

- **config wlan acl** *wlan_id acl_name*

  Note To see the ACL that is applied to a WLAN, enter the **show wlan** *wlan_id command*. To remove the ACL that is applied to a WLAN, enter the **config wlan acl** *wlan_id* **none** command.

Step 4 To apply a pre-authentication ACL to a WLAN, enter this command:

- **config wlan security web-auth acl** *wlan_id acl_name*

Step 5 Save your changes by entering this command:

save config

Configuring Layer 2 Access Control Lists

Layer 2 Access Control Lists

You can configure rules for Layer 2 access control lists (ACLs) based on the Ethertype associated with the packets. Using this feature, if a WLAN with central switching is required to support only PPPoE clients, you can apply Layer 2 ACL rules on the WLAN to allow only PPPoE packets after the client is authenticated and the rest of the packets are dropped. Similarly, if the WLAN is required to support only IPv4 clients or only IPv6 clients, you can apply Layer 2 ACL rules on the WLAN to allow only IPv4 or IPv6 packets after the client is authenticated and the rest of the packets are dropped. For a locally-switched WLAN, you can apply the same Layer 2 ACL either for the WLAN or a FlexConnect AP. AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs. The Layer 2 ACL that is applied to the FlexConnect AP takes precedence over the Layer 2 ACL that is applied to the WLAN.

In a mobility scenario, the mobility anchor configuration is applicable.

The following traffic is not blocked:

- Wireless traffic for wireless clients:
  - 802.1X
  - Inter-Access Point Protocol
  - 802.11
  - Cisco Discovery Protocol
- Traffic from a distributed system:
  - Broadcast

- Multicast
- IPv6 Neighbor Discovery Protocol (NDP)
- Address Resolution Protocol (ARP) and Gratuitous ARP Protection (GARP)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)

Layer 2 ACL Mapping to WLAN

If you map a Layer 2 ACL to a WLAN, the Layer 2 ACL rules that you configure apply to all the clients that are associated with that WLAN.

When you map a Layer 2 ACL to a centrally switched WLAN, the rule to pass traffic based on the Ethertype is determined by Fast-Path for every client that is associated with the WLAN. Fast-Path looks into the Ethernet headers associated with the packets and forwards the packets whose Ethertype matches with the one that is configured for the ACL.

When you map a Layer 2 ACL to a locally switched WLAN, the rule to pass traffic based on the Ethertype is determined by the forwarding plane of the AP for every client that is associated with the WLAN. The AP forwarding plane looks into the Ethernet headers associated with the packets and forwards or denies the packets based on the action whose Ethertype matches with the one that is configured for the ACL.

Note Controllers configured to preform Central Switching and Centralized Authentication displays the name of the Layer-2 ACL being applied to roaming users incorrectly. The situation occurs when an authorized device preforms a Layer-3 roam from the anchor controller to a foreign controller. After roaming, if an administrator issues the **show acl layer2 summary** command on the CLI of the foreign controller the incorrect information is displayed. It is expected that the ACL applied by the anchor will follow the authenticated client as it roams from controller to controller.

This section contains the following subsections:

Restrictions on Layer 2 Access Control Lists

- You can create a maximum of 16 rules for a Layer 2 ACL.
- AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs.
- You can create a maximum of 64 Layer 2 ACLs on a controller.
- A maximum of 16 Layer 2 ACLs are supported per AP because an AP supports a maximum of 16 WLANs.
- Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an AP does not support the same Layer 2 and Layer 3 ACL names.

Configuring Layer 2 Access Control Lists (CLI)

Procedure

- **config acl layer2** {**create** | **delete**} *acl-name*—Creates or deletes a Layer 2 ACL.
- **config acl layer2 apply** *acl-name*—Applies a Layer 2 ACL to a data path.
- **config acl layer2 rule** {**add** | **delete**} *acl-rule-name index*—Creates or deletes a Layer 2 ACL rule.
- **config acl layer2 rule change index** *acl-rule-name old-index new-index*—Changes the index of a Layer 2 ACL rule.
- **config acl layer2 rule action** *acl-rule-name index* {*permit* | *deny*}—Configures an action for a rule.
- **config acl layer2 rule etherType** *name index ether-type-number-in-hex ether-type-mask-in-hex*—Configures the destination IP address and netmask for a rule.
- **config acl layer2 rule swap index** *acl-rule-name index-1 index-2*—Swaps the index values of two rules.
- **config acl counter** {**start** | **stop**}—Starts or stops the ACL counter. This command is applicable for all types of ACLs. In an HA environment, the counters are not synchronized between the active and standby controllers.
- **show acl layer2 summary**—Shows a summary of the Layer 2 ACL profiles.
- **show acl layer2 detailed** *acl-name*—Shows a detailed description of the Layer 2 ACL profile specified.
- **show client detail** *client-mac-addr*—Shows the Layer 2 ACL rule that is applied to the client.

Mapping of Layer 2 ACLs with WLANs (CLI)

This is applicable to centrally switched WLANs and locally switched WLANs without FlexConnect access points.

Procedure

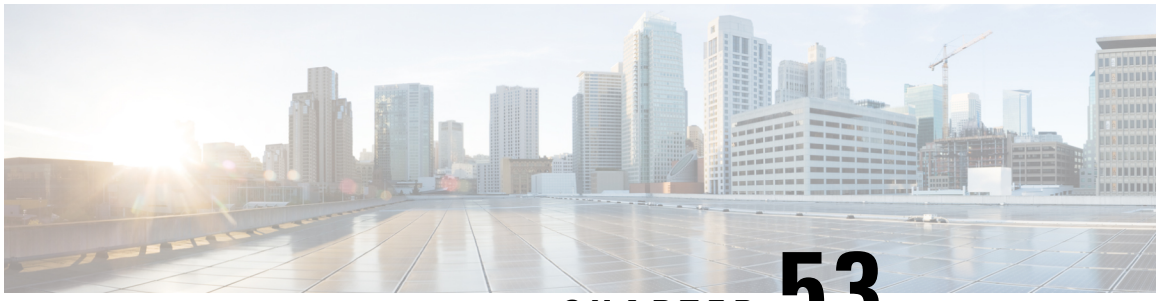
- **config wlan layer2 acl** *wlan-id acl-name*—Maps a Layer 2 ACL to a centrally switched WLAN.
- **config wlan layer2 acl** *wlan-id none*—Clears the Layer 2 ACLs mapped to a WLAN.
- **show wlan** *wlan-id*—Shows the status of a Layer 2 ACL that is mapped to a WLAN.

Mapping of Layer 2 ACLs with Locally Switched WLANs Using FlexConnect Access Points (CLI)

This is applicable to locally switched WLANs that have FlexConnect access points.

Procedure

- **config ap flexconnect wlan l2acl add** *wlan-id ap-name acl-name*—Maps a Layer 2 ACL to a locally switched WLAN.
- **config ap flexconnect wlan l2acl** *delete wlan-id ap-name*—Deletes the mapping.
- **show ap config general** *ap-name*—Shows the details of the mapping.



CHAPTER 53

Configuring Management Frame Protection

- Protected Management Frames (Management Frame Protection), on page 449
- Restrictions for Management Frame Protection, on page 450
- Configuring Infrastructure MFP (GUI), on page 451
- Viewing the Management Frame Protection Settings (GUI), on page 451
- Configuring Infrastructure MFP (CLI), on page 452
- Viewing the Management Frame Protection Settings (CLI), on page 452
- Debugging Management Frame Protection Issues (CLI), on page 452

Protected Management Frames (Management Frame Protection)

By default, 802.11 management frames are unauthenticated and hence not protected against spoofing. Infrastructure management frame protection (MFP) and 802.11w protected management frames (PMF) provide protection against such attacks.

Infrastructure MFP

Infrastructure MFP protects management frames by detecting adversaries that are invoking denial-of-service attacks, flooding the network with associations and probes, interjecting as rogue APs, and affecting network performance by attacking the QoS and radio measurement frames. Infrastructure MFP is a global setting that provides a quick and effective means to detect and report phishing incidents.

Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by APs (and not those emitted by clients), which are then validated by other APs in the network. Infrastructure MFP is passive, can detect and report intrusions but has no means to stop them.

Infrastructure MFP consists of three main components:

- **Management frame protection**: The AP protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving AP configured to detect MFP frames to report the discrepancy. MFP is supported for use with Cisco Aironet lightweight APs.
- **Management frame validation**: In infrastructure MFP, the AP validates every management frame that it receives from other APs in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an AP that is configured to

transmit MFP frames, it reports the discrepancy to the network management system. In order for the timestamps to operate properly, all controllers must be Network Time Protocol (NTP) synchronized.

- **Event reporting**: The AP notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and can report the results through SNMP traps to the network management system.

Infrastructure MFP is disabled by default, and you can enable it globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if you have enabled AP authentication because the two features are mutually exclusive. When you enable infrastructure MFP globally, signature generation (adding MICs to outbound frames) can be disabled for selected WLANs, and validation can be disabled for selected APs.

Note CCXv5 client MFP is no longer supported. Client MFP is enabled as optional by default on WLANs that are configured for WPA2. However, client MFP is not supported on Wave 2 APs or 802.11ax Wi-Fi6 APs, and there exist no clients that support CCXv5.

802.11w PMF

802.11w standard protects the transmission of control and management frames, between APs and clients, against forgery and replay attacks. The frame types protected include Disassociation, Deauthentication, and Robust Action frames such as:

- Spectrum Management
- Quality of Service (QoS)
- Block Ack
- Radio measurement
- Fast Basic Service Set (BSS) Transition

For information about 802.11w PMF, see the 802.11w, on page 589 section.

Additional Reference: Configure 802.11w Management Frame Protection on WLC

This section contains the following subsections:

Restrictions for Management Frame Protection

- Lightweight access points support infrastructure MFP in local and monitor modes and in FlexConnect mode when the access point is connected to a controller. They support client MFP in local, FlexConnect, and bridge modes.
- Client MFP is supported for use only with CCXv5 clients using WPA2 with TKIP or AES-CCMP.
- Non-CCXv5 clients may associate to a WLAN if client MFP is disabled or optional.
- Error reports generated on a FlexConnect access point in standalone mode cannot be forwarded to the controller and are dropped.

Configuring Infrastructure MFP (GUI)

Step 1 Choose **Security> Wireless Protection Policies > AP Authentication/MFP** to open the AP Authentication Policy page.

Step 2 Enable infrastructure MFP globally for the controller by choosing **Management Frame Protection** from the **Protection Type** drop-down list.

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

Note If more than one controller is included in the mobility group, you must configure an NTP/SNTP server on all controllers in the mobility group that are configured for infrastructure MFP.

Step 4 Configure client MFP for a particular WLAN after infrastructure MFP has been enabled globally for the controller as follows:

a) Choose **WLANs**.
b) Click the profile name of the desired **WLAN**. The **WLANs > Edit** page appears.
c) Choose **Advanced**. The **WLANs > Edit (Advanced) page** is displayed.
d) From the **MFP Client Protection** drop-down list, choose **Disabled**, **Optional**, or **Required** . The default value is **Optional**. If you choose **Required**, clients are allowed to associate only if MFP is negotiated (that is, if WPA2 is configured on the controller and the client supports CCXv5 MFP and is also configured for WPA2).

Note For Cisco OEAP 600, MFP is not supported. It should either be Disabled or Optional.

e) Click **Apply** to commit your changes.

Step 5 Save the configuration.

Viewing the Management Frame Protection Settings (GUI)

To see the controller's current global MFP settings, choose **Security** > **Wireless Protection Policies** > **Management Frame Protection**. The Management Frame Protection Settings page appears.

On this page, you can see the following MFP settings:

- The **Management Frame Protection** field shows if infrastructure MFP is enabled globally for the controller.
- The **Controller Time Source Valid** field indicates whether the controller time is set locally (by manually entering the time) or through an external source (such as the NTP/SNTP server). If the time is set by an external source, the value of this field is "True." If the time is set locally, the value is "False." The time source is used for validating the timestamp on management frames between access points of different controllers within a mobility group.
- The **Client Protection** field shows if client MFP is enabled for individual WLANs and whether it is optional or required.

Configuring Infrastructure MFP (CLI)

Procedure

- Enable or disable infrastructure MFP globally for the controller by entering this command:

  config wps mfp infrastructure {enable | disable}
- Enable or disable client MFP on a specific WLAN by entering this command:

  config wlan mfp client {**enable** | **disable**} *wlan_id* [**required**]

  If you enable client MFP and use the optional **required** parameter, clients are allowed to associate only if MFP is negotiated.

Viewing the Management Frame Protection Settings (CLI)

Procedure

- See the controller's current MFP settings by entering this command:

  show wps mfp summary
- See the current MFP configuration for a particular WLAN by entering this command:

  show wlan wlan_id
- See whether client MFP is enabled for a specific client by entering this command:

  show client detail *client_mac*
- See MFP statistics for the controller by entering this command:

  show wps mfp *statistics*

Note This report contains no data unless an active attack is in progress. This table is cleared every 5 minutes when the data is forwarded to any network management stations.

Debugging Management Frame Protection Issues (CLI)

Procedure

- Use this command if you experience any problems with MFP:

  debug wps mfp ? {**enable** | **disable**}

  where ? is one of the following:

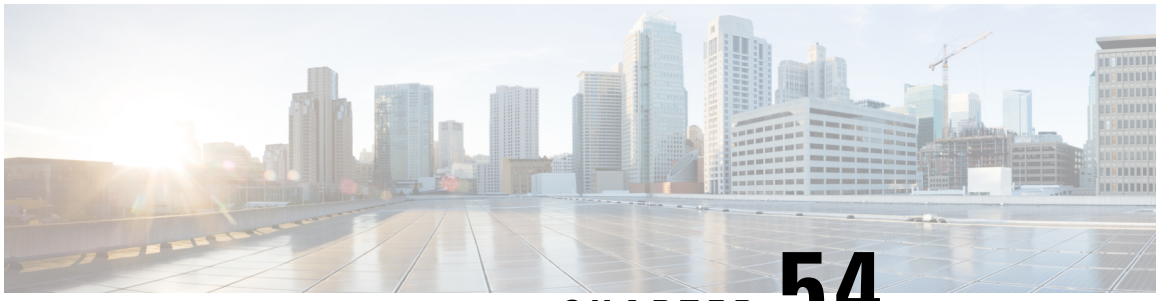
  client—Configures debugging for client MFP messages.

capwap—Configures debugging for MFP messages between the controller and access points.

detail—Configures detailed debugging for MFP messages.

report—Configures debugging for MFP reporting.

mm—Configures debugging for MFP mobility (inter-controller) messages.



CHAPTER 54

Configuring Client Exclusion Policies

- Configuring Client Exclusion Policies (GUI), on page 455
- Configuring Client Exclusion Policies (CLI), on page 455

Configuring Client Exclusion Policies (GUI)

Step 1 Choose **Security** > **Wireless Protection Policies** > **Client Exclusion Policies** to open the Client Exclusion Policies page.

Step 2 Select any of these check boxes if you want the controller to exclude clients for the condition specified. The default value for each exclusion policy is enabled.

- **Excessive 802.11 Association Failures**—Clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- **Excessive 802.11 Authentication Failures**—Clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- **Excessive 802.1X Authentication Failures**—Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- **IP Theft or IP Reuse**—Clients are excluded if the IP address is already assigned to another device.
- **Excessive Web Authentication Failures**—Clients are excluded on the fourth web authentication attempt, after three consecutive failures.

Step 3 Save your configuration.

Configuring Client Exclusion Policies (CLI)

Step 1 Enable or disable the controller to exclude clients on the sixth 802.11 association attempt, after five consecutive failures by entering this command:

config wps client-exclusion 802.11-assoc {**enable** | **disable**}

Step 2 Enable or disable the controller to exclude clients on the sixth 802.11 authentication attempt, after five consecutive failures by entering this command:

config wps client-exclusion 802.11-auth {**enable** | **disable**}

Step 3 Enable or disable the controller to exclude clients on the fourth 802.1X authentication attempt, after three consecutive failures by entering this command:

config wps client-exclusion 802.1x-auth {**enable** | **disable**}

Step 4 Configure the controller to exclude clients that reaches the maximum failure 802.1X authentication attempt with the RADIUS server by entering this command:

config wps client-exclusion 802.1x-auth max-1x-aaa-fail-attempts

You can configure the maximum failure 802.1X authentication attempt from 1 to 3 and the default value is 3.

Step 5 Enable or disable the controller to exclude clients if the IP address is already assigned to another device by entering this command:

config wps client-exclusion ip-theft {**enable** | **disable**}

Step 6 Enable or disable the controller to exclude clients on the fourth web authentication attempt, after three consecutive failures by entering this command:

config wps client-exclusion web-auth {**enable** | **disable**}

Step 7 Enable or disable the controller to exclude clients for all of the above reasons by entering this command:

config wps client-exclusion all {**enable** | **disable**}

Step 8 Use the following command to add or delete client exclusion entries.

config exclusionlist {**add** *mac-addr description* | **delete** *mac-addr* | **description** *mac-addr description*}

Step 9 Save your changes by entering this command:

save config

Step 10 See a list of clients that have been dynamically excluded, by entering this command:

show exclusionlist

Information similar to the following appears:

```
Dynamically Disabled Clients
----------------------------
  MAC Address             Exclusion Reason        Time Remaining (in secs)
  -----------             ----------------        ------------------------

00:40:96:b4:82:55         802.1X Failure           51
```

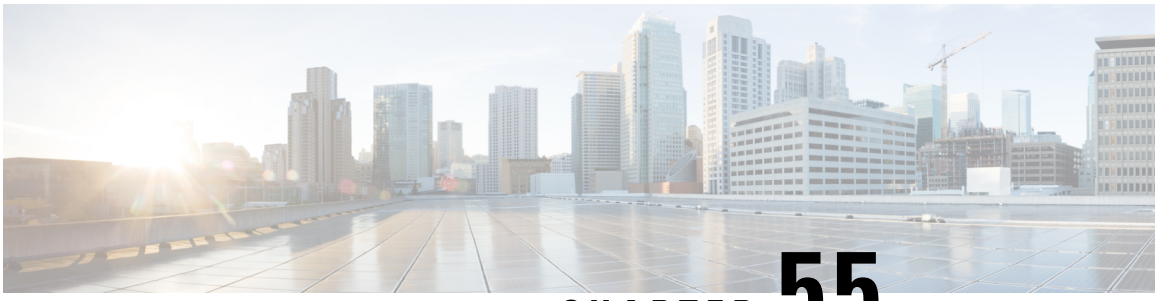
Step 11 See the client exclusion policy configuration settings by entering this command:

show wps summary

Information similar to the following appears:

```
Auto-Immune
 Auto-Immune..................................... Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
  Maximum 802.1x-AAA failure attempts............ 3
```

```
Signature Policy
  Signature Processing..................... Enabled
```



CHAPTER 55

Configuring Identity Networking

- Identity Networking, on page 459
- RADIUS Attributes Used in Identity Networking, on page 460

Identity Networking

In most wireless LAN systems, each WLAN has a static policy that applies to all clients associated with an SSID. Although powerful, this method has limitations because it requires clients to associate with different SSIDs to inherit different QoS and security policies.

However, the Cisco Wireless LAN solution supports identity networking, which allows the network to advertise a single SSID but allows specific users to inherit different QoS or security policies based on their user profiles. The specific policies that you can control using identity networking are as follows:

- ACL—When the ACL attribute is present in the RADIUS Access Accept, the system applies the ACL name to the client station after it authenticates, which overrides any ACLs that are assigned to the interface.
- VLAN—When a VLAN Interface-name or VLAN tag is present in a RADIUS Access Accept, the system places the client on a specific interface.

Note The VLAN feature only supports MAC filtering, 802.1X, and WPA. The VLAN feature does not support web authentication or IPsec.

- Tunnel Attributes.

Note When any of the other RADIUS attributes (QoS-Level, ACL-Name, Interface-Name, or VLAN-Tag), which are described later in this section, are returned, the Tunnel Attributes must also be returned.

The operating system's local MAC filter database has been extended to include the interface name, allowing local MAC filters to specify to which interface the client should be assigned. A separate RADIUS server can also be used, but the RADIUS server must be defined using the Security menus.

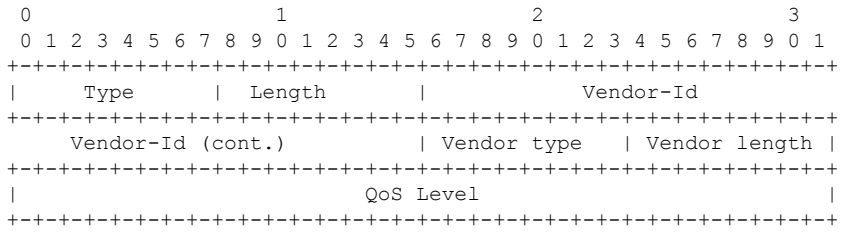
This section contains the following subsection:

RADIUS Attributes Used in Identity Networking

QoS-Level

This section explains the RADIUS attributes used in identity networking.

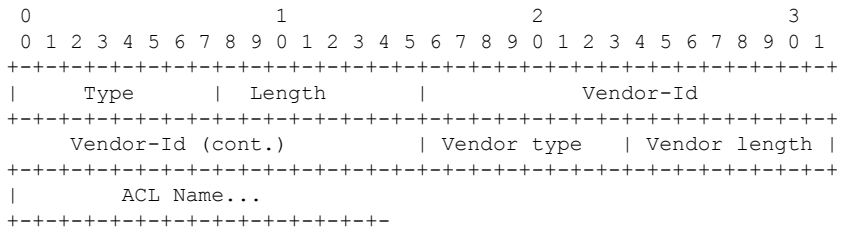
This attribute indicates the QoS level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The text boxes are transmitted from left to right.



- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – Three octets:
  - 3 – Bronze (Background)
  - 0 – Silver (Best Effort)
  - 1 – Gold (Video)
  - 2 – Platinum (Voice)

ACL-Name

This attribute indicates the ACL name to be applied to the client. A summary of the ACL-Name Attribute format is shown below. The text boxes are transmitted from left to right.

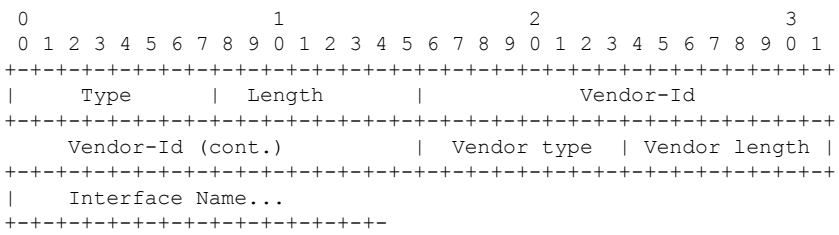


- Type – 26 for Vendor-Specific

- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value – A string that includes the name of the ACL to use for the client

Interface Name

This attribute indicates the VLAN Interface a client is to be associated to. A summary of the Interface-Name Attribute format is shown below. The text boxes are transmitted from left to right.



- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value – A string that includes the name of the interface the client is to be assigned to.

Note This Attribute only works when MAC filtering is enabled or if 802.1X or WPA is used as the security policy.

VLAN Tag

This attribute indicates the group ID for a particular tunneled session and is also known as the Tunnel-Private-Group-ID attribute.

This attribute might be included in the Access-Request packet if the tunnel initiator can predetermine the group resulting from a particular connection and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. Private groups may be used to associate a tunneled session with a particular group of users. For example, it may be used to facilitate routing of unregistered IP addresses through a particular interface. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session.

A summary of the Tunnel-Private-Group-ID Attribute format is shown below. The text boxes are transmitted from left to right.

```
 0                   1                   2                   3
 0 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 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Length     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 81 for Tunnel-Private-Group-ID.
- Length – >= 3
- Tag – The Tag text box is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. If the value of the Tag text box is greater than 0x00 and less than or equal to 0x1F, it should be interpreted as indicating which tunnel (of several alternatives) this attribute pertains. If the Tag text box is greater than 0x1F, it should be interpreted as the first byte of the following String text box.
- String – This text box must be present. The group is represented by the String text box. There is no restriction on the format of group IDs.

Note When any of the other RADIUS attributes (QoS-Level, ACL-Name, Interface-Name, or VLAN-Tag) are returned, the Tunnel Attributes must also be returned.

Tunnel Attributes

RFC 2868 defines RADIUS tunnel attributes used for authentication and authorization, and RFC2867 defines tunnel attributes used for accounting. Where the IEEE 802.1X authenticator supports tunneling, a compulsory tunnel may be set up for the Supplicant as a result of the authentication.

In particular, it may be desirable to allow a port to be placed into a particular VLAN, defined in IEEE 8021Q, based on the result of the authentication. This configuration can be used, for example, to allow a wireless host to remain on the same VLAN as it moves within a campus network.

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept. However, the IEEE 802.1X authenticator may also provide a hint as to the VLAN to be assigned to the Supplicant by including Tunnel attributes within the AccessRequest.

For use in VLAN assignment, the following tunnel attributes are used:

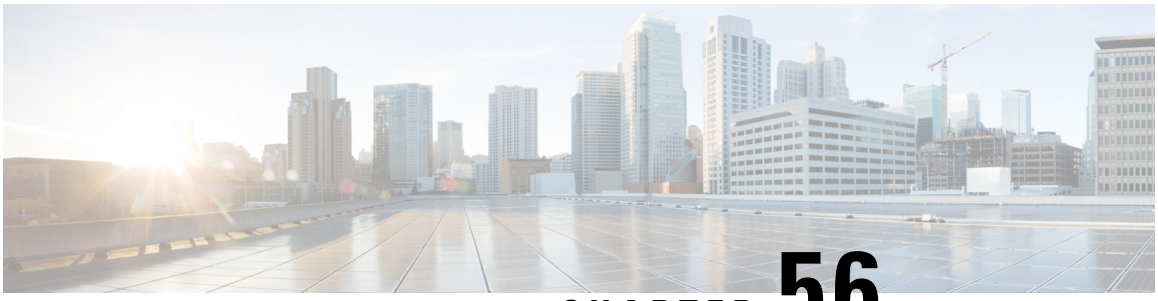
- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

The VLAN ID is 12 bits, with a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type String as defined in RFC 2868, for use with IEEE 802.1X, the VLANID integer value is encoded as a string.

When Tunnel attributes are sent, it is necessary to fill in the Tag text box. As noted in RFC 2868, section 3.1:

- The Tag text box is one octet in length and is intended to provide a means of grouping attributes in the same packet that refer to the same tunnel. Valid values for this text box are 0x01 through 0x1F, inclusive. If the Tag text box is unused, it must be zero (0x00).

- For use with Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Client-Auth-ID or Tunnel-Server-Auth-ID attributes (but not Tunnel-Type, Tunnel-Medium-Type, Tunnel-Password, or Tunnel-Preference), a tag text box of greater than 0x1F is interpreted as the first octet of the following text box.
- Unless alternative tunnel types are provided, (e.g. for IEEE 802.1X authenticators that may support tunneling but not VLANs), it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag text box should be set to zero (0x00) in all tunnel attributes. Where alternative tunnel types are to be provided, tag values between 0x01 and 0x1F should be chosen.



CHAPTER 56

Configuring AAA Override

- AAA Override, on page 465
- Restrictions for AAA Override, on page 465
- Updating the RADIUS Server Dictionary File for Proper QoS Values, on page 466
- Configuring AAA Override (GUI), on page 467
- Configuring AAA Override (CLI), on page 468

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.

AAA Override for IPv6 ACLs

In order to support centralized access control through a centralized AAA server such as the Cisco Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis using AAA Override attributes. In order to use this feature, the IPv6 ACL must be configured on the controller and the WLAN must be configured with the AAA Override feature enabled. The actual named AAA attribute for an IPv6 ACL is ***Airespace-IPv6-ACL-Name***, which is similar to the *Airespace-ACL-Name* attribute that is used for provisioning an IPv4-based ACL. The AAA attribute returned contents should be a string equal to the name of the IPv6 ACL as configured on the controller.

Note From Release 7.5, the upstream AAA override rate limiting value is same as the downstream AAA override rate limiting value.

This section contains the following subsections:

Restrictions for AAA Override

- If a client moves to a new interface due to the AAA override and then you apply an ACL to that interface, the ACL does not take effect until the client reauthenticates. To work around this issue, apply the ACL and then enable the WLAN so that all clients connect to the ACL that is already configured on the

interface, or disable and then reenable the WLAN after you apply the interface so that the clients can reauthenticate.

- If the ACL returned from the AAA server does not exist on the controller or if the ACL is configured with an incorrect name, then the clients are not allowed to be authenticated.
- With FlexConnect local switching, Multicast is forwarded only for the VLAN that the SSID is mapped to and not to any overridden VLANs. Therefore, IPv6 does not work as expected because Multicast traffic is forwarded from the incorrect VLAN.
- When the interface group is mapped to a WLAN and clients connect to the WLAN, the client does not get the IP address in a round robin fashion. The AAA override with interface group is supported.
- Most of the configuration for allowing AAA override is done at the RADIUS server, where you should configure the Access Control Server (ACS) with the override properties you would like it to return to the controller (for example, Interface-Name, QoS-Level, and VLAN-Tag).
- On the controller, enable the Allow AAA Override configuration parameter using the GUI or CLI. Enabling this parameter allows the controller to accept the attributes returned by the RADIUS server. The controller then applies these attributes to its clients.
- During Layer2 authentication if AAA override is enabled, local policies are not applied and the override takes precedence.
- Cisco TrustSec security group tag is not applied until you enable AAA override on a WLAN.

Updating the RADIUS Server Dictionary File for Proper QoS Values

If you are using a Steel-Belted RADIUS (SBR), FreeRadius, or similar RADIUS server, clients may not obtain the correct QoS values after the AAA override feature is enabled. For these servers, which allow you to edit the dictionary file, you need to update the file to reflect the proper QoS values: Silver is 0, Gold is 1, Platinum is 2, and Bronze is 3. To update the RADIUS server dictionary file, follow these steps:

Note This issue does not apply to the Cisco Secure Access Control Server (ACS).

To update the RADIUS server dictionary file, follow these steps:

1. Stop the SBR service (or other RADIUS service).
2. Save the following text to the `Radius_Install_Directory\Service` folder as `ciscowlan.dct`:

```
##################################################################################
# CiscoWLAN.dct- Cisco Wireless Lan Controllers
#
# (See README.DCT for more details on the format of this file)
##################################################################################

# Dictionary - Cisco WLAN Controllers
#
# Start with the standard Radius specification attributes
#
```

```
@radius.dct
#
# Standard attributes supported by Airespace
#
# Define additional vendor specific attributes (VSAs)
#

MACRO Airespace-VSA(t,s) 26 [vid=14179 type1=%t% len1=+2 data=%s%]

ATTRIBUTE   WLAN-Id                 Airespace-VSA(1, integer)     cr
ATTRIBUTE   Aire-QoS-Level          Airespace-VSA(2, integer)     r
VALUE Aire-QoS-Level Bronze     3
VALUE Aire-QoS-Level Silver     0
VALUE Aire-QoS-Level Gold       1
VALUE Aire-QoS-Level Platinum   2

ATTRIBUTE   DSCP                    Airespace-VSA(3, integer)     r
ATTRIBUTE   802.1P-Tag              Airespace-VSA(4, integer)     r
ATTRIBUTE   Interface-Name          Airespace-VSA(5, string)      r
ATTRIBUTE   ACL-Name                Airespace-VSA(6, string)      r

# This should be last.

##############################################################################
# CiscoWLAN.dct - Cisco WLC dictionary
##############################################################################
```

3. Open the `dictiona.dcm` file (in the same directory) and add the line "@ciscowlan.dct."
4. Save and close the `dictiona.dcm` file.
5. Open the `vendor.ini` file (in the same directory) and add the following text:

```
vendor-product       = Cisco WLAN Controller
dictionary           = ciscowlan
ignore-ports         = no
port-number-usage    = per-port-type
help-id              =
```

6. Save and close the `vendor.ini` file.
7. Start the SBR service (or other RADIUS service).
8. Launch the SBR Administrator (or other RADIUS Administrator).
9. Add a RADIUS client (if not already added). Choose **Cisco WLAN Controller** from the Make/Model drop-down list.

Configuring AAA Override (GUI)

Step 1 Choose **WLANs** to open the **WLANs** page.

Step 2 Click the ID number of the WLAN that you want to configure. The **WLANs > Edit** page appears.

Step 3 Choose the **Advanced** tab.

Step 4 Select the **Allow AAA Override** check box to enable AAA override or unselect it to disable this feature. The default value is disabled.

Step 5 Click **Apply**.

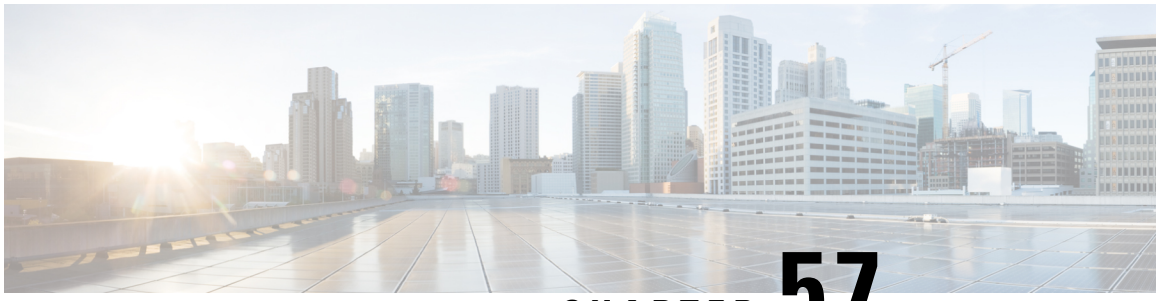
Step 6 Click **Save Configuration**.

Configuring AAA Override (CLI)

Procedure

- Configure override of user policy through AAA on a WLAN by entering this command:
  config wlan aaa-override {**enable** | **disable**} *wlan-id*

  For *wlan-id*, enter a value between 1 and 16.
- Configure debugging of 802.1X AAA interactions by entering this command:
  debug dot1x aaa {**enable** | **disable**}
- Configure debugging of AAA QoS override by entering this command:
  debug ap aaaqos-dump {**enable** | **disable**}



CHAPTER 57

Managing Rogue Devices

- Rogue Devices, on page 469
- Configuring Rogue Detection (GUI), on page 474
- Configuring Rogue Detection (CLI), on page 476

Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. There is an increased chance of enterprise security breach when wireless users connect to access points in the enterprise network.

The following are some guidelines to manage rogue devices:

- The containment frames are sent immediately after the authorization and associations are detected. The enhanced containment algorithm provides more effective containment of ad hoc clients.
- In a dense RF environment, where maximum rogue access points are suspected, the chances of detecting rogue access points by a local mode access point and FlexConnect mode access point in channel 157 or channel 161 are less when compared to other channels. To mitigate this problem, we recommend that you use dedicated monitor mode access points.
- The local and FlexConnect mode access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each channel.

- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect many rogue devices.
- Client card implementations might mitigate the effectiveness of ad hoc containment.
- It is possible to classify and report rogue access points by using rogue states and user-defined classification rules that enable rogues to automatically move between states.
- Each controller limits the number of rogue containments to three per radio (or six per radio for access points in the monitor mode).
- Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.
- RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.
- RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller , RLDP does not work.
- RLDP does not work on 5-GHz Dynamic Frequency Selection (DFS) channels. However, RLDP works when the managed access point is in the monitor mode on a DFS channel.
- If RLDP is enabled on mesh APs, and the APs perform RLDP tasks, the mesh APs are dissociated from the controller . The workaround is to disable RLDP on mesh APs.
- If RLDP is enabled on non-monitor APs, client connectivity outages occur when RLDP is in process.
- If the rogue is manually contained, the rogue entry is retained even after the rogue expires.
- If the rogue is contained by any other means, such as auto, rule, and AwIPS preventions, the rogue entry is deleted when it expires.
- The controller requests to the AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling **Validate Rogue Clients Against AAA**.
- In the 7.4 and earlier releases, if a rogue that was already classified by a rule was not reclassified. In the 7.5 release, this behavior is enhanced to allow reclassification of rogues based on the priority of the rogue rule. The priority is determined by using the rogue report that is received by the controller .
- The rogue detector AP fails to co-relate and contain the wired rogue AP on a 5Mhz channel because the MAC address of the rogue AP for WLAN, LAN, 11a radio and 11bg radio are configured with a difference of +/-1 of the rogue BSSID. In the 8.0 release, this behavior is enhanced by increasing the range of MAC address, that the rogue detector AP co-relates the wired ARP MAC and rogue BSSID, by +/-3.
- The rogue access points with open authentication can be detected on wire. The NAT wired or rogue wired detection is not supported in by WLC (both RLDP and rogue detector AP). The non-adjacent MAC address is supported by rogue detector mode of AP and not by RLDP.
- In a High Availability scenario, if the rogue detection security level is set to either High or Critical, the rogue timer on the standby controller starts only after the rogue detection pending stabilization time, which is 300 seconds. Therefore, the active configurations on the standby controller are reflected only after 300 seconds.

- After an AP is moved from rogue detection mode to any other mode or after an AP is moved from sniffer mode to local or monitor mode, the rogue detection functionality is not retained on the AP. To enable rogue detection functionality on the AP, you have to explicitly move the AP to the rogue detection mode.
- Some rogue devices exhibit RSSI value of –128 dBm although the minimum RSSI has seen configured to a higher value. In some scenarios, APs show the RSSI value of 0 for some rogue devices. If the controller receives the RSSI value as 0, the controller invalidates the value and replaces it with –128 dBm so that rogue rules or policies are not applied to the rogue device.
- Even though rogue events are reported to Cisco DNA Center instantly, due to a big number of rogue events, the rogue sync occurs only on detection, on moving to contained state, and every half hour. The rogue sync does not occur for any other rogue event.

Note A rogue AP or client or adhoc containment configuration is not saved after the reload. You have to configure all the rogues again after the reload.

Note No separate command exists for controlling rogue client traps. However, you can enable or disable rogue client traps using the **config trapflags rogueap** {**enable** | **disable**} command, which is also used for rouge APs. In GUI configuration also, you should use the rogue AP flag under **Management** > **SNMP** > **TrapControl** > **Security** > **Rogue AP** to control rogue clients.

Restrictions on Rogue Detection

- Rogue containment is not supported on DFS channels.

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature.

RLDP has 100 % accuracy in rouge AP detection. It detects Open APs and NAT APs.

Note Use the **debug dot11 rldp enable** command in order to check if the Lightweight AP associates and receives a DHCP address from the rogue AP. This command also displays the UDP packet sent by the Lightweight AP to the controller .

A sample of a UDP (destination port 6352) packet sent by the Lightweight AP is shown here: 0020 0a 01 01 0d 0a 01 .....(.*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 .....x..... 0040 00 00 00 00 00 00 00 00 00 00 00 00

The first 5 bytes of the data contain the DHCP address given to the local mode AP by the rogue AP. The next 5 bytes are the IP address of the controller , followed by 6 bytes that represent the rogue AP MAC address. Then, there are 18 bytes of zeroes.

The following steps describe the functioning of RLDP:

1. Identify the closest Unified AP to the rogue using signal strength values.
2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.
4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the controller 's IP addresses.
5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire.

Note The RLDP packets are unable to reach the controller if filtering rules are placed between the controller 's network and the network where the rogue device is located.

Restrictions for RLDP:

- RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.
- RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.
- Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.
- During RLDP process, the AP is unable to serve clients. This negatively impacts performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.
- RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.
- RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS). If the automatic RLDP attempt does not detect the rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue device.

Detecting Rogue Devices

The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) and the rogue detector mode access point is connected to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authenticated and configured. If RLDP uses FlexConnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen (auto-configuration), the RLDP process is initiated.

You can configure the controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the controller to use RLDP on all the access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration. Retries can be configured using the **config rogue ap rldp retries** command.

You can initiate or trigger RLDP from controller in three ways:

1. Enter the RLDP initiation command manually from the controller CLI. The equivalent GUI option for initiating RLDP is not supported.

   config rogue ap rldp initiate *mac-address*

2. Schedule RLDP from the controller CLI. The equivalent GUI option for scheduling RLDP is not supported.

   config rogue ap rldp schedule

3. Auto RLDP. You can configure auto RLDP on controller either from controller CLI or GUI but keep in mind the following guidelines:

   - The auto RLDP option can be configured only when the rogue detection security level is set to custom.
   - Either auto RLDP or schedule of RLDP can be enabled at a time.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.
- Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

Cisco Prime Infrastructure Interaction and Rogue Detection

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:

- If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.
- If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points that are categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

This section contains the following subsections:

Configuring Rogue Detection (GUI)

Step 1 Make sure that rogue detection is enabled on the corresponding access points. Rogue detection is enabled by default for all access points joined to the controller (except for OfficeExtend access points). However, you can enable or disable rogue detection for individual access points by selecting or unselecting the **Rogue Detection** check box on the **All APs > Details for (Advanced)** page.

Step 2 Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **General**.

The **Rogue Policies** page is displayed.

Step 3 Choose the **Rogue Detection Security Level** from the following options:

- **Low**—Basic rogue detection for small-scale deployments.
- **High**—Basic rogue detection with auto containment for medium-scale deployments.
- **Critical**—Basic rogue detection with auto containment and RLDP for highly sensitive deployments.
- **Custom**

Note For auto RLDP, set the security level to **Custom** mode. Do not enable scheduling for RLDP even in the **Custom** mode.

Step 4 Choose one of the following options from the **Rogue Location Discovery Protocol** drop-down list:

- **Disable**—Disables RLDP on all the access points. This is the default value.
- **All APs**—Enables RLDP on all the access points.
- **Monitor Mode APs**—Enables RLDP only on the access points in the monitor mode.

Step 5 In the **Expiration Timeout for Rogue AP and Rogue Client Entries** text box, enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds, and the default value is 1200 seconds.

Note If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.

Step 6 To use the AAA server or local database to validate if rogue clients are valid clients, select the **Validate Rogue Clients Against AAA** check box. By default, the check box is unselected.

Note To validate a rogue client against AAA, the format of the Cisco AVP pair is mandatory. The free RADIUS format is:

- e09d3166fb2c Cleartext-Password := "e09d3166fb2c"
- Cisco-AVPair := "rogue-ap-state=threat"

Step 7 To use the Cisco Mobility Services Engine (MSE) that has the rogue client details to validate the clients, select the **Validate Rogue Clients Against MSE** check box.

MSE responds with information about whether the rogue client is a valid learned client or not. The controller can contain or consider the rogue client as a threat.

Step 8 If necessary, select the **Detect and Report Ad-Hoc Networks** check box to enable ad hoc rogue detection and reporting. By default, the check box is selected.

Step 9 In the **Rogue Detection Report Interval** text box, enter the time interval, in seconds, at which APs send the rogue detection report to the Cisco WLC. The valid range is 10 to 300 seconds, and the default value is 10 seconds.

Note The minimum value of 10 seconds is applicable only to APs in monitor mode. For the APs in Local mode, the minimum interval value that you can set is 30 seconds.

Step 10 In the **Rogue Detection Minimum RSSI** text box, enter the minimum Received Signal Strength Indicator (RSSI) value for APs to detect the rogue and for a rogue entry to be created in the controller. The valid range is –128 dBm to –0 dBm, and the default value is 0 dBm.

Note This feature is applicable to all the AP modes. There can be many rogues with weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs detect rogues.

Step 11 In the **Rogue Detection Transient Interval** text box, enter the time interval at which a rogue should be scanned for by the AP after the first time the rogue is scanned. After the rogue is scanned for consistently, updates are sent periodically to the controller. Thus, the APs filter the transient rogues, which are active for a short period and are then silent. The valid range is between 120 to 1800 seconds, and the default value is 0.

The rogue detection transient interval is applicable to the monitor mode APs only.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues is avoided.

Step 12 In the **Rogue Client Threshold** text box, enter the threshold value. A value of 0 disables the rogue client threshold parameter.

Step 13 Enable or disable the **Rogue Containment Automatic Rate Selection** check box.

Using this option, you can optimize the rate to use the best rate for the target rogue. The AP selects the best rate based on rogue RSSI.

Step 14 If you want the controller to automatically contain certain rogue devices, enable the following parameters. By default, these parameters are in disabled state.

Caution When you select any of the Auto Contain parameters and click **Apply**, the following message is displayed: "Using this feature may have legal consequences. Do you want to continue?" The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

- **Auto Containment Level**—Set the auto containment level. By default, the auto containment level is set to **1**.

  If you choose **Auto**, the controller dynamically chooses the number of APs required for effective containment.

- **Auto Containment only for Monitor mode APs**—Configure the monitor mode access points for auto-containment.
- **Auto Containment on FlexConnect Standalone**—Configure the FlexConnect Standalone mode access points for auto containment.

Note The auto-containment is continued if it was configured when the AP was in connected FlexConnect mode. After the standalone AP reassociates with the controller, auto containment is stopped. The configuration on the controller the AP is associated with determines the future course of action. You can also configure auto containment on the ad hoc SSIDs and managed SSIDs on FlexConnect APs.

- **Rogue on Wire**—Configure the auto containment of rogues that are detected on the wired network.
- **Using Our SSID**—Configure the auto containment of rogues that are advertising your network's SSID. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
- **Valid Client on Rogue AP**—Configure the auto containment of a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
- **AdHoc Rogue AP**—Configure the auto containment of ad hoc networks detected by the controller. If you leave this parameter unselected, the controller only generates an alarm when such a network is detected.

Step 15 Click **Apply**.

Step 16 Click **Save Configuration**.

Configuring Rogue Detection (CLI)

Step 1 Ensure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all the access points that are associated with the controller. You can enable or disable rogue detection for individual access points by entering this command:

config rogue detection {**enable** | **disable**} *cisco-ap command.*

Note To see the current rogue detection configuration for a specific access point, enter the **show ap config general** *Cisco_AP* command.

Note Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

Step 2 Configure the rogue detection security level by entering this command:

config rogue detection security-level {**critical** | **custom** | **high** | **low**}

- **critical**—Basic rogue detection with auto containment and RLDP for highly sensitive deployments.
- **high**—Basic rogue detection with auto containment for medium-scale deployments.
- **low**—Basic rogue detection for small-scale deployments.

Step 3 Enable, disable, or initiate RLDP by entering these commands:

- **config rogue ap rldp enable alarm-only**—Enables RLDP on all the access points.
- **config rogue ap rldp enable alarm-only** *monitor_ap_only*—Enables RLDP only on the access points in the monitor mode.
- **config rogue ap rldp initiate** *rogue_mac_address*—Initiates RLDP on a specific rogue access point.
- **config rogue ap rldp disable**—Disables RLDP on all the access points.

- **config rogue ap rldp retries**—Specifies the number of times RLDP to be tried per rogue access point. The range is from 1 to 5 and default is 1.

Step 4 Specify the number of seconds after which the rogue access point and client entries expire and are removed from the list by entering this command:

config rogue ap timeout *seconds*

The valid range for the *seconds* parameter is 240 to 3600 seconds (inclusive). The default value is 1200 seconds.

Note If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for a classification type.

Step 5 Enable or disable ad hoc rogue detection and reporting by entering this command:

config rogue adhoc {**enable** | **disable**}

Step 6 Enable or disable the AAA server or local database to validate if rogue clients are valid clients by entering this command:

config rogue client aaa {**enable** | **disable**}

Step 7 Enable or disable the use of MSE that has the rogue client details to validate the clients by entering this command:

config rogue client mse {**enable** | **disable**}

Step 8 Specify the time interval, in seconds, at which APs should send the rogue detection report to the controller by entering this command:

config rogue detection monitor-ap report-interval *time in sec*

The valid range for the *time in sec* parameter is 10 seconds to 300 seconds. The default value is 10 seconds.

Note This feature is applicable only to the monitor mode APs.

Step 9 Specify the minimum RSSI value that rogues should have for APs to detect them and for the rogue entries to be created in the controller by entering this command:

config rogue detection min-rssi *rssi in dBm*

The valid range for the *rssi in dBm* parameter is –128 dBm to 0 dBm. The default value is 0 dBm.

Note This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.

Step 10 Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned for by entering this command:

config rogue detection monitor-ap transient-rogue-interval *time in sec*

The valid range for the *time in sec* parameter is 120 seconds to 1800 seconds. The default value is 0.

Note This feature is applicable only to the monitor mode APs.

Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter rogues based on their transient interval values.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues are avoided.

Step 11 If you want the controller to automatically contain certain rogue devices, enter these commands.

Caution When you enter any of these commands, the following message is displayed: `Using this feature may have legal consequences. Do you want to continue?` The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

- **config rogue ap rldp enable auto-contain**—Automatically contains the rogues that are detected on the wired network.
- **config rogue ap ssid auto-contain**—Automatically contains the rogues that are advertising your network's SSID.

  Note If you want the controller to only generate an alarm when such a rogue is detected, enter the **config rogue ap ssid alarm** command.

- **config rogue ap valid-client auto-contain**—Automatically contains a rogue access point to which trusted clients are associated.

  Note If you want the controller to only generate an alarm when such a rogue is detected, enter the **config rogue ap valid-client alarm** command.

- **config rogue adhoc auto-contain**—Automatically contains ad hoc networks detected by the controller.

  Note If you want the controller to only generate an alarm when such a network is detected, enter the **config rogue adhoc alert** command.

- **config rogue auto-contain level** *level monitor_mode_ap_only*—Sets the auto containment level for the monitor mode access points. The default value is 1. If you enter the level as 0, then the controller dynamically chooses the number of APs required for effective containment.
- **config rogue containment flexconnect** {**enable** | **disable**}—Sets the auto containment options for standalone FlexConnect access points.

  Note The auto containment is continued if the auto containment was configured when the AP was in the connected FlexConnect mode. After the standalone AP is reassociated with the controller, auto containment is stopped and the future course of action is determined by the configuration on the controller the AP is associated with. You can also configure auto containment on ad hoc SSIDs and managed SSIDs on FlexConnect APs.

- **config rogue containment auto-rate** {**enable** | **disable**}—Sets the auto rate for containment of rogues.

Step 12 Configure ad hoc rogue classification by entering these commands:

- **config rogue adhoc classify friendly state** {**internal** | **external**} *mac-addr*
- **config rogue adhoc classify malicious state** {**alert** | **contain**} *mac-addr*
- **config rogue adhoc classify unclassified state** {**alert** | **contain**} *mac-addr*

The following is a brief description of the parameters:

- **internal**—Trusts a foreign ad hoc rogue.
- **external**—Acknowledges the presence of an ad hoc rogue.
- **alert**—Generates a trap when an ad hoc rogue is detected.
- **contain**—Starts containing a rogue ad hoc.

Step 13 Configure RLDP scheduling by entering this command:

config rogue ap rldp schedule { **add** | **delete** | **disable** | **enable** }

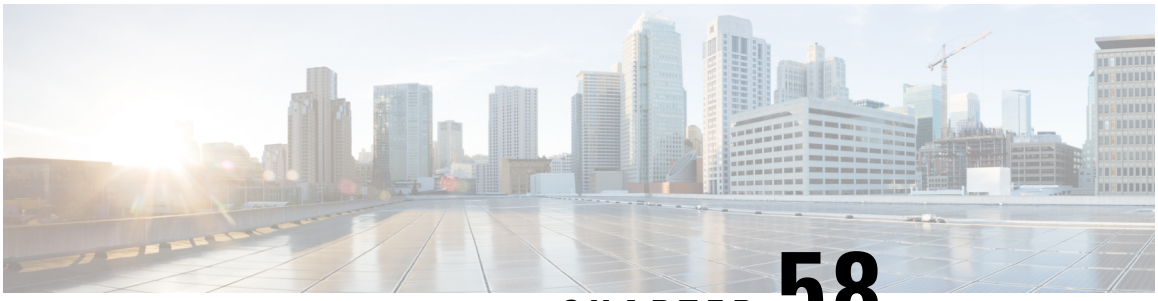
- **add**—Enables you to schedule RLDP on a particular day of the week. You must enter the day of the week (for example, **mon**, **tue**, **wed**, and so on) on which you want to schedule RLDP and the start time and end time in HH:MM:SS format. For example: **config rogue ap rldp schedule add mon 22:00:00 23:00:00**.
- **delete**—Enables you to delete the RLDP schedule. You must enter the number of days.
- **disable**— Configure to disable RLDP scheduling.
- **enable**— Configure to enable RLDP scheduling.

Note When you configure RLDP scheduling, it is assumed that the scheduling will occur in the future, that is, after the configuration is saved.

Step 14 Save your changes by entering this command:

save config

Note Rogue client detection on non monitor AP on serving channel was not done until 8.1 Release . From Release 8.1 onwards, serving channel rogue client detection will happen only if WIPS submode is turned on non monitor AP's.



CHAPTER 58

Classifying Rogue Access Points

- Rogue Access Point Classification, on page 481
- Guidelines and Restrictions for Classifying Rogue Access Points, on page 484
- Configuring Rogue Classification Rules (GUI), on page 484
- Viewing and Classifying Rogue Devices (GUI), on page 487
- Configuring Rogue Classification Rules (CLI), on page 490
- Viewing and Classifying Rogue Devices (CLI), on page 493

Rogue Access Point Classification

The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, Custom, or Unclassified. For the Custom type, you must specify a severity score and a classification name.

Note Manual classification and classification that is the result of auto-containment or rogue-on-wire overrides the rogue rule. If you have manually changed the class and/or the state of a rogue AP, then to apply rogue rules to the AP, you must change it to unclassified and alert condition.

Note If you manually move any rogue device to contained state (any class) or friendly state, this information is stored in the standby Cisco WLC flash memory; however, the database is not updated. When HA switchover occurs, the rogue list from the previously standby Cisco WLC flash memory is loaded.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, custom, and unclassified) in the Alert state only.

You can configure up to 64 rogue classification rules per controller.

You can also apply rogue rules to ad hoc rogues except for client count condition.

The number of rogue clients that can be stored in the database table of a rogue access point is 256.

If a rogue AP or an ad hoc rogue is classified because of an RSSI rogue rule condition, the RSSI value that caused the trigger is displayed on the controller GUI/CLI. The controller includes the classified RSSI, the classified AP MAC address, and rule name in the trap. A new trap is generated for every new classification or change of state due to rogue rule but[3] is rate limited to every half hour for every rogue AP or ad hoc rogue. However, if there is a change of state in containment by rogue rule, the trap is sent immediately. The 'classified by,' 'classified at,' and 'classified by rule name' are valid for the non-default classification types, which are Friendly, Malicious, and Custom classifications. For the unclassified types, these fields are not displayed.

Note For the RSSI condition of rogue rule, reclassification occurs only if the RSSI change is more than 2 dBm of the configured RSSI value.

The rogue rule may not work properly if friendly rogue rule is configured with RSSI as a condition. Then, you need to modify the rules with the expectation that friendly rule is using maximum RSSI and modify rules accordingly.

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

Table 17: Classification Mapping

Rule-Based Classification Type	Rogue States
Friendly	• Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. An example is the access points in your lab network. • External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. An example is an access point that belongs to a neighboring coffee shop. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.
Malicious	• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained.
Custom	• Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained.
Unclassified	• Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list. • Contained—The unknown access point is contained. • Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

The classification and state of the rogue access points are configured as follows:

- From Known to Friendly, Internal
- From Acknowledged to Friendly, External
- From Contained to Malicious, Contained

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

This section contains the following subsections:

Guidelines and Restrictions for Classifying Rogue Access Points

- Classifying Custom type rogues is tied to rogue rules. Therefore, it is not possible to manually classify a rogue as Custom. Custom class change can occur only when rogue rules are used.
- Some are sent for containment by rule and every 30 minutes for rogue classification change. For custom classification, the first trap does not contain the severity score because the trap has existed before the custom classification. The severity score is obtained from the subsequent trap that is generated after 30 minutes if the rogue is classified.
- Rogue rules are applied on every incoming new rogue report in the controller in the order of their priority.
- After a rogue satisfies a higher priority rule and is classified, it does not move down the priority list for the same report.
- Previously classified rogue gets re-classified on every new rogue report with the following restrictions:
  - Rogues which are classified as friendly by rule and whose state is set to ALERT, go through re-classification on receiving the new rogue report.
  - If a rogue is classified as friendly by the administrator manually, then the state is INTERNAL and it does not get re-classified on successive rogue reports.
  - If rogue is classified as malicious, irrespective of the state it does not get re-classified on subsequent rogue reports.
- Transition of the rogue's state from friendly to malicious is possible by multiple rogue rules if some attribute is missing in new rogue report.
- Transition of the rogue's state from malicious to any other classification is not possible by any rogue rule.
- If a rogue AP is classified as friendly, it means that the rogue AP exists in the vicinity, is a known AP, and need not be tracked. Therefore, all the rogue clients are either deleted or not tracked if they are associated with the friendly rogue AP.
- Until the controller discovers all the APs through neighbor reports from APs, the rogue APs are kept in unconfigured state for three minutes after they are detected. After 3 minutes, the rogue policy is applied on the rogue APs and the APs are moved to unclassified, friendly, malicious, or custom class. Rogue APs kept in unconfigured state means that no rogue policy has yet been applied on them.

Configuring Rogue Classification Rules (GUI)

Step 1 Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Rogue Rules** to open the Rogue Rules page.

Any rules that have already been created are listed in priority order. The name, type, and status of each rule is provided.

Note To delete a rule, hover your cursor over the blue drop-down arrow for that rule and click **Remove**.

Step 2 Create a new rule as follows:

a) Click **Add Rule**. An Add Rule section appears at the top of the page.

b) In the **Rule Name** text box, enter a name for the new rule. Ensure that the name does not contain any spaces.
c) From the **Rule Type** drop-down list, choose from the following options to classify rogue access points matching this rule as friendly or malicious:

- **Friendly**
- **Malicious**
- **Custom**

d) Configure the notification when the rule is matched from the **Notify** drop-down list to **All**, **Global**, **Local**, or **None**.

Rule description:

- **All**—Notifies the Cisco WLC and a trap receiver such as Cisco Prime Infrastructure.
- **Global**—Notifies only a trap receiver such as Cisco Prime Infrastructure.
- **Local**—Notifies only Cisco WLC.
- **None**—No notifications are sent.

Note Rogue Rule Notification options **All**, **Global**, **Local**, and **None** can control only the following rogue traps mentioned:

- Rogue AP Detected (Rogue AP: XX:XX:XX:XX:XX:XX detected on Base Radio MAC: XX:XX:XX:XX:XX:XX Interface no: 0(1) Channel: 6 RSSI: 45 SNR: 10 Classification: unclassified, State: alert, RuleClassified : unclassified, Severity Score: 100, RuleName: rule1, Classified AP MAC: XX:XX:XX:XX:XX:XX, Classified RSSI: 45)
- Rogue Adhoc Detected (Adhoc Rogue : XX:XX:XX:XX:XX:XX detected on Base Radio MAC : XX:XX:XX:XX:XX:XX Interface no: 0(1) on Channel 6 with RSSI: 45 and SNR: 10 Classification: unclassified, State: alert, RuleClassified: unclassified, Severity Score: 100, RuleName: rule1,Classified APMAC: XX:XX:XX:XX:XX:XX, Classified RSSI: 45)
- Rogue AP contained (Rogue AP: Rogue with MAC Address: XX:XX:XX:XX:XX:XX has been contained due to rule with containment Level : 1)
- Rogue AP clear contained (Rogue AP: Rogue with MAC Address: XX:XX:XX:XX:XX:XX is no longer contained due to rule

e) Configure the state of the rogue AP when the rule is matched from the **State** drop-down list.
f) If you choose the Rule Type as Custom, enter the Severity Score and the Classification Name.
g) Click **Add** to add this rule to the list of existing rules, or click **Cancel** to discard this new rule.

Step 3 Edit a rule as follows:

a) Click the name of the rule that you want to edit. The **Rogue Rule > Edit** page appears.
b) From the Type drop-down list, choose from the following options to classify rogue access points matching this rule:

- **Friendly**
- **Malicious**
- **Custom**

c) Configure the notification when the rule is matched from the **Notify** drop-down list to **All**, **Global**, **Local**, or **None**.

d) Configure the state of the rogue AP when the rule is matched from the **State** drop-down list.
e) From the Match Operation text box, choose one of the following:

Match All—If this rule is enabled, a detected rogue access point must meet all of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule.

Match Any—If this rule is enabled, a detected rogue access point must meet any of the conditions specified by the rule in order for the rule to be matched and the rogue to adopt the classification type of the rule. This is the default value.

f) To enable this rule, select the **Enable Rule** check box. The default value is unselected.
g) If you choose the Rule Type as Custom, enter the Severity Score and the Classification Name.
h) From the Add Condition drop-down list, choose one or more of the following conditions that the rogue access point must meet and click **Add Condition**.

- **SSID**—Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the **User Configured SSID** text box, and click **Add SSID**.

  Note To delete an SSID, highlight the SSID and click **Remove**.

- **RSSI**—Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the **Minimum RSSI** text box. The valid range is 0 to –128 dBm (inclusive).
- **Duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the **Time Duration** text box. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
- **Client Count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the **Minimum Number of Rogue Clients** text box. The valid range is 1 to 10 (inclusive), and the default value is 0.
- **No Encryption**—Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option.

  Note Cisco Prime Infrastructure refers to this option as "Open Authentication."

- **Managed SSID**—Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.

  Note The SSID and Managed SSID conditions cannot be used with the Match All operation because these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

  You can add up to six conditions per rule. When you add a condition, it appears under the Conditions section.

  Note To delete a condition from this rule, hover your cursor over the blue drop-down arrow for that condition and click **Remove**.

- **SSID Wildcard**—Requires that the rogue access point have a substring of the specific user-configured SSID. The controller searches the substring in the same occurrence pattern and returns a match if the substring is found in the whole string of an SSID.

i) Click **Apply**.

Step 4 Click **Save Configuration**.

Step 5 If you want to change the order in which rogue classification rules are applied, follow these steps:

a. Click **Back** to return to the Rogue Rules page.

b. Click **Change Priority** to access the Rogue Rules > Priority page.

The rogue rules are listed in priority order in the Change Rules Priority text box.

c. Highlight the rule for which you want to change the priority, and click **Up** to raise its priority in the list or **Down** to lower its priority in the list.

d. Continue to move the rules up or down until the rules are in the desired order.

e. Click **Apply**.

Step 6 Classify any rogue access points as friendly and add them to the friendly MAC address list as follows:

- Choose **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Friendly Rogue** to open the Friendly Rogue > Create page.
- In the MAC Address text box, enter the MAC address of the friendly rogue access point.
- Click **Apply**.
- Click **Save Configuration**. This access point is added to the controller's list of friendly access points and should now appear on the Friendly Rogue APs page.

Viewing and Classifying Rogue Devices (GUI)

Before you begin

Caution When you choose to **contain a rogue device**, the following warning appears: "There may be legal issues following this containment. Are you sure you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Step 1 Choose **Monitor** > **Rogues**.

Step 2 Choose the following options to view the different types of rogue access points detected by the controller:

- **Friendly APs**
- **Malicious APs**

- **Unclassified APs**
- **Custom APs**

The respective rogue APs pages provide the following information: the MAC address and SSID of the rogue access point, channel number, the number of radios that detected the rogue access point, the number of clients connected to the rogue access point, and the current status of the rogue access point.

Note To remove acknowledged rogues from the database, change the rogue state to Alert. If the rogue is no longer present, the rogue data is deleted from the database in 20 minutes.

Note To delete a rogue access point from one of these pages, hover your cursor over the blue drop-down arrow and click **Remove**. To delete multiple rogue access points, select the check box corresponding to the row you want to delete and click **Remove**.

Note You can move the Malicious or Unclassified rogue APs that are being contained or were contained back to Alert state by clicking the **Move to Alert** button on the respective pages.

Step 3 Get more details about a rogue access point by clicking the MAC address of the access point. The Rogue AP Detail page appears.

This page provides the following information: the MAC address of the rogue device, the type of rogue device (such as an access point), whether the rogue device is on the wired network, the dates and times when the rogue device was first and last reported, and the current status of the device.

The Class Type text box shows the current classification for this rogue access point:

- **Friendly**—An unknown access point that matches the user-defined friendly rules or an existing known and acknowledged rogue access point. Friendly access points cannot be contained.
- **Malicious**—An unknown access point that matches the user-defined malicious rules or is moved manually by the user from the Friendly or Unclassified classification type.

  Note Once an access point is classified as Malicious, you cannot apply rules to it in the future, and it cannot be moved to another classification type. If you want to move a malicious access point to the Unclassified classification type, you must delete the access point and allow the controller to reclassify it.

- **Unclassified**—An unknown access point that does not match the user-defined friendly or malicious rules. An unclassified access point can be contained. It can also be moved to the Friendly or Malicious classification type automatically in accordance with user-defined rules or manually by the user.
- **Custom**—A user-defined classification type that is tied to rogue rules. It is not possible to manually classify a rogue as Custom. Custom class change can occur only using rogue rules.

Step 4 If you want to change the classification of this device, choose a different classification from the Class Type drop-down list.

Note A rogue access point cannot be moved to another class if its current state is Contain.

Step 5 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue access point:

- **Internal**—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly.
- **External**—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly.

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

The bottom of the page provides information on both the access points that detected this rogue access point and any clients that are associated to it. To see more details for any of the clients, click **Edit** to open the Rogue Client Detail page.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Step 8 View any rogue clients that are connected to the controller by choosing **Rogue Clients**. The Rogue Clients page appears. This page shows the following information: the MAC address of the rogue client, the MAC address of the access point to which the rogue client is associated, the SSID of the rogue client, the number of radios that detected the rogue client, the date and time when the rogue client was last reported, and the current status of the rogue client.

Step 9 Obtain more details about a rogue client by clicking the MAC address of the client. The Rogue Client Detail page appears.

This page provides the following information: the MAC address of the rogue client, the MAC address of the rogue access point to which this client is associated, the SSID and IP address of the rogue client, the dates and times when the rogue client was first and last reported, and the current status of the rogue client.

Step 10 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue client:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.

The bottom of the page provides information on the access points that detected this rogue client.

Step 11 Click **Apply**.

Step 12 If desired, you can test the controller's connection to this client by clicking **Ping**.

Step 13 Click **Save Configuration**.

Step 14 See any ad-hoc rogues detected by the controller by choosing **Adhoc Rogues**. The Adhoc Rogues page appears.

This page shows the following information: the MAC address, BSSID, and SSID of the ad-hoc rogue, the number of radios that detected the ad-hoc rogue, and the current status of the ad-hoc rogue.

Step 15 Obtain more details about an ad-hoc rogue by clicking the MAC address of the rogue. The Adhoc Rogue Detail page appears.

This page provides the following information: the MAC address and BSSID of the ad-hoc rogue, the dates and times when the rogue was first and last reported, and the current status of the rogue.

Step 16 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this ad-hoc rogue:

- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action.

- **Internal**—The controller trusts this rogue access point.
- **External**—The controller acknowledges the presence of this rogue access point.

Step 17 From the Maximum number of APs to contain the rogue drop-down list, choose one of the following options to specify the maximum number of access points used to contain this ad-hoc rogue: **1**, **2**, **3**, or **4**.

The bottom of the page provides information on the access points that detected this ad-hoc rogue.

- **1**—Specifies targeted rogue access point is contained by one access point. This is the lowest containment level.
- **2**—Specifies targeted rogue access point is contained by two access points.
- **3**—Specifies targeted rogue access point is contained by three access points.
- **4**—Specifies targeted rogue access point is contained by four access points. This is the highest containment level.

Step 18 Click **Apply**.

Step 19 Click **Save Configuration**.

Step 20 View any access points that have been configured to be ignored by choosing **Rogue AP Ignore-List**. The Rogue AP Ignore-List page appears.

This page shows the MAC addresses of any access points that are configured to be ignored. The rogue-ignore list contains a list of any autonomous access points that have been manually added to Cisco Prime Infrastructure maps by the users. The controller regards these autonomous access points as rogues even though the Prime Infrastructure is managing them. The rogue-ignore list allows the controller to ignore these access points. The list is updated as follows:

- When the controller receives a rogue report, it checks to see if the unknown access point is in the rogue-ignore access point list.
- If the unknown access point is in the rogue-ignore list, the controller ignores this access point and continues to process other rogue access points.
- If the unknown access point is not in the rogue-ignore list, the controller sends a trap to the Prime Infrastructure. If the Prime Infrastructure finds this access point in its autonomous access point list, the Prime Infrastructure sends a command to the controller to add this access point to the rogue-ignore list. This access point is then ignored in future rogue reports.
- If a user removes an autonomous access point from the Prime Infrastructure, the Prime Infrastructure sends a command to the controller to remove this access point from the rogue-ignore list.

Configuring Rogue Classification Rules (CLI)

Step 1 Create a rule by entering this command:

config rogue rule add ap priority *priority* **classify** {**friendly** | **malicious**} *rule-name*

If you later want to change the priority of this rule and shift others in the list accordingly, enter the **config rogue rule priority** *priority rule-name* command.

If you later want to change the classification of this rule, enter the **config rogue rule classify** {**friendly** | **malicious**} *rule-name* command.

If you ever want to delete all of the rogue classification rules or a specific rule, enter the {**config rogue rule delete** {**all** | *rule-name*} command.

Step 2 Create a rule by entering these commands:

- Configure a rule for friendly rogues by entering this command:

  config rogue rule add ap priority *priority* **classify friendly notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **internal** | **external** | **delete**} *rule-name*

- Configure a rule for malicious rogues by entering this command:

  config rogue rule add ap priority *priority* **classify malicious notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **contain** | **delete**} *rule-name*

- Configure a rule for custom rogues by entering this command:

  config rogue rule add ap priority *priority* **classify custom** *severity-score classification-name* **notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **contain** | **delete**} *rule-name*

If you later want to change the priority of this rule and shift others in the list accordingly, enter the **config rogue rule priority** *priority rule-name* command.

If you later want to change the classification of this rule, enter the **config rogue rule classify** {**friendly** | **malicious** | **custom** *severity-score classification-name*} *rule-name* command.

If you ever want to delete all of the rogue classification rules or a specific rule, enter the {**config rogue rule delete** {**all** | *rule-name*} command.

Step 3 Configure the state on the rogue AP upon rule match by entering this command:

config rogue rule state {**alert** | **contain** | **internal** | **external** | **delete**} *rule-name*

Step 4 Configure the notification upon rule match by entering this command:

config rogue rule notify {**all** | **global** | **local** | **none**} *rule-name*

Step 5 Disable all rules or a specific rule by entering this command:

config rogue rule disable {*all* | *rule_name*}

Note A rule must be disabled before you can modify its attributes.

Step 6 Add conditions to a rule that the rogue access point must meet by entering this command:

config rogue rule condition ap set *condition_type condition_value rule_name*

The following condition types are available:

- **ssid**—Requires that the rogue access point have a specific SSID. You should add SSIDs that are not managed by the controller. If you choose this option, enter the SSID for the *condition_value parameter*. The SSID is added to the user-configured SSID list.

  Note If you ever want to delete all of the SSIDs or a specific SSID from the user-configured SSID list, enter the **config rogue rule condition ap delete ssid** {**all** | **ssid**} *rule_name* command.

Note The sub-string should be specified in full or part of SSID (without any asterisks). This sub-string is matched in the same sequence to its occurrence in the rogue AP SSID. Once the condition is met, the rogue AP is classified (depending on OR or AND match condition).

- **rssi**—Requires that the rogue access point have a minimum RSSI value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value for the *condition_value parameter*.

  In Release 8.0 and later releases, for friendly rogue rules, you are required to set a maximum RSSI value. The RSSI value of the rogue AP must be less than the RSSI value set, for the rogue AP to be classified as a friendly rogue. For malicious and custom rogue rules, there is no change in functionality.

  For example, for a friendly rogue rule, the RSSI value is set at –80 dBm. All the rogue APs that are detected and have RSSI value that is less than –80 dBm are classified as friendly rogues. For malicious and custom rogue rules, the RSSI value is set at –80 dBm. All the rogue APs that are detected and have RSSI value that is more than –80 dBm are classified as malicious or custom rogue APs.

- **duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the *condition_value parameter*. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.

- **client-count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point for the *condition_value parameter*. The valid range is 1 to 10 (inclusive), and the default value is 0.

- **managed-ssid**—Requires that the rogue access point's SSID be known to the controller. A *condition_value parameter* is not required for this option.

  Note You can add up to six conditions per rule. If you ever want to delete all of the conditions or a specific condition from a rule, enter the **config rogue rule condition ap delete all** *condition_type condition_value rule_name* command.

- **wildcard-ssid**—Requires that the rogue access point have a wildcard of the specific user-configured SSID. The controller searches the wildcard in the same occurrence pattern and returns a match if the substring is found in the whole string of an SSID.

Step 7 Specify whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule by entering this command:

config rogue rule match {**all** | **any**} *rule_name*

Step 8 Enable all rules or a specific rule by entering this command:

config rogue rule enable {**all** | **rule_name**}

Note For your changes to become effective, you must enable the rule.

Step 9 Add a new friendly access point entry to the friendly MAC address list or delete an existing friendly access point entry from the list by entering this command:

config rogue ap friendly {**add** | **delete**} *ap_mac_address*

Step 10 Save your changes by entering this command:

save config

Step 11 View the rogue classification rules that are configured on the controller by entering this command:
show rogue rule summary

Step 12 View detailed information for a specific rogue classification rule by entering this command:
show rogue rule detailed *rule_name*

Viewing and Classifying Rogue Devices (CLI)

Procedure

- View a list of all rogue access points detected by the controller by entering this command:
  show rogue ap summary
- See a list of the friendly rogue access points detected by the controller by entering this command:
  show rogue ap friendly summary
- See a list of the malicious rogue access points detected by the controller by entering this command:
  show rogue ap malicious summary
- See a list of the unclassified rogue access points detected by the controller by entering this command:
  show rogue ap unclassified summary
- See detailed information for a specific rogue access point by entering this command:
  show rogue ap detailed *ap_mac_address*
- See the rogue report (which shows the number of rogue devices detected on different channel widths) for a specific 802.11a/n/ac radio by entering this command:
  show ap auto-rf 802.11a *Cisco_AP*
- See a list of all rogue clients that are associated to a rogue access point by entering this command:
  show rogue ap clients *ap_mac_address*
- See a list of all rogue clients detected by the controller by entering this command:
  show rogue client summary
- See detailed information for a specific rogue client by entering this command:
  show rogue client detailed *Rogue_AP client_mac_address*
- See a list of all ad-hoc rogues detected by the controller by entering this command:
  show rogue adhoc summary
- See detailed information for a specific ad-hoc rogue by entering this command:
  show rogue adhoc detailed *rogue_mac_address*
- See a summary of ad hoc rogues based on their classification by entering this command:
  show rogue adhoc {**friendly** | **malicious** | **unclassified**} **summary**

- See a list of rogue access points that are configured to be ignore by entering this command:

  show rogue ignore-list

- Classify a rogue access point as friendly by entering this command:

  config rogue ap classify friendly state {**internal** | **external**} *ap_mac_address*

  where

  internal means that the controller trusts this rogue access point.

  external means that the controller acknowledges the presence of this rogue access point.

Note A rogue access point cannot be moved to the Friendly class if its current state is Contain.

- Mark a rogue access point as malicious by entering this command:

  config rogue ap classify malicious state {**alert** | **contain**} *ap_mac_address*

  where

  alert means that the controller forwards an immediate alert to the system administrator for further action.

  contain means that the controller contains the offending device so that its signals no longer interfere with authorized clients.

Note A rogue access point cannot be moved to the Malicious class if its current state is Contain.

- Mark a rogue access point as unclassified by entering this command:

  config rogue ap classify unclassified state {**alert** | **contain**} *ap_mac_address*

Note A rogue access point cannot be moved to the Unclassified class if its current state is Contain.

alert means that the controller forwards an immediate alert to the system administrator for further action.

contain means that the controller contains the offending device so that its signals no longer interfere with authorized clients.

- Choose the maximum number of access points used to contain the ad-hoc rogue by entering this command:

  config rogue ap classify unclassified state contain *rogue_ap_mac_address 1, 2, 3, or 4*

  - **1**—Specifies targeted rogue access point will be contained by one access point. This is the lowest containment level.
  - **2**—Specifies targeted rogue access point will be contained by two access points.
  - **3**—Specifies targeted rogue access point will be contained by three access points.
  - **4**—Specifies targeted rogue access point will be contained by four access points. This is the highest containment level.

- Specify how the controller should respond to a rogue client by entering one of these commands:

  config rogue client alert *client_mac_address*—The controller forwards an immediate alert to the system administrator for further action.

  config rogue client contain *client_mac_address*—The controller contains the offending device so that its signals no longer interfere with authorized clients.

- Specify how the controller should respond to an ad-hoc rogue by entering one these commands:

  config rogue adhoc alert *rogue_mac_address*—The controller forwards an immediate alert to the system administrator for further action.

  config rogue adhoc contain *rogue_mac_address*—The controller contains the offending device so that its signals no longer interfere with authorized clients.

  config rogue adhoc external *rogue_mac_address*—The controller acknowledges the presence of this ad-hoc rogue.

- Configure the classification of ad hoc rogues by entering any one of these commands:
  - Friendly state—**config rogue adhoc classify friendly state** {**internal** | **external**} *mac-addr*
  - Malicious state—**config rogue adhoc classify malicious state** {**alert** | **contain**} *mac-addr*
  - Unclassified state—**config rogue adhoc classify unclassified state** {**alert** | **contain**} *mac-addr*
- View a summary of custom rogue AP information by entering this command:

  show rogue ap custom summary

- See custom ad hoc rogue information by entering this command:

  show rogue adhoc custom summary

- Delete the rogue APs by entering this command:

  config rogue ap delete {**class** | **all** | *mac-addr*}

- Delete the rogue clients by entering this command:

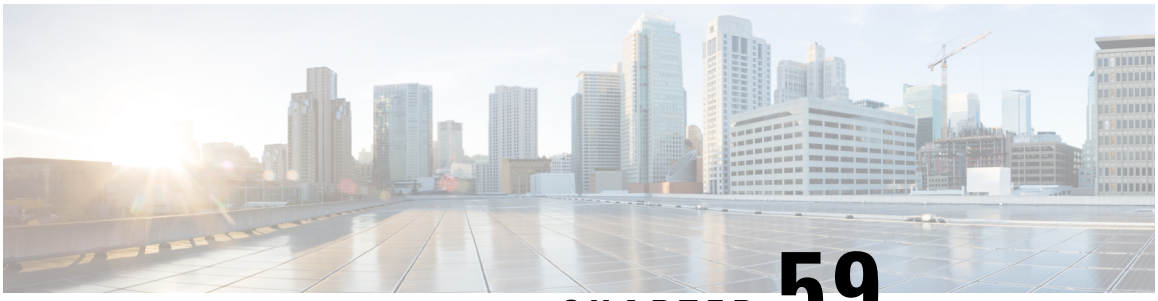
  config rogue client delete {**state** | **all** | *mac-addr*}

- Delete the ad hoc rogues by entering this command:

  config rogue adhoc delete {**class** | **all** | *mac-addr*}

- Save your changes by entering this command:

  save config



CHAPTER 59

Configuring Cisco TrustSec SXP

- Cisco TrustSec, on page 497
- Guidelines and Restrictions on Cisco TrustSec, on page 499
- Configuring SXP on Cisco WLC (GUI), on page 499
- Creating a New SXP Connection (GUI), on page 500
- Configuring SXP on Cisco WLC (CLI), on page 500

Cisco TrustSec

Cisco TrustSec enables organizations to secure their networks and services through identity-based access control to anyone, anywhere, anytime. The solution also offers data integrity and confidentiality services, policy-based governance, and centralized monitoring, troubleshooting, and reporting services. You can combine Cisco TrustSec with personalized, professional service offerings to simplify the solution deployment and management, and is a foundational security component to Cisco Borderless Networks.

The Cisco TrustSec security architecture helps build secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between the devices in the domain is secured with a combination of encryption, message integrity check, and data path replay protection mechanisms. Cisco TrustSec uses a device and user credentials that are acquired during authentication for classifying the packets by security groups (SGs), as they enter the network. This packet classification is maintained by tagging packets on an ingress to the Cisco TrustSec network. This is because they can be correctly identified to apply security and other policy criteria along the data path. The tag, called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. Note that the Cisco TrustSec security group tag is applied only when you enable AAA override on a WLAN.

One of the components of Cisco TrustSec architecture is the security group-based access control. In the security group-based access control component, access policies in the Cisco TrustSec domain are topology-independent, based on the roles (as indicated by the security group number) of source and destination devices rather than on network addresses. Individual packets are tagged with the security group number of the source.

The Cisco TrustSec solution is implemented across the following three distinct phases:

- Client classification at ingress by a centralized policy database (Cisco ISE) and assigning unique SGT to clients based on client identity attributes such as the role and so on.
- Propagation of IP-to-SGT binding to neighboring devices using the SGT Exchange Protocol (SXP) or inline tagging methods or both.

- Security Group Access Control List (SGACL) policy enforcement. Cisco AP is the enforcement point for central or local switching (central authentication).

For more information about deploying the Cisco TrustSec solution, see the *Wireless TrustSec Deployment Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_wireless_trustsec_deployment_guide.html.

SGT Exchange Protocol

Cisco devices use the SGT Exchange Protocol (SXP) to propagate SGTs across network devices that do not have any hardware support for Cisco TrustSec. The SXP is the software solution to eliminate the need for upgrade of Cisco TrustSec hardware on all Cisco switches. Controller supports the SXP as part of the Cisco TrustSec architecture. The SXP sends SGT information to the Cisco TrustSec-enabled switches so that appropriate role-based access control lists (RBAC lists) can be activated. This depends on the role information present in the SGT. To implement the SXP on a network, only the egress distribution switch has to be Cisco TrustSec-enabled. All the other switches can be non-Cisco TrustSec-capable switches.

The SXP runs between the access layer and the distribution switch or between two distribution switches. The SXP uses TCP as the transport layer. Cisco TrustSec authentication is performed for the host (client) joining the network on the access layer switch. This is similar to an access switch with the hardware that is enabled with Cisco TrustSec. The access layer switch is not Cisco TrustSec hardware enabled. Therefore, data traffic is not encrypted or cryptographically authenticated when it passes through the access layer switch. The SXP is used to pass the IP address of the authenticated device, which is a wireless client and the corresponding SGT up to the distribution switch. If the distribution switch is a hardware that is enabled with Cisco TrustSec, the switch inserts the SGT into the packet on behalf of the access layer switch. If the distribution switch is not a hardware that is enabled with Cisco TrustSec, the SXP on the distribution switch passes the IP-SGT mapping to all the distribution switches that have the Cisco TrustSec hardware. On the egress side, the enforcement of the RBAC lists occurs at the egress L3 interface on the distribution switch.

The following are some guidelines for Cisco TrustSec SXP:

- The SXP is supported only on the following security policies:
  - WPA2-dot1x
  - WPA-dot1x
  - MAC filtering using RADIUS servers
  - Web authentication using RADIUS servers for user authentication
- The SXP is supported for both IPv4 and IPv6 clients.
- By default, the controller always works in the Speaker mode.
- From Release 8.3, the SXP on the controller is supported for both centrally and locally switched networks.
- It is possible to do IP-SGT mapping on the WLANs as well for clients that are not authenticated by Cisco ISE.

For more information about Cisco TrustSec, see http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html.

Guidelines and Restrictions on Cisco TrustSec

- SXP is not supported on FlexConnect access points.
- SXP is supported only in centrally switched networks that have central authentication.
- By default, SXP is supported for APs that work in local mode only.
- The configuration of the default password should be consistent for both the controller and the switch.
- Fault tolerance is not supported because fault tolerance requires local switching on APs.
- Static IP-SGT mapping for local authentication of users is not supported.
- IP-SGT mapping requires authentication with external Cisco ISE servers.
- In auto-anchor/guest-anchor mobility, the SGT information that is passed by the RADIUS server to a foreign controller can be communicated to the anchor controller through the EoIP/CAPWAP mobility tunnel. The anchor controller can then build the SGT-IP mapping and communicate it to another peer via SXP.
- In a local web authentication with AAA override scenario, if a client tries to login after logging out, SGT from WLAN is not applied again and the client retains the AAA overridden SGT.
- It is possible to change the interface management IP address even if you have Cisco TrustSec SXP in enabled state.

Configuring SXP on Cisco WLC (GUI)

Step 1 Choose **Security** > **TrustSec** > **SXP Config**.

The **SXP Configuration** page is displayed with the following SXP configuration details:

- **Total SXP Connections**—Number of SXP connections that are configured.
- **SXP State**—Status of SXP connections as either disabled or enabled.
- **SXP Mode**—SXP mode of the Cisco WLC. The Cisco WLC is always set to Speaker mode for SXP connections.
- **Default Password**—Password for MD5 authentication of SXP messages. We recommend that the password contain a minimum of 6 characters.
- **Default Source IP**—IP address of the management interface. SXP uses the default source IP address for all new TCP connections.
- **Retry Period**—SXP retry timer. The default value is 120 seconds (2 minutes). The valid range is 0 to 64000 seconds. The SXP retry period determines how often the controller retries for an SXP connection. When an SXP connection is not successfully set up, the controller makes a new attempt to set up the connection after the SXP retry period timer expires. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

This page also displays the following information about SXP connections:

- **Peer IP Address**—The IP address of the peer, that is, the IP address of the next-hop switch to which the Cisco WLC is connected. There is no effect on the existing TCP connections when you configure a new peer connection.
- **Source IP Address**—The IP address of the source, that is, the management IP address of the Cisco WLC.
- **Connection Status**—Status of the SXP connection.

Step 2 From the **SXP State** drop-down list, choose **Enabled** to enable SXP.

Step 3 Enter the default password that should be used to make an SXP connection. We recommend that the password contain a minimum of 6 characters.

Step 4 In the **Retry Period** field, enter the time, in seconds, that determines how often the Cisco TrustSec software retries for an SXP connection.

Step 5 Click **Apply** to commit your changes.

Creating a New SXP Connection (GUI)

Step 1 Choose **SECURITY** > **TrustSec SXP** and click **New** to open the SXP Connection > New page.

Step 2 In the **Peer IP Address** text box, enter the IP address of the next hop switch to which the controller is connected.

Step 3 Click **Apply**.

Configuring SXP on Cisco WLC (CLI)

Procedure

- Enable or disable the SXP on the controller by entering this command:

  config cts sxp {**enable** | **disable**}

- Configure the default password for MD5 authentication of SXP messages by entering this command:

  config cts sxp default password *password*

- Configure the IP address of the next-hop switch with which the controller is connected by entering this command:

  config cts sxp connection peer *ip-address*

- Configure the interval between connection attempts by entering this command:

  config cts sxp retry period *time-in-seconds*

- Remove an SXP connection by entering this command:

  config cts sxp connection delete *ip-address*

- See a summary of the SXP configuration by entering this command:

  show cts sxp summary

The following is a sample output of this command:

```
SXP State..................................... Enable
SXP Mode...................................... Speaker
Default Password.............................. ****
Default Source IP............................. 209.165.200.224
Connection retry open period ................. 120
```

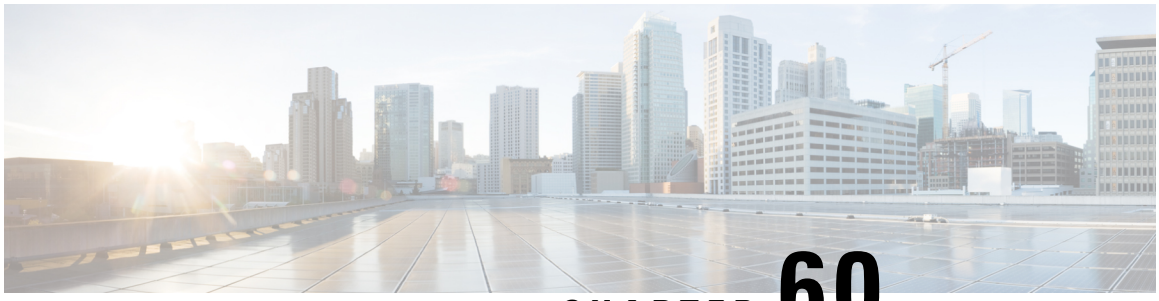
- See the list of SXP connections that are configured by entering this command:

  show cts sxp connections

  The following is a sample output of this command:

```
Total num of SXP Connections..................... 1
SXP State..................................... Enable
Peer IP            Source IP           Connection Status
---------------    ---------------     -----------------
209.165.200.229   209.165.200.224              On
```

- Establish connection between the controller and a Cisco Nexus 7000 Series switch by following either of these steps:
  - Enter the following commands:
    1. **config cts sxp version sxp version 1 or 2** *1*
    2. **config cts sxp disable**
    3. **config cts sxp enable**
  - If SXP version 2 is used on the controller and version 1 is used on the Cisco Nexus 7000 Series switch, an amount of retry period is required to establish the connection. We recommend that you initially have less interval between connection attempts. The default is 120 seconds.



CHAPTER 60

Configuring Local Policies

- Local Policies, on page 503
- Guidelines and Restrictions for Local Policy Classification, on page 504
- Configuring Local Policies (GUI), on page 505
- Configuring Local Policies (CLI), on page 506

Local Policies

Controller can do profiling of devices based on protocols such as HTTP, DHCP, and so on to identify the clients. You can configure the device-based policies and enforce per-user or per-device policy on the network. The controller also displays statistics that are based on per-user or per-device end points and policies that are applicable per device. The maximum number of policies that you can configure is 64.

The policies are defined based on the following attributes:

- User group or user role
- Device type such as Windows clients, smartphones, tablets, and so on
- Service Set Identifier (SSID)
- Location, based on the access point group that the end point is connected to
- Time of the day
- Extensible Authentication Protocol (EAP) type, to check what EAP method that the client is getting connected to

When these policy attributes match, you can define the following actions:

- Virtual local area network (VLAN)
- Access control list (ACL)
- Quality of Service (QoS) level
- Session timeout value
- Sleeping client timeout value

This section contains the following subsections:

Guidelines and Restrictions for Local Policy Classification

- If you enable AAA override and there are AAA attributes other than the role type from the AAA server, the configured policy action is not applied. The AAA override attributes have higher precedence.
- On a WLAN, when local profiling is enabled, RADIUS profiling is not allowed.
- Client profiling uses existing profiles on the controller.
- You cannot create custom profiles.
- Wired clients behind the workgroup bridge (WGB) are not profiled and the policy action is not taken.
- Only the first policy rule which matches with the policy profile is given precedence. Each policy profile has an associated policy rule, which is used to match the policies.
- You can configure up to 64 policies, out of which you can configure up to 16 policies per WLAN.
- Policy action is taken after Layer 2 authentication is complete, or after Layer 3 authentication is complete, or when the device sends HTTP traffic and gets the device profiled. Therefore, profiling and policy actions occur more than once per client.
- Only VLAN, ACL, Session Timeout, and QoS are supported as policy action attributes.
- If you want a local policy session timeout to be applied and overridden for a WLAN, you must enable the session timeout at the WLAN with a value greater than 0.
- Profiling is performed only on IPv4 clients.
- For all the controllers in a mobility group, it is mandatory that the local policy configurations have the same match criteria attributes and action attributes. Otherwise, the local policy configuration becomes invalid when roaming occurs across the controllers.
- Local policies are enforced after profiling using OUI irrespective of DHCP or HTTP profiling. For more information, see CSCvp70783.

Table 18: Differences Between Cisco Identity Services Engine (ISE) and Controller Profiling Support

ISE	Controller
Supports profiling using RADIUS probes, DHCP probes, HTTP, and other protocols used to identify the client type.	Supports MAC OUI, DHCP, and HTTP-based profiling.
Supports multiple different attributes for the policy action and has an interface to pick and select each of the attributes.	Supports VLAN, ACL, Session Timeout, and QoS as policy action attributes.
Supports customization of profiling rules with user-defined attributes.	Supports only default profiling rules.

Configuring Local Policies (GUI)

Step 1 Choose **Security** > **Local Policies**.

Step 2 Click **New** to create a new policy.

Step 3 Enter the policy name and click **Apply**.

Step 4 On the **Policy List** page, click the policy name to be configured.

Step 5 On the **Policy > Edit** page, follow these steps:

a) In the **Match Criteria** area, enter a value for **Match Role String**. This is the user type or user group of the user, for example, student, teacher, and so on.

b) From the **Match EAP Type** drop-down list, choose the EAP authentication method used by the client.

c) From the **Device Type** drop-down list, choose the device type.

d) Click **Add** to add the device type to the policy device list.

The device type you choose is listed in the **Device List**.

e) In the **Action** area, specify the policies that are to be enforced. From the **IPv4 ACL** drop-down list, choose an IPv4 ACL for the policy.

f) Enter the **VLAN ID** that should be associated with the policy.

g) From the **QoS Policy** drop-down list, choose a QoS policy to be applied.

h) Enter a value for **Session Timeout**. This is the maximum amount of time, in seconds, after which a client is forced to reauthenticate.

i) Enter a value for **Sleeping Client Timeout**, which is the timeout for sleeping clients.

Sleeping clients are clients with guest access that have had successful web authentication that are allowed to sleep and wake up without having to go through another authentication process through the login page.

This sleeping client timeout configuration overrides the WLAN-specific sleeping client timeout configuration.

j) In the **Active Hours** area, from the **Day** drop-down list, choose the days on which the policy has to be active.

k) Enter the **Start Time** and **End Time** of the policy.

l) Click **Add**.

The day and start time and end time that you specify is listed.

m) Click **Apply**.

What to do next

Apply a local policy that you have created to a WLAN by following these steps:

1. Choose **WLANs**.
2. Click the corresponding WLAN ID.

   The **WLANs > Edit** page is displayed.
3. Click the **Policy-Mapping** tab.
4. Enter the **Priority Index** for a policy.

5. From the **Local Policy** drop-down list, choose the policy that has to be applied for the WLAN.
6. Click **Add**.

   The priority index and the policy that you choose is listed. You can apply up to 16 policies for a WLAN.

Configuring Local Policies (CLI)

Procedure

- Create or delete a local policy by entering this command:

  config policy *policy-name* {**create** | **delete**}

- Configure a match type to a policy by entering these commands:
  - **config policy** *policy-name* **match device-type** {**add** | **delete**} *device-type*
  - **config policy** *policy-name* **match eap-type** {**add** | **delete**} {**eap-fast** | **eap-tls** | **leap** | **peap**}
  - **config policy** *policy-name* **match role** {*role-name* | *none*}
- Configure an action that has to be enforced as part of a policy by entering these commands:
  - ACL action to a policy—**config policy** *policy-name* **action acl** {**enable** | **disable**} *acl-name*
  - QoS average data rate—**config policy** *policy-name* **action average-data-rate** {**enable** | **disable**} *rate*
  - QoS average real-time data rate—**config policy** *policy-name* **action average-realtime-rate** {**enable** | **disable**} *rate*
  - QoS burst data rate—**config policy** *policy-name* **action burst-data-rate** {**enable** | **disable**} *rate*
  - QoS burst real-time data rate—**config policy** *policy-name* **action burst-realtime-rate** {**enable** | **disable**} *rate*
  - QoS action—**config policy** *policy-name* **action qos** {**enable** | **disable**} {**bronze** | **gold** | **platinum** | **silver**}
  - Session timeout action—**config policy** *policy-name* **action session-timeout** {**enable** | **disable**} *timeout-in-seconds*
  - Sleeping client timeout action—**config policy** *policy-name* **action sleeping-client-timeout** {**enable** | **disable**} *timeout-in-hours*
  - VLAN action—**config policy** *policy-name* **action vlan** {**enable** | **disable**} *vlan-id*

Note Ensure that you configure the Average Data Rate before you configure the Burst Data Rate.

- Configure the active time for a policy by entering this command:

  config policy *policy-name* **active** {**add** | **delete**} **hours start-time end-time days** {*mon* | *tue* | *wed* | *thu* | *fri* | *sat* | *sun* | *daily* | *weekdays*}

- Apply a local policy to a WLAN by entering this command:

  config wlan policy {**add** | **delete**} *priority-index policy-name wlan-id*

- Enable or disable client profiling in local mode for a WLAN, based on HTTP, DHCP, or both by entering this command:

  config wlan profiling local {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

- Apply a local policy to an AP group of a WLAN by entering this command:

  config wlan apgroup policy {**add** | **delete**} *priority-index policy-name ap-group-name wlan-id*

- View information about a policy by entering this command:

  show policy {**summary** | *policy-name*} **statistics**

- View local device classification profile summary by entering this command:

  show profiling policy summary

- View all the clients with a type of device by entering this command:

  show client wlan *wlan-id* **device-type** *device-type*

- View a client profiling status that includes profiling done by the RADIUS server and the controller by entering this command:

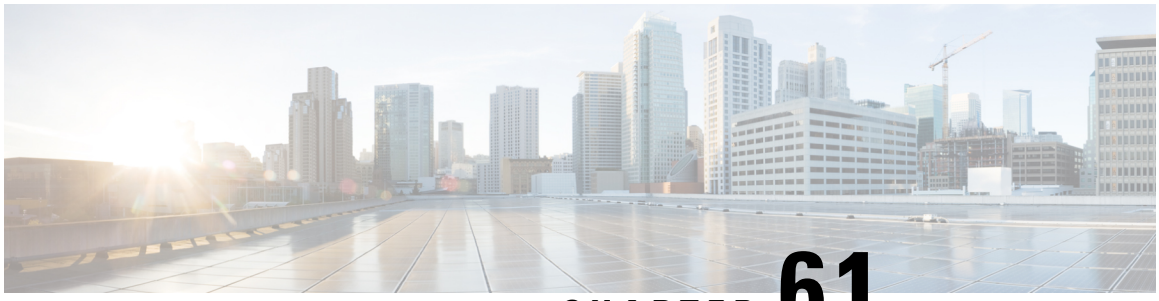
  show wlan *wlan-id*

- View the policy details for AP groups by entering this command:

  show wlan apgroups

- Configure the task of debugging of policies by entering this command:

  debug policy {**error** | **event**} {**enable** | **disable**}



CHAPTER 61

Configuring Cisco Intrusion Detection System

- Cisco Intrusion Detection System, on page 509
- Configuring IDS Sensors (GUI), on page 510
- Viewing Shunned Clients (GUI), on page 510
- Configuring IDS Sensors (CLI), on page 511
- Viewing Shunned Clients (CLI), on page 512

Cisco Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected at Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse. Two methods are available to detect potential attacks:

- IDS sensors
- IDS signatures

You can configure IDS sensors to detect various types of IP-level attacks in your network. When the sensors identify an attack, they can alert the controller to shun the offending client. When you add a new IDS sensor, you register the controller with that IDS sensor so that the controller can query the sensor to get the list of shunned clients.

This section contains the following subsections:

Shunned Clients

When an IDS sensor detects a suspicious client, it alerts the controller to shun this client. The shun entry is distributed to all controllers within the same mobility group. If the client to be shunned is currently joined to a controller in this mobility group, the anchor controller adds this client to the dynamic exclusion list, and the foreign controller removes the client. The next time that the client tries to connect to a controller, the anchor controller rejects the handoff and informs the foreign controller that the client is being excluded.

Configuring IDS Sensors (GUI)

Step 1 Choose **Security** > **Advanced** > **CIDS** > **Sensors** to open the CIDS Sensors List page.

Note If you want to delete an existing sensor, hover your cursor over the blue drop-down arrow for that sensor and choose **Remove**.

Step 2 Click **New** to add a new IDS sensor to the list. The **CIDS Sensor Add** page is displayed.

Step 3 From the **Index** drop-down list, choose a number (between 1 and 5) to determine the sequence in which the controller consults the IDS sensors. For example, if you choose 1, the controller consults this IDS sensor first.

Cisco WLC supports up to five IDS sensors.

Step 4 In the **Server Address** text box, enter the IP address of your IDS server.

Step 5 In the **Port** text box, enter the number of the HTTPS port through which the controller has to communicate with the IDS sensor.

We recommend that you set this parameter to 443 because the sensor uses this value to communicate by default. The default value is 443 and the range is 1 to 65535.

Step 6 In the **Username** text box, enter the name that the controller uses to authenticate to the IDS sensor.

Note This username must be configured on the IDS sensor and have at least a read-only privilege.

Step 7 In the **Password** and **Confirm Password** text boxes, enter the password that the controller uses to authenticate to the IDS sensor.

Step 8 In the **Query Interval** text box, enter the time (in seconds) for how often the controller should query the IDS server for IDS events.

The default is 60 seconds and the range is 10 to 3600 seconds.

Step 9 Check the **State** check box to register the controller with this IDS sensor or uncheck this check box to disable registration. The default value is disabled.

Step 10 Enter a 40-hexadecimal-character security key in the **Fingerprint** text box. This key is used to verify the validity of the sensor and is used to prevent security attacks.

Note Make sure you include colons that appear between every two bytes within the key. For example, enter AA:BB:CC:DD.

Step 11 Click **Apply**. Your new IDS sensor appears in the list of sensors on the CIDS Sensors List page.

Step 12 Click **Save Configuration**.

Viewing Shunned Clients (GUI)

Step 1 Choose **Security** > **Advanced > CIDS** > **Shunned Clients** to open the CIDS Shun List page.

This page shows the IP address and MAC address of each shunned client, the length of time that the client's data packets should be blocked by the controller as requested by the IDS sensor, and the IP address of the IDS sensor that discovered the client.

Step 2 Click **Re-sync** to purge and reset the list as desired.

Note The controller does not take any action on shun entries when the corresponding timers have expired. The shun entry timers are maintained only for the display purpose. The shun entries are cleaned up whenever the controller polls the IPS server. If the CIDS IPS server is not reachable, the shun entries are not removed even if they are timed out on the controller. The shun entries are cleaned up only when the CIDS IPS server is operational again and the controller polls the CIDS IPS server.

Configuring IDS Sensors (CLI)

Step 1 Add an IDS sensor by entering this command:

config wps cids-sensor add index ids_ip_address username password.

The index parameter determines the sequence in which the controller consults the IDS sensors. The controller supports up to five IDS sensors. Enter a number (between 1 and 5) to determine the priority of this sensor. For example, if you enter 1, the controller consults this IDS sensor first.

Note The username must be configured on the IDS sensor and have at least a read-only privilege.

Step 2 (Optional) Specify the number of the HTTPS port through which the controller is to communicate with the IDS sensor by entering this command:

config wps cids-sensor port index port

For the port-number parameter, you can enter a value between 1 and 65535. The default value is 443. This step is optional because we recommend that you use the default value of 443. The sensor uses this value to communicate by default.

Step 3 Specify how often the controller should query the IDS server for IDS events by entering this command:

config wps cids-sensor interval index interval

For the interval parameter, you can enter a value between 10 and 3600 seconds. The default value is 60 seconds.

Step 4 Enter a 40-hexadecimal-character security key used to verify the validity of the sensor by entering this command:

config wps cids-sensor fingerprint index sha1 fingerprint

You can get the value of the fingerprint by entering show tls fingerprint on the sensor's console.

Note Make sure to include the colons that appear between every two bytes within the key (for example, AA:BB:CC:DD).

Step 5 Enable or disable this controller's registration with an IDS sensor by entering this command:

config wps cids-sensor {**enable** | **disable**} *index*

Step 6 Enable or disable protection from DoS attacks by entering this command:

The default value is disabled.

Note A potential attacker can use specially crafted packets to mislead the IDS into treating a legitimate client as an attacker. It causes the controller to wrongly disconnect this legitimate client and launches a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

Step 7 Save your settings by entering this command:

save config

Step 8 See the IDS sensor configuration by entering one of these commands:

- **show wps cids-sensor summary**
- **show wps cids-sensor detail** index

Step 9 The second command provides more information than the first.

Step 10 See the auto-immune configuration setting by entering this command:

show wps summary

Information similar to the following appears:

```
Auto-Immune
  Auto-Immune..................................... Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
Signature Policy
  Signature Processing........................... Enabled
```

Step 11 Obtain debug information regarding IDS sensor configuration by entering this command:

debug wps cids enable

Note If you ever want to delete or change the configuration of a sensor, you must first disable it by entering the config wps cids-sensor disable index command. To delete the sensor, enter the config wps cids-sensor delete index command.

Viewing Shunned Clients (CLI)

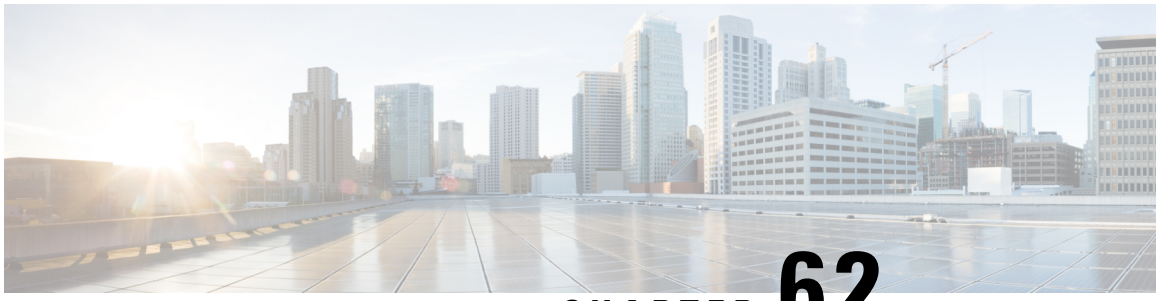
Step 1 View the list of clients to be shunned by entering this command:

show wps shun-list

Step 2 Force the controller to synchronize with other controllers in the mobility group for the shun list by entering this command:

config wps shun-list re-sync

Note The controller does not take any action on shun entries when the corresponding timers have expired. The shun entry timers are maintained only for the display purpose. The shun entries are cleaned up whenever the controller polls the IPS server. If the CIDS IPS server is not reachable, the shun entries are not removed even if they are timed out on the controller. The shun entries are cleaned up only when the CIDS IPS server is operational again and the controller polls the CIDS IPS server.



CHAPTER 62

Configuring IDS Signatures

- Intrusion Detection System Signatures, on page 515
- Configuring IDS Signatures (GUI), on page 517
- Viewing IDS Signature Events (GUI), on page 520
- Configuring IDS Signatures (CLI), on page 520
- Viewing IDS Signature Events (CLI), on page 522

Intrusion Detection System Signatures

You can configure intrusion detection system (IDS) signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, appropriate mitigation is initiated.

Cisco supports 17 standard signatures. These signatures are divided into six main groups. The first four groups contain management signatures, and the last two groups contain data signatures.

- **Broadcast deauthentication frame signatures**—During a broadcast deauthentication frame attack, a hacker sends an 802.11 deauthentication frame to the broadcast MAC destination address of another client. This attack causes the destination client to disassociate from the access point and lose its connection. If this action is repeated, the client experiences a denial of service. When the broadcast deauthentication frame signature (precedence 1) is used to detect such an attack, the access point listens for clients transmitting broadcast deauthentication frames that match the characteristics of the signature. If the access point detects such an attack, it alerts the controller. Depending on how your system is configured, the offending device is contained so that its signals no longer interfere with authorized clients, or the controller forwards an immediate alert to the system administrator for further action, or both.
- **NULL probe response signatures**—During a NULL probe response attack, a hacker sends a NULL probe response to a wireless client adapter. As a result, the client adapter locks up. When a NULL probe response signature is used to detect such an attack, the access point identifies the wireless client and alerts the controller. The NULL probe response signatures are as follows:
  - NULL probe resp 1 (precedence 2)
  - NULL probe resp 2 (precedence 3)

Note Controller does not log historical NULL Probe IDS events within the Signature Events Summary output.

- **Management frame flood signatures**—During a management frame flood attack, a hacker floods an access point with 802.11 management frames. The result is a denial of service to all clients associated or attempting to associate to the access point. This attack can be implemented with different types of management frames: association requests, authentication requests, reassociation requests, probe requests, disassociation requests, deauthentication requests, and reserved management subtypes.

  When a management frame flood signature is used to detect such an attack, the access point identifies management frames matching the entire characteristic of the signature. If the frequency of these frames is greater than the value of the frequency set in the signature, an access point that hears these frames triggers an alarm. The controller generates a trap and forwards it to Cisco Prime Infrastructure.

  The management frame flood signatures are as follows:

  - Assoc flood (precedence 4)
  - Auth flood (precedence 5)
  - Reassoc flood (precedence 6)
  - Broadcast probe flood (precedence 7)
  - Disassoc flood (precedence 8)
  - Deauth flood (precedence 9)
  - Reserved mgmt 7 (precedence 10)
  - Reserved mgmt F (precedence 11)

    The reserved management frame signatures 7 and F are reserved for future use.

- **Wellenreiter signature**—Wellenreiter is a wireless LAN scanning and discovery utility that can reveal access point and client information. When the Wellenreiter signature (precedence 17) is used to detect such an attack, the access point identifies the offending device and alerts the controller.
- **EAPOL flood signature—**During an EAPOL flood attack, a hacker floods the air with EAPOL frames that contain 802.1X authentication requests. As a result, the 802.1X authentication server cannot respond to all of the requests and fails to send successful authentication responses to valid clients. The result is a denial of service to all affected clients. When the EAPOL flood signature (precedence 12) is used to detect such an attack, the access point waits until the maximum number of allowed EAPOL packets is exceeded. It then alerts the controller and proceeds with the appropriate mitigation.
- **NetStumbler signatures**—NetStumbler is a wireless LAN scanning utility that reports access point broadcast information (such as operating channel, RSSI information, adapter manufacturer name, SSID, WEP status, and the latitude and longitude of the device running NetStumbler when a GPS is attached). If NetStumbler succeeds in authenticating and associating to an access point, it sends a data frame with the following strings, depending on the NetStumbler version:

Version	String
3.2.0	“Flurble gronk bloopit, bnip Frundletrune”

Version	String
3.2.3	“All your 802.11b are belong to us”
3.3.0	Sends white spaces

When a NetStumbler signature is used to detect such an attack, the access point identifies the offending device and alerts the controller. The NetStumbler signatures are as follows:

- NetStumbler 3.2.0 (precedence 13)
- NetStumbler 3.2.3 (precedence 14)
- NetStumbler 3.3.0 (precedence 15)
- NetStumbler generic (precedence 16)

A standard signature file exists on the controller by default. You can upload this signature file from the controller, or you can create a custom signature file and download it to the controller or modify the standard signature file to create a custom signature.

Configuring IDS Signatures (GUI)

Uploading or Downloading IDS Signatures

Step 1 If desired, create your own custom signature file.

Step 2 Make sure that you have a Trivial File Transfer Protocol (TFTP) server available. Follow these guidelines when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

Step 3 If you are downloading a custom signature file (*.sig), copy it to the default directory on your TFTP server.

Step 4 Choose **Commands** to open the **Download File to Controller** page.

Step 5 Perform one of the following:

- If you want to download a custom signature file to the controller, choose **Signature File** from the File Type drop-down list on the Download File to Controller page.
- If you want to upload a standard signature file from the controller, choose **Upload File** and then **Signature File** from the **File Type** drop-down list on the **Upload File from Controller** page.

Step 6 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

The SFTP option was added in Release 7.4.

Step 7 In the **IP Address** text box, enter the IP address of the **TFTP**, **FTP**, or **SFTP** server.

Step 8 If you are downloading the signature file using a TFTP server, enter the maximum number of times that the controller should attempt to download the signature file in the **Maximum retries** text box.

The range is 1 to 254 and the default value is 10.

Step 9 If you are downloading the signature file using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the signature file in the **Timeout** text box.

The range is 1 to 254 seconds and the default is 6 seconds.

Step 10 In the **File Path** text box, enter the path of the signature file to be downloaded or uploaded. The default value is "/."

Step 11 In the **File Name** text box, enter the name of the signature file to be downloaded or uploaded.

Note When uploading signatures, the controller uses the filename that you specify as a base name and then adds "_std.sig" and "_custom.sig" to it in order to upload both standard and custom signature files to the TFTP server. For example, if you upload a signature file called "ids1," the controller automatically generates and uploads both ids1_std.sig and ids1_custom.sig to the TFTP server. If desired, you can then modify ids1_custom.sig on the TFTP server (making sure to set "Revision = custom") and download it by itself.

Step 12 If you are using an FTP or SFTP server, follow these steps:

a. In the **Server Login Username** text box, enter the username to log into the FTP or SFTP server.

b. In the **Server Login Password** text box, enter the password to log into the FTP or SFTP server.

c. In the **Server Port Number** text box, enter the port number on the FTP or SFTP server through which the download occurs. The default value is 21.

Step 13 Choose **Download** to download the signature file to the controller or **Upload** to upload the signature file from the controller.

Enabling or Disabling IDS Signatures

Step 1 Choose **Security** > **Wireless Protection Policies** > **Standard Signatures** or **Custom Signatures** to open the Standard Signatures page or the Custom Signatures page.

The Standard Signatures page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. This page shows the following information for each signature:

- The order, or precedence, in which the controller performs the signature checks.
- The name of the signature, which specifies the type of attack that the signature is trying to detect.
- The frame type on which the signature is looking for a security attack. The possible frame types are data and management.
- The action that the controller is directed to take when the signature detects an attack. The possible actions are None and Report.

- The state of the signature, which indicates whether the signature is enabled to detect security attacks.
- A description of the type of attack that the signature is trying to detect.

Step 2 Perform one of the following:

- If you want to allow all signatures (both standard and custom) whose individual states are set to Enabled to remain enabled, select the **Enable Check for All Standard and Custom Signatures** check box at the top of either the Standard Signatures page or the Custom Signatures page. The default value is enabled (or selected). When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.
- If you want to disable all signatures (both standard and custom) on the controller, unselect the **Enable Check for All Standard and Custom Signatures** check box. If you unselected this check box, all signatures are disabled, even the ones whose individual states are set to Enabled.

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

Step 4 Click the precedence number of the desired signature to enable or disable an individual signature. The **Standard Signature (or Custom Signature) > Detail** page appears.

This page shows much of the same information as the Standard Signatures and Custom Signatures pages but provides these additional details:

- The tracking method used by the access points to perform signature analysis and report the results to the controller. The possible values are as follows:
  - Per Signature—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis.
  - Per MAC—Signature analysis and pattern matching are tracked and reported separately for individual client MAC addresses on a per-channel basis.
  - Per Signature and MAC—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis as well as on a per-MAC-address and per-channel basis.
- The pattern that is being used to detect a security attack

Step 5 In the Measurement Interval text box, enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value varies per signature.

Step 6 In the Signature Frequency text box, enter the number of matching packets per interval that must be identified at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 7 In the Signature MAC Frequency text box, enter the number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 8 In the Quiet Time text box, enter the length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds, and the default value varies per signature.

Step 9 Select the **State** check box to enable this signature to detect security attacks or unselect it to disable this signature. The default value is enabled (or selected).

Step 10 Click **Apply** to commit your changes. The Standard Signatures or Custom Signatures page reflects the signature's updated state.

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

Viewing IDS Signature Events (GUI)

Step 1 Choose **Security** > **Wireless Protection Policies** > **Signature Events Summary** to open the Signature Events Summary page.

Step 2 Click the Signature Type for the signature to see more information on the attacks detected by a particular signature. The Signature Events Detail page appears.

This page shows the following information:

- The MAC addresses of the clients identified as attackers
- The method used by the access point to track the attacks
- The number of matching packets per second that were identified before an attack was detected.
- The number of access points on the channel on which the attack was detected
- The day and time when the access point detected the attack

Step 3 Click the **Detail link** for that attack to see more information for a particular attack. The Signature Events Track Detail page appears.

- The MAC address of the access point that detected the attack
- The name of the access point that detected the attack
- The type of radio (802.11a or 802.11b/g) used by the access point to detect the attack
- The radio channel on which the attack was detected
- The day and time when the access point reported the attack

Configuring IDS Signatures (CLI)

Step 1 If desired, create your own custom signature file.

Step 2 Make sure that you have a TFTP server available.

Step 3 Copy the custom signature file (*.sig) to the default directory on your TFTP server.

Step 4 Specify the download or upload mode by entering the **transfer** {**download** | **upload**} **mode tftp** command.

Step 5 Specify the type of file to be downloaded or uploaded by entering the **transfer** {**download** | **upload**} **datatype signature** command.

Step 6 Specify the IP address of the TFTP server by entering the **transfer** {**download** | **upload**} **serverip** *tftp-server-ip-address* command.

Note Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

Step 7 Specify the download or upload path by entering the **transfer** {**download** | **upload**} *path absolute-tftp-server-path-to-file* command.

Step 8 Specify the file to be downloaded or uploaded by entering the **transfer** {**download** | **upload**} *filename filename.sig* command.

Note When uploading signatures, the controller uses the filename you specify as a base name and then adds "_std.sig" and "_custom.sig" to it in order to upload both standard and custom signature files to the TFTP server. For example, if you upload a signature file called "ids1," the controller automatically generates and uploads both ids1_std.sig and ids1_custom.sig to the TFTP server. If desired, you can then modify ids1_custom.sig on the TFTP server (making sure to set "Revision = custom") and download it by itself.

Step 9 Enter the **transfer** {**download** | **upload**} *start* command and answer y to the prompt to confirm the current settings and start the download or upload.

Step 10 Specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval by entering this command:

config wps signature interval *signature_id interval*

where signature_id is a number used to uniquely identify a signature. The range is 1 to 3600 seconds, and the default value varies per signature.

Step 11 Specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected by entering this command:

config wps signature frequency*signature_id frequency*

The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 12 Specify the number of matching packets per interval that must be identified per client per access point before an attack is detected by entering this command:

config wps signature mac-frequency *signature_id mac_frequency*

The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 13 Specify the length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop by entering by entering this command:

config wps signature quiet-time *signature_id quiet_time*

The range is 60 to 32,000 seconds, and the default value varies per signature.

Step 14 Perform one of the following:

- To enable or disable an individual IDS signature, enter this command:

  config wps signature {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

- To enable or disable IDS signature processing, which enables or disables the processing of all IDS signatures, enter this command:

  config wps signature {**enable** | **disable**}

Note If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Step 15 Save your changes by entering this command:

save config

Step 16 If desired, you can reset a specific signature or all signatures to default values. To do so, enter this command:

config wps signature reset {*signature_id* | *all*}

Note You can reset signatures to default values only through the controller CLI.

Viewing IDS Signature Events (CLI)

Procedure

- See whether IDS signature processing is enabled or disabled on the controller by entering this command:

  show wps summary

Note If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

- See individual summaries of all of the standard and custom signatures installed on the controller by entering this command:

  show wps signature summary

- See the number of attacks detected by the enabled signatures by entering this command:

  show wps signature events summary

- See more information on the attacks detected by a particular standard or custom signature by entering this command:

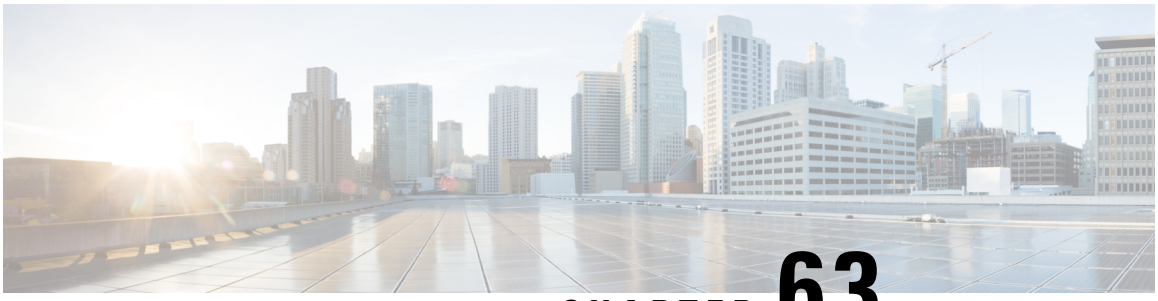
  show wps signature events {**standard** | **custom**} **precedence# summary**

- See information on attacks that are tracked by access points on a per-signature and per-channel basis by entering this command:

  show wps signature events {**standard** | **custom**} **precedence# detailed per-signature** *source_mac*

- See information on attacks that are tracked by access points on an individual-client basis (by MAC address) by entering this command:

  show wps signature events {**standard** | **custom**} **precedence# detailed per-mac** *source_mac*



CHAPTER 63

Configuring wIPS

- Wireless Intrusion Prevention System, on page 523
- Restrictions for wIPS, on page 529
- Configuring wIPS on an Access Point (GUI), on page 530
- Configuring wIPS on an Access Point (CLI), on page 530
- Viewing wIPS Information (CLI), on page 531

Wireless Intrusion Prevention System

The Cisco Adaptive Wireless Intrusion Prevention System (wIPS) uses an advanced approach to wireless threat detection and performance management. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both the wired and wireless networks and use that network intelligence to analyze attacks from many sources to accurately pinpoint and proactively prevent attacks, rather than wait until damage or exposure has occurred.

Cisco Adaptive wIPS is a part of the Cisco 3300 Series Mobility Services Engine (MSE), which centralizes the processing of intelligence collected by the continuous monitoring of Cisco Aironet APs. With Cisco Adaptive wIPS functionalities and Cisco Prime Infrastructure integration into the Cisco MSE, the wIPS can configure and monitor wIPS policies and alarms and report threats.

Note If your wIPS deployment consists of a controller, access point, and Cisco MSE, you must set all the three entities to the UTC time zone.

Cisco Adaptive wIPS is not configured on the controller. Instead, the Cisco Prime Infrastructure forwards the profile configuration to the wIPS service, which forwards the profile to the controller. The profile is stored in flash memory on the controller and sent to APs when they join the controller. When an access point disassociates and joins another controller, it receives the wIPS profile from the new controller.

Local-mode or FlexConnect mode APs with a subset of wIPS capabilities are referred to as Enhanced Local Mode access point or ELM AP. You can configure an access point to work in the wIPS mode if the AP is in any of the following modes:

- Monitor
- Local

- FlexConnect

The regular local mode or FlexConnect mode AP is extended with a subset of wIPS capabilities. This feature enables you to deploy your APs to provide protection without needing a separate overlay network.

wIPS ELM has the limited capability of detecting off-channel alarms. AN AP periodically goes off-channel, and monitors the nonserving channels for a short duration, and triggers alarms if any attack is detected on the channel. But off-channel alarm detection is best effort, and it takes a longer time to detect attacks and trigger alarms, which might cause the ELM AP to intermittently detect an alarm and clear it because it is not visible. APs in any of the above modes can periodically send alarms based on the policy profile to the wIPS service through the controller. The wIPS service stores and processes the alarms and generates SNMP traps. Cisco Prime Infrastructure configures its IP address as a trap destination to receive SNMP traps from the Cisco MSE.

This table lists all the SNMP trap controls and their respective traps. When a trap control is enabled, all the traps of that trap control are also enabled.

Note The controller uses only SNMPv2 for SNMP trap transmission.

Table 19: SNMP Trap Controls and Their Respective Traps

Tab Name	Trap Control	Trap
General	Link (Port) Up/Down	linkUp, linkDown
	Spanning Tree	newRoot, topologyChange, stpInstanceNewRootTrap, stpInstanceTopologyChangeTrap
	Config Save	bsnDot11EssCreated, bsnDot11EssDeleted, bsnConfigSaved, ciscoLwappScheduledResetNotif, ciscoLwappClearResetNotif, ciscoLwappResetFailedNotif, ciscoLwappSysInvalidXmlConfig
AP	AP Register	bsnAPDisassociated, bsnAPAssociated
	AP Interface Up/Down	bsnAPIfUp, bsnAPIfDown

Tab Name	Trap Control	Trap
Client Traps	802.11 Association	bsnDot11StationAssociate
	802.11 Disassociation	bsnDot11StationDisassociate
	802.11 Deauthentication	bsnDot11StationDeauthenticate
	802.11 Failed Authentication	bsnDot11StationAuthenticateFail
	802.11 Failed Association	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted
	NAC Alert	cldcClientWlanProfileName, cldcClientIPAddress, cldcApMacAddress, cldcClientQuarantineVLAN, cldcClientAccessVLAN
Security Traps	User Authentication	bsnTooManyUnsuccessLoginAttempts, cLWAGuestUserLoggedIn, cLWAGuestUserLoggedOut
	RADIUS Servers Not Responding	bsnRADIUSServerNotResponding, ciscoLwappAAARadiusReqTimedOut
	WEP Decrypt Error	bsnWepKeyDecryptError
	Rogue AP	bsnAdhocRogueAutoContained, bsnRogueApAutoContained, bsnTrustedApHasInvalidEncryption, bsnMaxRogueCountExceeded, bsnMaxRogueCountClear, bsnApMaxRogueCountExceeded, bsnApMaxRogueCountClear, bsnTrustedApHasInvalidRadioPolicy, bsnTrustedApHasInvalidSsid, bsnTrustedApIsMissing
	SNMP Authentication	agentSnmpAuthenticationTrapFlag
	Multiple Users	multipleUsersTrap
Auto RF Profile Traps	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
Auto RF Update Traps	Channel Update	bsnAPCurrentChannelChanged
	Tx Power Update	bsnAPCurrentTxPowerChanged

Tab Name	Trap Control	Trap
Mesh Traps	Child Excluded Parent	ciscoLwappMeshChildExcludedParent
	Parent Change	ciscoLwappMeshParentChange
	Authfailure Mesh	ciscoLwappMeshAuthorizationFailure
	Child Moved	ciscoLwappMeshChildMoved
	Excessive Parent Change	ciscoLwappMeshExcessiveParentChange
	Excessive Children	ciscoLwappMeshExcessiveChildren
	Poor SNR	ciscoLwappMeshAbateSNR, ciscoLwappMeshOnsetSNR
	Console Login	ciscoLwappMeshConsoleLogin
	Excessive Association	ciscoLwappMeshExcessiveAssociation
	Default Bridge Group Name	ciscoLwappMeshDefaultBridgeGroupName

The following are the trap descriptions for the traps mentioned in the *SNMP Trap Controls and Their Respective Traps* table:

- General Traps
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

    Note When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Link (Port) Up/Down—Link changes status from up or down.
  - Link (Port) Up/Down—Link changes status from up or down.
  - Multiple Users—Two users log in with the same ID.
  - Rogue AP—Whenever a rogue access point is detected, this trap is sent with its MAC address; when a rogue access point that was detected earlier no longer exists, this trap is sent.
  - Config Save—Notification that is sent when the controller configuration is modified.
- Cisco AP Traps
  - AP Register—Notification sent when an access point associates or disassociates with the controller.
  - AP Interface Up/Down—Notification sent when an access point interface (802.11X) status goes up or down.
- Client-Related Traps

- 802.11 Association—Associate notification that is sent when a client sends an association frame.
- 802.11 Disassociation—Disassociate notification that is sent when a client sends a disassociation frame.
- 802.11 Deauthentication—Deauthenticate notification that is sent when a client sends a deauthentication frame.
- 802.11 Failed Authentication—Authenticate failure notification that is sent when a client sends an authentication frame with a status code other than successful.
- 802.11 Failed Association—Associate failure notification that is sent when the client sends an association frame with a status code other than successful.
- Exclusion—Associate failure notification that is sent when a client is exclusion listed (in a blocked list).

Note The maximum number of static blocked list entries that the APs can have is 340.

- Authentication—Authentication notification that is sent when a client is successfully authenticated.
- Max Clients Limit Reached—Notification that is sent when the maximum number of clients, defined in the Threshold field, are associated with the controller.
- NAC Alert—Alert that is sent when a client joins an SNMP NAC-enabled WLAN.

  This notification is generated when a client on NAC-enabled SSIDs completes Layer2 authentication to inform the NAC appliance about the client's presence. cldcClientWlanProfileName represents the profile name of the WLAN that the 802.11 wireless client is connected to, cldcClientIPAddress represents the unique IP address of the client. cldcApMacAddress represents the MAC address of the AP to which the client is associated. cldcClientQuarantineVLAN represents the quarantine VLAN for the client. cldcClientAccessVLAN represents the access VLAN for the client.
- Association with Stats—Associate notification that is sent with data statistics when a client is associated with the controller, or roams. Data statistics include transmitted and received bytes and packets.
- Disassociation with Stats—Disassociate notification that is sent with data statistics when a client disassociates from the controller. Data statistics include transmitted and received bytes and packets, SSID, and session ID.

Note When you downgrade to Release 7.4 from a later release, if a trap that was not supported in Release 7.4 (for example, NAC Alert trap) is enabled before the downgrade, all traps are disabled. After the downgrade, you must enable all the traps that were enabled before the downgrade. We recommend that you disable the new traps before the downgrade so that all the other traps are not disabled.

- Security Traps
  - User Auth Failure—This trap informs that a client RADIUS Authentication failure has occurred.

- RADIUS Server No Response—This trap is to indicate that no RADIUS servers are responding to authentication requests sent by the RADIUS client.
- WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
- Rouge AP—Whenever a rogue access point is detected, this trap is sent with its MAC address; when a rogue access point that was detected earlier no longer exists, this trap is sent.
- SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

Note When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

- Multiple Users—Two users log in with the same ID.

- SNMP Authentication
  - Load Profile—Notification sent when the Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when the Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when the Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when the Coverage Profile state changes between PASS and FAIL.

- Auto RF Profile Traps
  - Load Profile—Notification sent when the Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when the Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when the Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when the Coverage Profile state changes between PASS and FAIL.

- Auto RF Update Traps
  - Channel Update—Notification sent when the access point dynamic channel algorithm is updated.
  - Tx Power Update—Notification sent when the access point dynamic transmit power algorithm is updated.

- Mesh Traps
  - Child Excluded Parent—Notification that is sent when a defined number of failed association to the controller occurs through a parent mesh node.
  - Notification sent when a child mesh node exceeds the threshold limit of the number of discovery response timeouts. The child mesh node does not try to associate an excluded parent mesh node for

the interval defined. The child mesh node remembers the excluded parent MAC address when it joins the network, and informs the controller.

- Parent Change—Notification is sent by the agent when a child mesh node changes its parent. The child mesh node remembers previous parent and informs the controller about the change of parent when it rejoins the network.
- Child Moved—Notification sent when a parent mesh node loses connection with its child mesh node.
- Excessive Parent Change—Notification sent when the child mesh node changes its parent frequently. Each mesh node keeps a count of the number of parent changes in a fixed time. If it exceeds the defined threshold, the child mesh node informs the controller.
- Excessive Children—Notification sent when the child count exceeds for a RAP and a MAP.
- Poor SNR—Notification sent when the child mesh node detects a lower SNR on a backhaul link. For the other trap, a notification is sent to clear a notification when the child mesh node detects an SNR on a backhaul link that is higher then the object defined by 'clMeshSNRThresholdAbate'.
- Console Login—Notification is sent by the agent when a login on a MAP console is either successful or fail after three attempts.
- Default Bridge Group Name—Notification sent when the MAP mesh node joins its parent using the default bridge group name.

Note The remaining traps do not have trap controls. These traps are not generated too frequently and do not require any trap control. Any other trap that is generated by the controller cannot be turned off.

Note In all of the above cases, the controller functions solely as a forwarding device.

Restrictions for wIPS

- wIPS ELM is not supported on the following APs:
  - 702i
  - 702W
  - 1130
  - 1240
- WIPS and Rogue Detection must be disabled on the AP in IPv6 mode to prevent it from leaking traffic outside CAPWAP towards 32.x.x.x destination.

Configuring wIPS on an Access Point (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** > **ap-name**.

Step 2 Set the **AP Mode** parameter. To configure an access point for wIPS, you must choose one of the following modes from the **AP Mode** drop-down list:

- **Local**
- **FlexConnect**
- **Monitor**

Step 3 Choose **wIPS** from the **AP Sub Mode** drop-down list.

Step 4 Save the configuration.

Configuring wIPS on an Access Point (CLI)

Step 1 Configure an access point for the monitor mode by entering this command:

config ap mode {monitor | local | flexconnect} *Cisco_AP*

Note To configure an access point for wIPS, the access point must be in **monitor**, **local**, or **flexconnect** modes.

Step 2 Enter **Y** when you see the message that the access point will be rebooted if you want to continue.

Step 3 Save your changes by entering this command:

save config

Step 4 Disable the access point radio by entering this command:

config {802.11a | 802.11b} disable *Cisco_AP*

Step 5 Configure the wIPS submode on the access point by entering this command:

config ap mode *ap_mode* **submode wips** *Cisco_AP*

Note To disable wIPS on the access point, enter the **config ap mode** *ap_mode* **submode none** *Cisco_AP* command.

Step 6 Enable wIPS-optimized channel scanning for the access point by entering this command:

config ap monitor-mode wips-optimized *Cisco_AP*

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 one of these options:

- **All**—All channels are 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

The 802.11a or 802.11b Monitor Channels information in the output of the **show advanced {802.11a | 802.11b} monitor** command shows the monitor configuration channel set:

```
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
```

Step 7 Reenable the access point radio by entering this command:

config { **802.11a** | **802.11b**} **enable** *Cisco_AP*

Step 8 Save your changes by entering this command:

save config

Viewing wIPS Information (CLI)

Note You can also view the access point submode from the controller GUI. To do so, choose **Wireless** > **Access Points** > **All APs** > *access point name* > the **Advanced** tab. The **AP Sub Mode** field shows *wIPS* if the access point is in the monitor mode and the wIPS submode is configured on the access point, or *None* if the access point is not in the monitor mode or the access point is in the monitor mode, but the wIPS submode is not configured.

Procedure

- See the wIPS submode in the access point by entering this command:

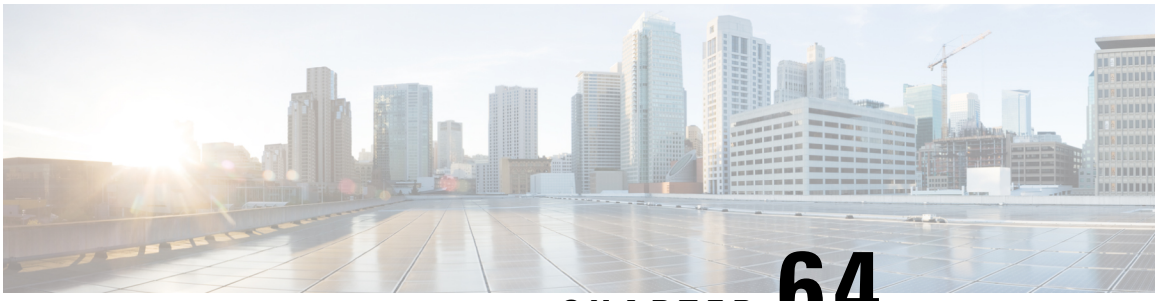
  show ap config general *Cisco_AP*
- See the wIPS-optimized channel-scanning configuration in the access point by entering this command:

  show ap monitor-mode summary
- See the wIPS configuration forwarded by Cisco Prime Infrastructure to the controller by entering this command:

  show wps wips summary
- See the current state of the wIPS operation in the controller by entering this command:

  show wps wips statistics
- Clear the wIPS statistics in the controller by entering this command:

  clear stats wps wips



CHAPTER 64

Configuring the Wi-Fi Direct Client Policy

- Wi-Fi Direct Client Policy, on page 533
- Restrictions for the Wi-Fi Direct Client Policy, on page 533
- Configuring the Wi-Fi Direct Client Policy (GUI), on page 534
- Configuring the Wi-Fi Direct Client Policy (CLI), on page 534
- Monitoring and Troubleshooting the Wi-Fi Direct Client Policy (CLI), on page 535

Wi-Fi Direct Client Policy

Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs.

This section contains the following subsections:

Restrictions for the Wi-Fi Direct Client Policy

- Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.
- Cisco APs in FlexConnect mode (even in central authentication and central switching) is not supported.
- We do not recommend enabling this feature in a mixed AP mode deployment (some APs in FlexConnect mode and some APs in local mode). Such types of deployment is not supported or tested in FlexConnect mode.
- If WLAN applied client policy is invalid, the client is excluded with the exclusion reason being 'Client QoS Policy failure'.

Configuring the Wi-Fi Direct Client Policy (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID of the WLAN for which you want to configure the Wi-Fi Direct Client Policy. The **WLANs > Edit** page appears.

Step 3 Click the **Advanced** tab.

Step 4 From the **Wi-Fi Direct Clients Policy** drop-down list, choose one of the following options:

- **Disabled**—Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
- **Allow**—Allows Wi-Fi Direct clients to associate with the WLAN
- **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN
- **Xconnect-Not-Allow**—Enables AP to allow a client with the Wi-Fi Direct option enabled to associate, but the client (if it works according to the Wi-Fi standards) will refrain from setting up a peer-to-peer connection

Step 5 Save the configuration.

Configuring the Wi-Fi Direct Client Policy (CLI)

Step 1 Configure the Wi-Fi Direct Client Policy on WLANs by entering this command:

config wlan wifidirect {**allow** | **disable** | **not-allow**} *wlan-id*

The syntax of the command is as follows:

- **allow**—Allows Wi-Fi Direct clients to associate with the WLAN
- **disable**—Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
- **not-allow**—Disallows the Wi-Fi Direct clients from associating with the WLAN
- **xconnect-not-allow**—Enables AP to allow a client with the Wi-Fi Direct option enabled to associate, but the client (if it works according to the Wi-Fi standards) will refrain from setting up a peer-to-peer connection
- *wlan-id*—WLAN identifier

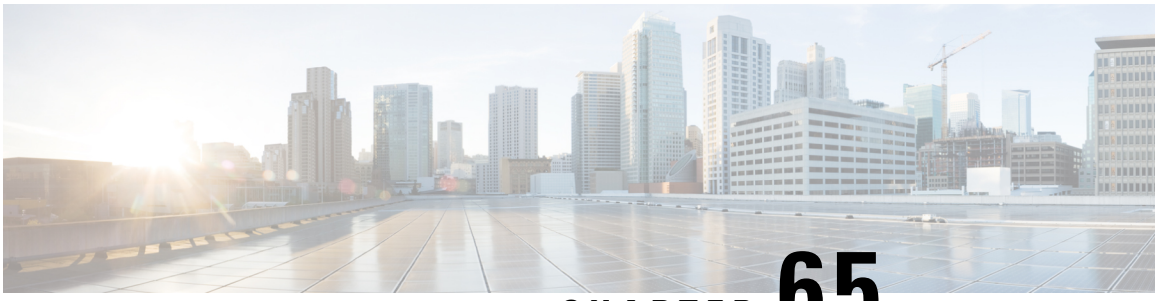
Step 2 Save your configuration by entering this command:

save config

Monitoring and Troubleshooting the Wi-Fi Direct Client Policy (CLI)

Procedure

- Monitor and troubleshoot the Wi-Fi Direct Client Policy by entering theses commands:
  - **show wlan wifidirect** *wlan-id*—Displays status of the Wi-Fi Direct Client Policy on the WLAN.
  - **show client wifiDirect-stats**—Displays the total number of clients associated and the number of clients rejected if the Wi-Fi Direct Client Policy is enabled.



CHAPTER 65

Configuring Web Auth Proxy

- Web Authentication Proxy, on page 537
- Configuring the Web Authentication Proxy (GUI), on page 538
- Configuring the Web Authentication Proxy (CLI), on page 538

Web Authentication Proxy

This feature enables clients that have manual web proxy enabled in the browser to facilitate authentication with the controller. If the user's browser is configured with manual proxy settings with a configured port number as 8080 or 3128 and if the client requests any URL, the controller responds with a web page prompting the user to change the Internet proxy settings to automatically detect the proxy settings so that the browser's manual proxy settings information does not get lost. After enabling this settings, the user can get access to the network through the web authentication policy. This functionality is given for port 8080 and 3128 because these are the most commonly used ports for the web proxy server.

Note The web authentication proxy redirect ports are not blocked through CPU ACL. If a CPU ACL is configured to block the port 8080, 3128, and one random port as part of web authentication proxy configuration, those ports are not blocked because the webauth rules take higher precedence than the CPU ACL rules unless the client is in the webauth_req state.

A web browser has the following three types of Internet settings that you can configure:

- Auto detect
- System Proxy
- Manual

In a manual proxy server configuration, the browser uses the IP address of a proxy server and a port. If this configuration is enabled on the browser, the wireless client communicates with the IP address of the destination proxy server on the configured port. In a web authentication scenario, the controller does not listen to such proxy ports and the client is not able to establish a TCP connection with the controller. The user is unable to get any login page to authentication and get access to the network.

When a wireless client enters a web-authenticated WLAN, the client tries to access a URL. If a manual proxy configuration is configured on the client's browser, all the web traffic going out from the client will be destined to the proxy IP and port configured on the browser.

- A TCP connection is established between the client and the proxy server IP address that the controller proxies for.
- The client processes the DHCP response and obtains a JavaScript file from the controller. The script disables all proxy configurations on the client for that session.

Note For external clients, the controller sends the login page as is (with or without JavaScipt).

- Any requests that bypass the proxy configuration. The controller can then perform web-redirection, login, and authentication.
- When the client goes out of the network, and then back into its own network, a DHCP refresh occurs and the client continues to use the old proxy configuration configured on the browser.
- If the external DHCP server is used with webauth proxy, then DHCP option 252 must be configured on the DHCP server for that scope. The value of option 252 will have the format http://<virtual ip>/proxy.js. No extra configuration is needed for internal DHCP servers.

Note When you configure FIPS mode with secure web authentication, we recommend that you use Mozilla Firefox as your browser.

This section contains the following subsections:

Configuring the Web Authentication Proxy (GUI)

Step 1 Choose **Controller > General**

Step 2 From the **WebAuth Proxy Redirection Mode** drop-down list, choose **Enabled** or **Disabled**.

Step 3 In the **WebAuth Proxy Redirection Port** text box, enter the port number of the web auth proxy.

This text box consists of the port numbers on which the controller listens to for web authentication proxy redirection. By default, the three ports 80, 8080, and 3128 are assumed. If you configured the web authentication redirection port to any port other than these values, you must specify that value.

Step 4 Click **Apply**.

Configuring the Web Authentication Proxy (CLI)

Procedure

- Enable web authentication proxy redirection by entering this command:

  config network web-auth proxy-redirect {**enable** | **disable**}

- Configure the secure web (HTTPS) authentication for clients by entering this command:

  config network web-auth secureweb {**enable** | **disable**}

  The default secure web (HTTPS) authentication for clients is enabled.

Note If you configure to disallow secure web (HTTPS) authentication for clients using the **config network web-auth secureweb disable** command, then you must reboot the Cisco WLC to implement the change.

- Set the web authentication port number by entering this command:

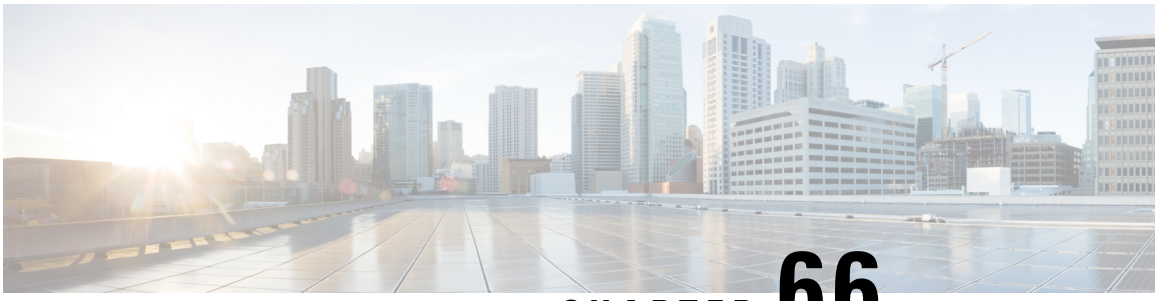
  config network web-auth port *port-number*

  This parameter specifies the port numbers on which the controller listens to for web authentication proxy redirection. By default, the three ports 80, 8080, and 3128 are assumed. If you configured the web authentication redirection port to any port other than these values, you must specify that value.

- Configure secure redirection (HTTPS) for web authentication clients by entering this command:

  config network web-auth https-redirect {**enable** | **disable**}

- See the current status of the web authentication proxy configuration by entering one of the following commands:
  - **show network summary**
  - **show running-config**



CHAPTER 66

Detecting Active Exploits

- Detecting Active Exploits, on page 541

Detecting Active Exploits

The controller supports three active exploit alarms that serve as notifications of potential threats. They are enabled by default and therefore require no configuration on the controller.

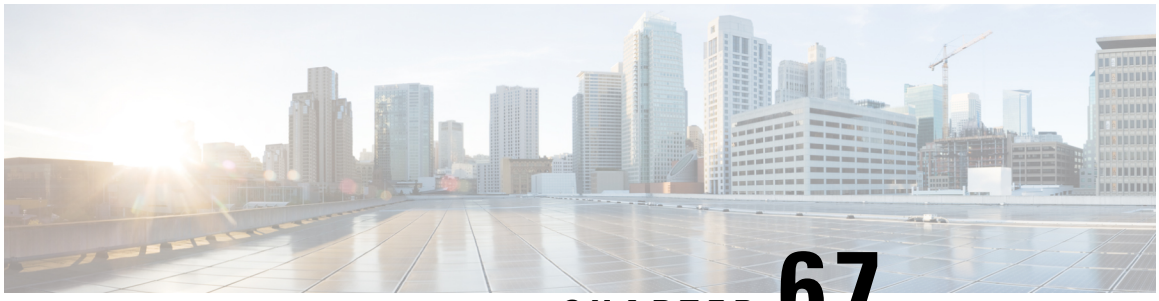
- **ASLEAP detection**—The controller raises a trap event if an attacker launches a LEAP crack tool. The trap message is visible in the controller's trap log.
- **Fake access point detection**—The controller tweaks the fake access point detection logic to avoid false access point alarms in high-density access point environments.
- **Honeypot access point detection**—The controller raises a trap event if a rogue access point is using managed SSIDs (WLANs configured on the controller). The trap message is visible in the controller's trap log.

PART V

WLANs

- Configuring WLANs, on page 545
- Setting the Client Count per WLAN, on page 553
- Configuring DHCP, on page 557
- Configuring DHCP Scopes, on page 563
- Configuring MAC Filtering for WLANs, on page 567
- Configuring Local MAC Filters, on page 569
- Configuring Timeouts, on page 571
- Configuring the DTIM Period, on page 575
- Configuring Peer-to-Peer Blocking, on page 577
- Configuring Layer2 Security, on page 581
- Configuring a WLAN for Static WEP, on page 593
- Configuring Sticky Key Caching, on page 599
- Configuring CKIP, on page 603
- Configuring Layer 3 Security, on page 607
- Configuring Captive Bypassing, on page 611
- Configuring a Fallback Policy with MAC Filtering and Web Authentication, on page 613
- Assigning a QoS Profile to a WLAN, on page 617
- Configuring QoS Enhanced BSS, on page 621
- Configuring Media Session Snooping and Reporting, on page 625
- Configuring Key Telephone System-Based CAC, on page 631
- Configuring Reanchoring of Roaming Voice Clients, on page 635
- Configuring Seamless IPv6 Mobility, on page 637
- Configuring Cisco Client Extensions, on page 643
- Configuring Remote LANs, on page 647

- AP Groups, on page 651
- Configuring RF Profiles, on page 659
- Configuring Web Redirect with 8021.X Authentication, on page 667
- Configuring NAC Out-of-Band Integration, on page 673
- Configuring Passive Clients, on page 679
- Configuring Client Profiling, on page 683
- Configuring Per-WLAN RADIUS Source Support, on page 687
- Configuring Mobile Concierge, on page 691
- Configuring Assisted Roaming, on page 703



CHAPTER 67

Configuring WLANs

- Prerequisites for WLANs, on page 545
- Restrictions for WLANs, on page 545
- Information About WLANs, on page 547
- Creating and Removing WLANs (GUI), on page 547
- Enabling and Disabling WLANs (GUI), on page 548
- Creating and Deleting WLANs (CLI), on page 549
- Enabling and Disabling WLANs (CLI), on page 549
- Viewing WLANs (CLI), on page 550
- Searching WLANs (GUI), on page 550
- Assigning WLANs to Interfaces, on page 550
- Configuring Network Access Identifier (CLI), on page 551

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 controllers properly route VLAN traffic.

Restrictions for WLANs

- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.

- The WLAN name and SSID can have up to 32 characters.
- Special characters are not supported for the WLAN name.
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to 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.
- All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.
- The Cisco Flex 7500 Series Controller does not support the 802.1X security variants on a centrally switched WLAN. For example, the following configurations are not allowed on a centrally switched WLAN:
  - WPA1/WPA2 with 802.1X AKM
  - WPA1/WPA2 with CCKM
  - Conditional webauth
  - Splash WEB page redirect
  - If you want to configure your WLAN in any of the above combinations, the WLAN must be configured to use local switching.
- If you configured your WLAN with EAP Passthrough and if you downgrade to an earlier controller version, you might encounter XML validation errors during the downgrade process. This problem is because EAP Passthrough is not supported in earlier releases. The configuration will default to the default security settings (WPA2/802.1X).

Note The OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the 600 Series access point to an AP group. The support for two WLANs and one remote LAN still applies to the AP Group If the 600 Series OEAP is in the default group, the WLAN or remote LAN IDs must be lower than 8.

- Profile name of WLAN can be of max 31 characters for a locally switched WLAN. For central switched WLAN, the profile name can be of 32 characters.
- 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.
- When WLAN is local switching, associate the client to local-switching WLAN where AVC is enabled. Send some traffic from client, when you check the AVC stats after 90 sec. Cisco WLC shows stats under top-apps but does not show under client. There is timer issue so for the first slot Cisco WLC might not

show stats for the clients. Earlier, only 1 sec stats for a client is seen if the timers at AP and at WLC are off by 89 seconds. Now, clearing of the stats is after 180 seconds so stats from 91 seconds to 179 seconds for a client is seen. This is done because two copies of the stats per client cannot be kept due to memory constraint in Cisco 5508 WLC.

- RADIUS Server Overwrite interface per wlan feature is not supported.
- Downloadable ACL (DACL) is not supported in the flexconnect mode or the local mode.

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

Information About WLANs

This feature enables you to control up to WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All controllers publish up to 16 WLANs to each connected access point. However, you can create till the maximum number of supported WLANs and then selectively publish these WLANs (using profiles and tags) to different access points for managing your wireless network in a better way.

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

Creating and Removing WLANs (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

This page lists all of the WLANs currently configured on the controller. For each WLAN, you can see its WLAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs appears in the upper right-hand corner of the page. If the list of WLANs spans multiple pages, you can access these pages by clicking the page number links.

Note If you want to delete a WLAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove,** or select the check box to the left of the WLAN, choose **Remove Selected** from the drop-down list, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the WLAN is removed from any access point group to which it is assigned and from the access point's radio.

Step 2 Create a new WLAN by choosing **Create New** from the drop-down list and clicking **Go**. The **WLANs > New** page appears.

Note The controller creates the default-group access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it nor delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the controller with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.

Step 3 From the Type drop-down list, choose **WLAN** to create a WLAN.

Note If you want to create a guest LAN for wired guest users, choose **Guest LAN**.

Step 4 In the Profile Name text box, enter up to 32 characters for the profile name to be assigned to this WLAN. The profile name must be unique.

Step 5 In the WLAN SSID text box, enter up to 32 characters for the SSID to be assigned to this WLAN.

Note The WLAN name and SSID can have up to 32 characters. If the WLAN is locally switched, the limit on the WLAN name is 31 characters.

Step 6 From the WLAN ID drop-down list, choose the ID number for this WLAN.

Note If the Cisco OEAP 600 is in the default group, the WLAN/Remote LAN IDs need to be set as lower than ID 8.

Step 7 Click **Apply** to commit your changes. The WLANs > Edit page appears.

Note You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

Step 8 Use the parameters on the General, Security, QoS, and Advanced tabs to configure this WLAN. See the sections in the rest of this chapter for instructions on configuring specific features for WLANs.

Step 9 On the General tab, select the **Status** check box to enable this WLAN. Be sure to leave it unselected until you have finished making configuration changes to the WLAN.

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

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

Enabling and Disabling WLANs (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

This page lists all of the WLANs currently configured on the controller.

Step 2 Enable or disable WLANs from the WLANs page by selecting the check boxes to the left of the WLANs that you want to enable or disable, choosing **Enable Selected** or **Disable Selected** from the drop-down list, and clicking **Go**.

Step 3 Click **Apply**.

Creating and Deleting WLANs (CLI)

- Create a new WLAN by entering this command:

  config wlan create wlan_id profile_name *ssid*

  Note If you do not specify an **ssid**, the **profile_name** parameter is used for both the profile name and the SSID.

  Note When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

- Delete a WLAN by entering this command:

  config wlan delete wlan_id

  Note If you try to delete a WLAN that is assigned to an access point group, you are prompted with message asking you to continue or not. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

- View the WLANs configured on the controller by entering this command:

  show wlan summary

Enabling and Disabling WLANs (CLI)

Procedure

- Enable a WLAN (for example, after you have finished making configuration changes to the WLAN) by entering this command:

  config wlan enable {*wlan_id* | **all**}

Note If the command fails, an error message appears (for example, "Request failed for wlan 10 - Static WEP key size does not match 802.1X WEP key size").

- Disable a WLAN (for example, before making any modifications to a WLAN) by entering this command: **config wlan disable** {*wlan_id* | **all**}

  where

wlan_id is a WLAN ID between 1 and 512.

all is all WLANs.

Note If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

Viewing WLANs (CLI)

- View the list of existing WLANs and to see whether they are enabled or disabled by entering this command:

  show wlan summary

Searching WLANs (GUI)

Step 1 On the WLANs page, click **Change Filter**. The Search WLANs dialog box appears.

Step 2 Perform one of the following:

- To search for WLANs based on profile name, select the **Profile Name** check box and enter the desired profile name in the edit box.
- To search for WLANs based on SSID, select the **SSID** check box and enter the desired SSID in the edit box.
- To search for WLANs based on their status, select the **Status** check box and choose **Enabled** or **Disabled** from the drop-down list.

Step 3 Click **Find**. Only the WLANs that match your search criteria appear on the WLANs page, and the Current Filter field at the top of the page specifies the search criteria used to generate the list (for example, None, Profile Name:user1, SSID:test1, Status: disabled).

Note To clear any configured search criteria and display the entire list of WLANs, click **Clear Filter**.

Assigning WLANs to Interfaces

Use these commands to assign a WLAN to an interface:

- Assign a WLAN to an interface by entering this command:

  config wlan interface {*wlan_id* | *foreignAp*} *interface_id*

- Use the *interface_id* option to assign the WLAN to a specific interface.
- Use the *foreignAp* option to use a third-party access point.

- Verify the interface assignment status by entering the **show wlan summary** command.

For the client with an IPv6 address, controller supports only one untagged interface for a controller. However, in an ideal scenario of IPv4 address, the controller supports one untagged interface per port.

Configuring Network Access Identifier (CLI)

You can configure a network access server identifier (NAS-ID) on each WLAN profile, VLAN interface, or AP group. The NAS-ID is sent to the RADIUS server by the controller through an authentication request to classify users to different groups so that the RADIUS server can send a customized authentication response.

If you configure a NAS-ID for an AP group, this NAS-ID overrides the NAS-ID that is configured for a WLAN profile or the VLAN interface. If you configure a NAS-ID for a WLAN profile, this NAS-ID overrides the NAS-ID that is configured for the VLAN interface.

- Configure a NAS-ID for a WLAN profile by entering this command:

  config wlan nasid {*nas-id-string* | **none**} *wlan-id*

- Configure a NAS-ID for a VLAN interface by entering this command:

  config interface nasid {*nas-id-string* | **none**} *interface-name*

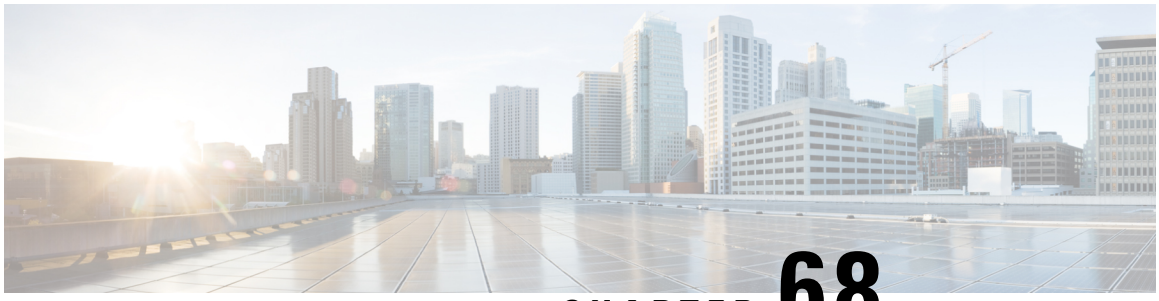
- Configure a NAS-ID for an AP group by entering this command:

  config wlan apgroup nasid {*nas-id-string* | **none**} *apgroup-name*

When the controller communicates with the RADIUS server, the NAS-ID attribute is replaced with the configured NAS-ID in an AP group, a WLAN, or a VLAN interface.

The NAS-ID that is configured on the controller for an AP group, a WLAN, or a VLAN interface is used for authentication. The configuration of NAS-ID is not propagated across controllers.

Note If WLAN interface is overridden at AP group then overridden interface NAS ID will be used. Since Interface NASID is given priority over WLAN NAS ID.



CHAPTER 68

Setting the Client Count per WLAN

- Restrictions for Setting Client Count for WLANs, on page 553
- Client Count per WLAN, on page 553
- Configuring the Client Count per WLAN (GUI), on page 554
- Configuring the Maximum Number of Clients per WLAN (CLI), on page 554
- Configuring the Maximum Number of Clients for each AP Radio per WLAN (GUI), on page 554
- Configuring the Maximum Number of Clients for each AP Radio per WLAN (CLI), on page 555
- Deauthenticating Clients (CLI), on page 555

Restrictions for Setting Client Count for WLANs

- The maximum number of clients for each WLAN feature is not supported when you use FlexConnect local authentication.
- The maximum number of clients for each WLAN feature is supported only for access points that are in connected mode.
- When a WLAN has reached the limit on the maximum number of clients connected to it or an AP radio and a new client tries to join the WLAN, the client cannot connect to the WLAN until an existing client gets disconnected.
- Roaming clients are considered as new clients. The new client can connect to a WLAN, which has reached the maximum limit on the number of connected clients, only when an existing client gets disconnected.

Note For more information about the number of clients that are supported, see the product data sheet of your controller.

Client Count per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a controller. For example, consider a scenario where the controller can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users

(employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure for each WLAN depends on the platform that you are using.

This section contains the following subsections:

Configuring the Client Count per WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to limit the number of clients. The **WLANs > Edit** page appears.

Step 3 Click the **Advanced** tab.

Step 4 In the **Maximum Allowed Clients** text box, enter the maximum number of clients that are to be allowed.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring the Maximum Number of Clients per WLAN (CLI)

Step 1 Determine the WLAN ID for which you want to configure the maximum clients by entering this command:

show wlan summary

Get the WLAN ID from the list.

Step 2 Configure the maximum number of clients for each WLAN by entering this command:

config wlan max-associated-clients *max-clients wlan-id*

Configuring the Maximum Number of Clients for each AP Radio per WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the **WLAN** for which you want to limit the number of clients. The WLANs > Edit page appears.

Step 3 In the **Advanced** tab, enter the maximum allowed clients for each access point radio in the Maximum Allowed Clients Per AP Radio text box. You can configure up to 200 clients.

Step 4 Click **Apply**.

Configuring the Maximum Number of Clients for each AP Radio per WLAN (CLI)

Step 1 Determine the WLAN ID for which you want to configure the maximum clients for each radio by entering this command:

show wlan summary

Obtain the WLAN ID from the list.

Step 2 Configure the maximum number of clients for each WLAN by entering this command:

config wlan max-radio-clients *client_count*

You can configure up to 200 clients.

Step 3 See the configured maximum associated clients by entering the **show 802.11a** command.

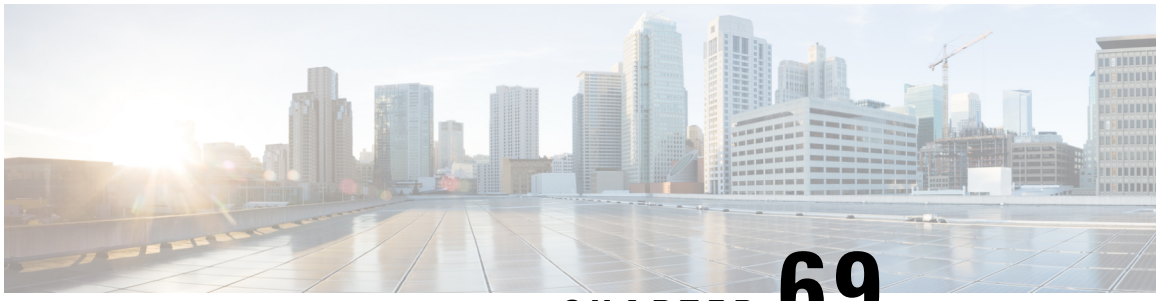
Deauthenticating Clients (CLI)

Using the controller, you can deauthenticate clients based on their user name, IP address, or MAC address. If there are multiple client sessions with the same user name, you can deauthenticate all the client sessions based on the user name. If there are overlapped IP addresses across different interfaces, you can use the MAC address to deauthenticate the clients.

Note It is not possible to deauthenticate clients using the controller GUI.

Procedure

- **config client deauthenticate** {*mac-addr* | *ipv4-addr* | *ipv6-addr* | *user-name*}



CHAPTER 69

Configuring DHCP

- Restrictions for Configuring DHCP for WLANs, on page 557
- Information about Dynamic Host Configuration Protocol, on page 557
- Configuring DHCP (GUI), on page 559
- Configuring DHCP (CLI), on page 560
- Debugging DHCP (CLI), on page 560
- DHCP Client Handling, on page 561

Restrictions for Configuring DHCP for WLANs

- Internal DHCP servers are not supported in Cisco Flex 7510 WLCs. As a workaround, you can use External DHCP servers.
- For WLANs with local switching and central DHCP feature enabled, clients with static IP addresses are not allowed. Enabling central DHCP will internally enable DHCP required option.

Information about 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.

This section contains the following subsections:

Internal DHCP Servers

The controllers 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 APs or less, with the APs on the same IP subnet as the controller.

The internal server provides DHCP addresses to wireless clients, direct-connect APs, and DHCP requests that are relayed from APs. Only lightweight access points are supported. When you want to use the internal DHCP server, ensure that you configure SVI for client VLAN and set the IP address as 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 controller, such as local subnet broadcast, Domain Name System (DNS), or priming.

Also, an internal DHCP server can serve only wireless clients, not wired clients.

When clients use the internal DHCP server of the controller, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned to 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 controller.

Note

- VRF is not supported in the internal DHCP servers.
- DHCPv6 is not supported in the internal DHCP servers.

General Guidelines

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

Note External DHCP servers can support DHCPv6.

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 controller 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 controller. 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.

Configuring DHCP (GUI)

To configure a primary DHCP server for a management, AP-manager, or dynamic interface, see the Configuring Ports and Interfaces chapter.

When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to assign an interface. The **WLANs > Edit (General)** page appears.

Step 3 On the **General** tab, unselect the **Status** check box and click Apply to disable the WLAN.

Step 4 Reclick the ID number of the WLAN.

Step 5 On the **General** tab, choose the interface for which you configured a primary DHCP server to be used with this WLAN from the **Interface** drop-down list.

Step 6 Choose the **Advanced** tab to open the **WLANs > Edit (Advanced)** page.

Step 7 If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, select the **DHCP Server Override** check box and enter the IP address of the desired DHCP server in the **DHCP Server IP Addr** text box. The default value for the check box is disabled.

Note The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override.

Note DHCP Server override is applicable only for the default group.

Note If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.

Step 8 If you want to require all clients to obtain their IP addresses from a DHCP server, select the **DHCP Addr. Assignment Required** check box. When this feature is enabled, any client with a static IP address is not allowed on the network. The default value is disabled.

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

Note PMIPv6 supports only DHCP based clients and Static IP address is not supported.

Step 9 Click **Apply**.

Step 10 On the General tab, select the **Status** check box and click **Apply** to reenable the WLAN.

Step 11 Click **Save Configuration**.

Configuring DHCP (CLI)

Step 1 Disable the WLAN by entering this command:

config wlan disable *wlan-id*

Step 2 Specify the interface for which you configured a primary DHCP server to be used with this WLAN by entering this command:

config wlan interface wlan-id *interface_name*

Step 3 If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, enter this command:

config wlan dhcp_server *wlan-id dhcp_server_ip_address* [**required**]

The **required** is an optional argument. Using this argument forces DHCP address assignment to be applied to the WLAN.

Note The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the **show wlan** command to verify that the DHCP server has been assigned to the WLAN.

Note If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.

Note PMIPv6 supports only DHCP based clients and Static IP address is not supported.

Step 4 Reenable the WLAN by entering this command:

config wlan enable *wlan-id*

Debugging DHCP (CLI)

Use these commands to debug DHCP:

- **debug dhcp packet** {**enable** | **disable**}—Enables or disables debugging of DHCP packets.

- **debug dhcp message** {**enable** | **disable**}—Enables or disables debugging of DHCP error messages.
- **debug dhcp service-port** {**enable** | **disable**}—Enables or disables debugging of DHCP packets on the service port.

DHCP Client Handling

Cisco WLC supports two modes of DHCP operations in case an external DHCP server is used, DHCP proxy mode and DHCP bridging mode.

The DHCP proxy mode serves as a DHCP helper function to achieve better security and control over DHCP transaction between the DHCP server and the wireless clients. DHCP bridging mode provides an option to make controller's role in DHCP transaction entirely transparent to the wireless clients.

Table 20: Comparison of DHCP Proxy and Bridging Modes

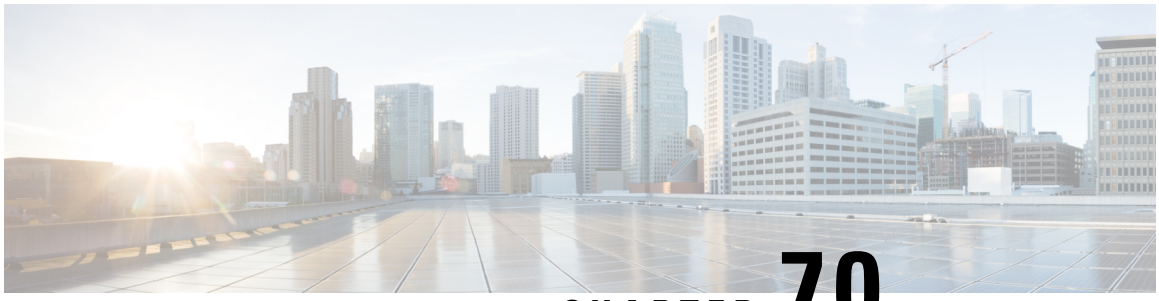
Handling Client DHCP	DHCP Proxy Mode	DHCP Bridging Mode
Modify giaddr	Yes	No
Modify siaddr	Yes	No
Modify Packet Content	Yes	No
Redundant offers not forwarded	Yes	No
Option 82 Support	Yes	No
Broadcast to Unicast	Yes	No
BOOTP support	No	Server
Per WLAN configurable	Yes	No
RFC Non-compliant	Proxy and relay agent are not exactly the same concept. But DHCP bridging mode is recommended for full RFC compliance.	No

SUMMARY STEPS

1. To enable client profiling, you must enable the **DHCP required** flag and disable the local authentication flag.
2. To configure a DHCP timeout value, use the **config dhcp timeout** command. If you have configured a WLAN to be in DHCP required state, this timer controls how long the WLC will wait for a client to get a DHCP lease through DHCP.

DETAILED STEPS

	Command or Action	Purpose
Step 1	To enable client profiling, you must enable the **DHCP required** flag and disable the local authentication flag.	
Step 2	To configure a DHCP timeout value, use the **config dhcp timeout** command. If you have configured a WLAN to be in DHCP required state, this timer controls how long the WLC will wait for a client to get a DHCP lease through DHCP.	



CHAPTER 70

Configuring DHCP Scopes

- Restrictions for Configuring Internal DHCP Server, on page 563
- Internal DHCP Server, on page 563
- Configuring DHCP Scopes (GUI), on page 564
- Configuring DHCP Scopes (CLI), on page 565

Restrictions for Configuring Internal DHCP Server

You can configure up to 16 internal DHCP servers.

Internal DHCP Server

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

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

Note The controller has the ability to provide internal DHCP server. This feature is very limited and considered as convenience that is often used simple demonstration or proof-of-concept, for example in a lab environment. The best practice is NOT to use this feature in an enterprise production network.

Read more about this at: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/110865-dhcp-wlc.html#anc16

This section contains the following subsections:

Configuring DHCP Scopes (GUI)

Step 1 Choose **Controller** > **Internal DHCP Server** > **DHCP Scope** to open the **DHCP Scopes** page.

This page lists any DHCP scopes that have already been configured.

Note If you ever want to delete an existing DHCP scope, hover your cursor over the blue drop-down arrow for that scope and choose **Remove**.

Step 2 Click **New** to add a new DHCP scope. The **DHCP Scope > New** page appears.

Step 3 In the **Scope Name** text box, enter a name for the new DHCP scope.

Step 4 Click **Apply**. When the **DHCP Scopes** page reappears, click the name of the new scope. The **DHCP Scope > Edit** page appears.

Step 5 In the **Pool Start Address** text box, enter the starting IP address in the range assigned to the clients.

Note This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 6 In the **Pool End Address** text box, enter the ending IP address in the range assigned to the clients.

Note This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 7 In the **Network** text box, enter the network served by this DHCP scope. This IP address is used by the management interface with Netmask applied, as configured on the **Interfaces** page.

Step 8 In the **Netmask** text box, enter the subnet mask assigned to all wireless clients.

Step 9 In the **Lease Time** text box, enter the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client.

Step 10 In the **Default Routers** text box, enter the IP address of the optional router connecting the controllers. Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 11 In the **DNS Domain Name** text box, enter the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers.

Step 12 In the **DNS Servers** text box, enter the IP address of the optional DNS server. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.

Step 13 In the **Netbios Name Servers** text box, enter the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server, such as the Internet Naming Service (WINS) server.

Step 14 From the **Status** drop-down list, choose **Enabled** to enable this DHCP scope or choose **Disabled** to disable it.

Step 15 Save the configuration.

Step 16 Choose **DHCP Allocated Leases** to see the remaining lease time for wireless clients. The DHCP Allocated Lease page appears, showing the MAC address, IP address, and remaining lease time for the wireless clients.

Configuring DHCP Scopes (CLI)

Step 1 Create a new DHCP scope by entering this command:

config dhcp create-scope scope

Note If you ever want to delete a DHCP scope, enter this command: **config dhcp delete-scope scope**.

Step 2 Specify the starting and ending IP address in the range assigned to the clients by entering this command:

config dhcp address-pool *scope start end*

Note This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 3 Specify the network served by this DHCP scope (the IP address used by the management interface with the Netmask applied) and the subnet mask assigned to all wireless clients by entering this command:

config dhcp network *scope network netmask*

Step 4 Specify the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client by entering this command:

config dhcp lease *scope lease_duration*

Step 5 Specify the IP address of the optional router connecting the controllers by entering this command:

config dhcp default-router *scope router_1* [*router_2*] [*router_3*]

Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 6 Specify the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers by entering this command:

config dhcp domain *scope domain*

Step 7 Specify the IP address of the optional DNS server(s) by entering this command:

config dhcp dns-servers scope *dns1* [*dns2*] [*dns3*]

Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope

Step 8 Specify the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server, such as the Internet Naming Service (WINS) server by entering this command:

config dhcp netbios-name-server *scope wins1* [*wins2*] [*wins3*]

Step 9 Enable or disable this DHCP scope by entering this command:

config dhcp {**enable** | **disable**} *scope*

Step 10 Save your changes by entering this command:

save config

Step 11 See the list of configured DHCP scopes by entering this command:

show dhcp summary

Information similar to the following appears:

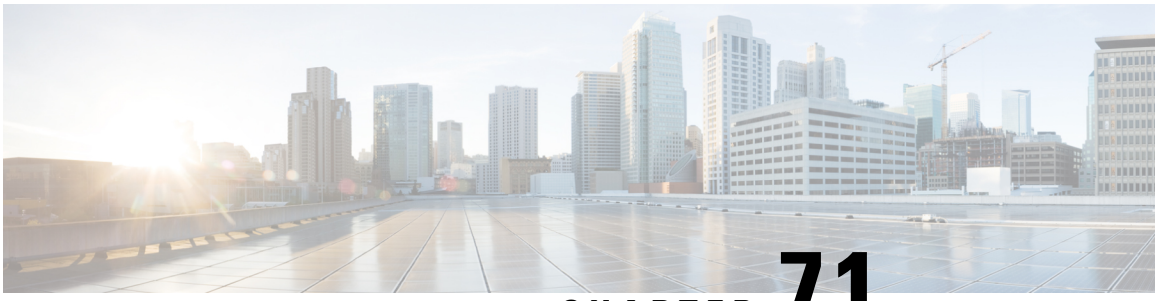
```
Scope Name            Enabled           Address Range
Scope 1       No       0.0.0.0 -> 0.0.0.0
Scope 2      No    0.0.0.0 -> 0.0.0.0
```

Step 12 Display the DHCP information for a particular scope by entering this command:

show dhcp *scope*

Information similar to the following appears:

```
Enabled..................................... No
Lease Time.................................. 0
Pool Start.................................. 0.0.0.0
Pool End.................................... 0.0.0.0
Network..................................... 0.0.0.0
Netmask..................................... 0.0.0.0
Default Routers............................. 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain.................................
DNS......................................... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers........................ 0.0.0.0 0.0.0.0 0.0.0.0
```



CHAPTER 71

Configuring MAC Filtering for WLANs

- Restrictions for MAC Filtering, on page 567
- MAC Filtering of WLANs, on page 567
- Enabling MAC Filtering, on page 567

Restrictions for MAC Filtering

- MAC filtering cannot be configured for Guest LANs.
- Central Authentication and Switching—MAC authentication takes priority over MAC filtering if an external RADIUS is configured for the WLAN.
- Local Authentication and Switching—MAC authentication does not work if MAC filtering is not supported on local authentication.
- Interface mapping and profile precedence—MAC filtering for the WLAN set to any WLAN/Interface requires a mandatory profile name, followed by the interface name for the traffic to work properly.

MAC Filtering of WLANs

When you use MAC filtering for client or administrator authorization, you need to enable it at the WLAN level first. If you plan to use local MAC address filtering for any WLAN, use the commands in this section to configure MAC filtering for a WLAN.

This section contains the following subsections:

Enabling MAC Filtering

Use these commands to enable MAC filtering on a WLAN:

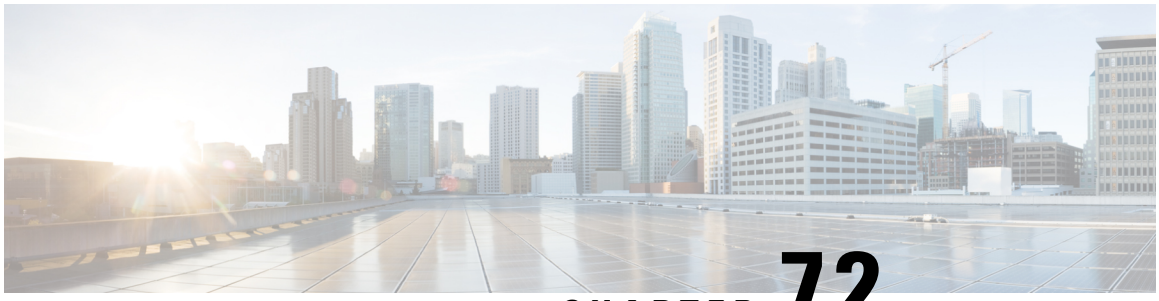
- Enable MAC filtering by entering the **config wlan mac-filtering enable** *wlan_id* command.
- Verify that you have MAC filtering enabled for the WLAN by entering the **show wlan** command.

When you enable MAC filtering, only the MAC addresses that you add to the WLAN are allowed to join the WLAN. MAC addresses that have not been added are not allowed to join the WLAN.

When a client tries to associate to a WLAN for the first time, the client gets authenticated with its MAC address from AAA server. If the authentication is successful, the client gets an IP address from DHCP server, and then the client is connected to the WLAN.

When the client roams or sends association request to the same AP or different AP and is still connected to WLAN, the client is not authenticated again to AAA server.

If the client is not connected to WLAN, then the client has to get authenticated from the AAA server.



CHAPTER 72

Configuring Local MAC Filters

- Prerequisites for Configuring Local MAC Filters, on page 569
- Local MAC Filters, on page 569
- Configuring Local MAC Filters (CLI), on page 569

Prerequisites for Configuring Local MAC Filters

You must have AAA enabled on the WLAN to override the interface name.

Local MAC Filters

Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

Configuring Local MAC Filters (CLI)

- Create a MAC filter entry on the controller by entering the **config macfilter add** *mac_addr wlan_id* [*interface_name*] [*description*] [*IP_addr*] command.

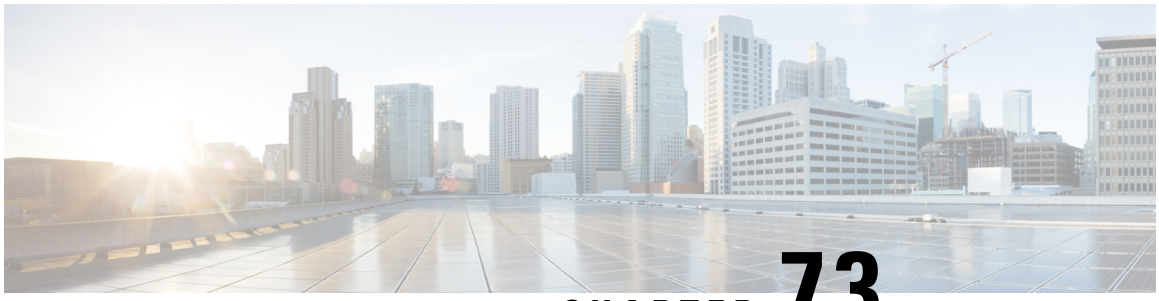
  The following parameters are optional:

  - *mac_addr*—MAC address of the client.
  - *wlan_id*—WLAN id on which the client is associating.
  - *interface_name*—The name of the interface. This interface name is used to override the interface configured to the WLAN.
  - *description*—A brief description of the interface in double quotes (for example, “Interface1”).
  - *IP_addr*—The IP address which is used for a passive client with the MAC address specified by the mac addr value above.

- Assign an IP address to an existing MAC filter entry, if one was not assigned in the **config macfilter add** command by entering the **config macfilter ip-address** *mac_addr IP_addr* command.
- Verify that MAC addresses are assigned to the WLAN by entering the **show macfilter** command.

Note For ISE NAC WLANs, the MAC authentication request is always sent to the external RADIUS server. The MAC authentication is not validated against the local database. This functionality is applicable to Releases 8.5, 8.7, 8.8, and later releases via the fix for CSCvh85830.

Previously, if MAC filtering was configured, the controller tried to authenticate the wireless clients using the local MAC filter. RADIUS servers were attempted only if the wireless clients were not found in the local MAC filter.



CHAPTER 73

Configuring Timeouts

- Configuring a Timeout for Disabled Clients, on page 571
- Configuring Session Timeout, on page 571
- Configuring the User Idle Timeout, on page 573

Configuring a Timeout for Disabled Clients

Timeout for Disabled Clients

You can configure a timeout for disabled clients. Clients who fail to authenticate three times when attempting to associate are automatically disabled from further association attempts. After the timeout period expires, the client is allowed to retry authentication until it associates or fails authentication and is excluded again. Use these commands to configure a timeout for disabled clients.

Configuring Timeout for Disabled Clients (CLI)

- Configure the timeout for disabled clients by entering the **config wlan exclusionlist** *wlan_id timeout* command. The valid timeout range is 1 to 2147483647 seconds. A value of 0 permanently disables the client.
- Verify the current timeout by entering the **show wlan** command.

Configuring Session Timeout

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.

If a WLAN is configured with Layer 2 security, for example WPA2-PSK, and a Layer 3 authentication is also configured, the WLAN session timeout value is overridden with the dot1x reauthentication timeout value. If apf reauthentication timeout value is greater than 65535, the WLAN session timeout is by default set to 65535; else, the configured dot1x reauthentication timeout value is applied as the WLAN session timeout.

This section contains the following subsections:

Configuring a Session Timeout (GUI)

Configurable session timeout range is:

- 300-86400 for 802.1X(EAP)
- 0-65535 for all other security types

Note If you configure a session-timeout of 0, it means 86400 seconds for 802.1X (EAP), and it disables the session-timeout for all other security types.

Note When a 802.1x WLAN session timeout value is modified, the associated clients pmk-cache does not change to reflect the new session time out value.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to assign a session timeout.

Step 3 When the **WLANs > Edit** page appears, choose the **Advanced** tab. The **WLANs > Edit (Advanced)** page appears.

Step 4 Select the **Enable Session Timeout** check box to configure a session timeout for this WLAN. Not selecting the checkbox is equal to setting it to 0, which is the maximum value for a session timeout for each session type.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring a Session Timeout (CLI)

Step 1 Configure a session timeout for wireless clients on a WLAN by entering this command:

config wlan session-timeout *wlan_id timeout*

The default value is 1800 seconds for the following Layer 2 security types: 802.1X, Static WEP+802.1X, WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types (Open WLAN/CKIP/Static WEP). A value of 0 is equivalent to no timeout.

For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.

Step 2 Save your changes by entering this command:

save config

Step 3 See the current session timeout value for a WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.............................. 9
Profile Name................................. test12
Network Name (SSID).......................... test12
...
Number of Active Clients..................... 0
Exclusionlist Timeout........................ 60 seconds
Session Timeout.............................. 1800 seconds
...
```

Configuring the User Idle Timeout

User Idle Timeout per WLAN

This is an enhancement to the present implementation of the user idle timeout feature, which is applicable to all WLAN profiles on the controller. With this enhancement, you can configure a user idle timeout for an individual WLAN profile. This user idle timeout is applicable to all the clients that belong to this WLAN profile.

You can also configure a threshold triggered timeout where if a client has not sent a threshold quota of data within the specified user idle timeout, the client is considered to be inactive and is deauthenticated. If the data sent by the client is more than the threshold quota specified within the user idle timeout, the client is considered to be active and the controller refreshes for another timeout period. If the threshold quota is exhausted within the timeout period, the timeout period is refreshed.

Suppose the user idle timeout is specified as 120 seconds and the user idle threshold is specified as 10 megabytes. After a period of 120 seconds, if the client has not sent 10 megabytes of data, the client is considered to be inactive and is deauthenticated. If the client has exhausted 10 megabytes within 120 seconds, the timeout period is refreshed.

This section contains the following subsections:

Configuring Per-WLAN User Idle Timeout (CLI)

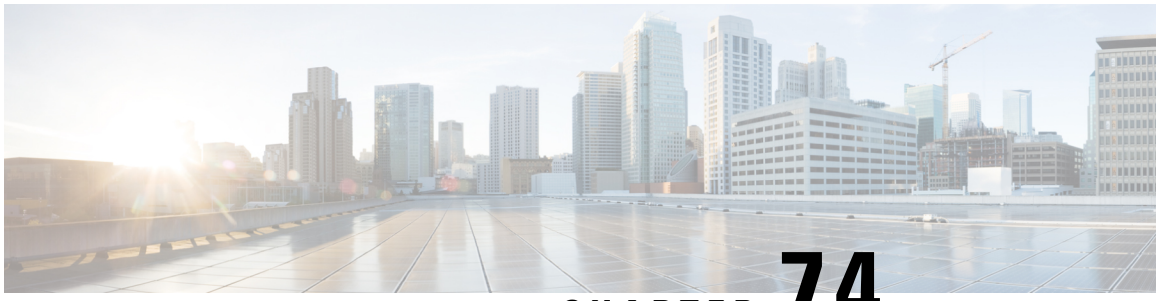
Procedure

- Configure user idle timeout for a WLAN by entering this command:

  config wlan usertimeout *timeout-in-seconds wlan-id*

- Configure user idle threshold for a WLAN by entering this command:

  config wlan user-idle-threshold *value-in-bytes wlan-id*



CHAPTER 74

Configuring the DTIM Period

- DTIM Period, on page 575
- Configuring the DTIM Period (GUI), on page 576
- Configuring the DTIM Period (CLI), on page 576

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 broadcast and multicast frames 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 for 10 times every 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 for 5 times every 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). The only recommended DTIM values are 1 and 2; higher DTIM values will likely cause communications problems.

Note A beacon period, which is specified in milliseconds on the controller, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. Depending on the AP model, the actual beacon period may vary slightly; for example, a beacon period of 100 ms may in practice equate to 104.448 ms.

You can configure the DTIM period for the 802.11 radio networks on specific WLANs. For example, you might want to set different DTIM values for voice and data WLANs.

This section contains the following subsections:

Configuring the DTIM Period (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure the DTIM period.

Step 3 Unselect the **Status** check box to disable the WLAN.

Step 4 Click **Apply**.

Step 5 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 6 Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n text boxes. The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 7 Click **Apply**.

Step 8 Choose the **General** tab to open the WLANs > Edit (General) page.

Step 9 Select the **Status** check box to reenable the WLAN.

Step 10 Click **Save Configuration**.

Configuring the DTIM Period (CLI)

Step 1 Disable the WLAN by entering this command:

config wlan disable *wlan_id*

Step 2 Configure the DTIM period for a 802.11 radio network on a specific WLAN by entering this command:

config wlan dtim {**802.11a** | **802.11b**} *dtim wlan_id*

where *dtim* is a value between 1 and 255 (inclusive). The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 3 Reenable the WLAN by entering this command:

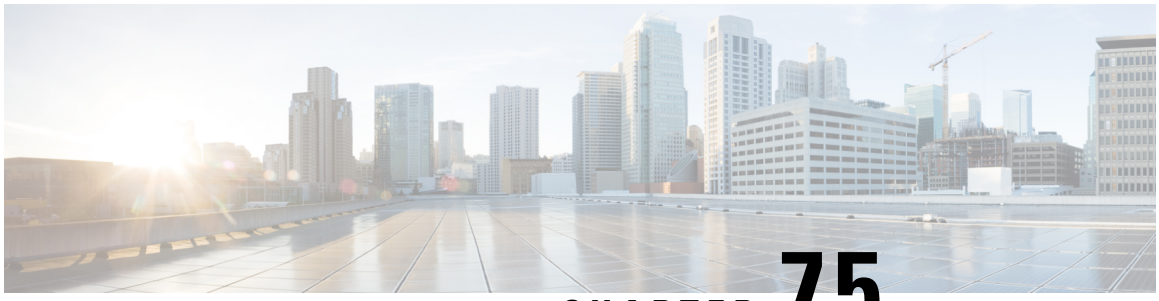
config wlan enable *wlan_id*

Step 4 Save your changes by entering this command:

save config

Step 5 Verify the DTIM period by entering this command:

show wlan *wlan_id*



CHAPTER 75

Configuring Peer-to-Peer Blocking

- Restrictions on Peer-to-Peer Blocking, on page 577
- Peer-to-Peer Blocking, on page 577
- Configuring Peer-to-Peer Blocking (GUI), on page 578
- Configuring Peer-to-Peer Blocking (CLI), on page 578

Restrictions on Peer-to-Peer Blocking

- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, solution peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all FlexConnect APs that broadcast the SSID.
- Cisco controller with central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect solution. This is treated as peer-to-peer drop and client packets are dropped.
- Cisco controller with central switching clients supports peer-to-peer blocking for clients associated with different APs. However, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.

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 controller, dropped by the controller, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.

Per WLAN, peer-to-peer configuration is pushed by the controller to FlexConnect AP. In controller software releases prior to 4.2, peer-to-peer blocking is applied globally to all clients on all WLANs and causes traffic between two clients on the same VLAN to be transferred to the upstream VLAN rather than being bridged by the controller . This behavior usually results in traffic being dropped at the upstream switch because switches do not forward packets out the same port on which they are received.

This section contains the following subsections:

Configuring Peer-to-Peer Blocking (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure peer-to-peer blocking.

Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4 Choose one of the following options from the P2P Blocking drop-down list:

- **Disabled**—Disables peer-to-peer blocking and bridges traffic locally within the controller whenever possible. This is the default value.

  Note Traffic is never bridged across VLANs in the controller.

- **Drop**—Causes the controller to discard the packets.
- **Forward-UpStream**—Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.

  Note To enable peer-to-peer blocking on a WLAN configured for FlexConnect local switching, select **Drop** from the P2P Blocking drop-down list and select the **FlexConnect Local Switching** check box.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring Peer-to-Peer Blocking (CLI)

Step 1 Configure a WLAN for peer-to-peer blocking by entering this command:

config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

Step 2 Save your changes by entering this command:

save config

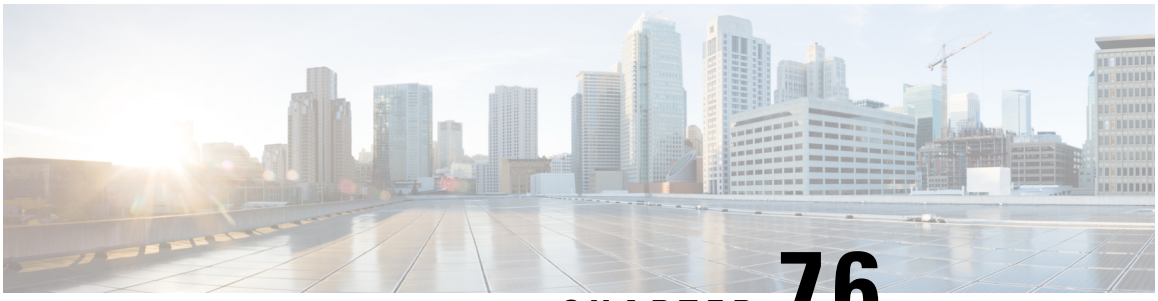
Step 3 See the status of peer-to-peer blocking for a WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
...
...
...
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
```

```
Local EAP Authentication..................... Disabled
```



CHAPTER 76

Configuring Layer2 Security

- Prerequisites for Layer 2 Security, on page 581
- Configuring Static WEP Keys (CLI), on page 582
- Configuring Dynamic 802.1X Keys and Authorization (CLI), on page 582
- Configuring 802.11r BSS Fast Transition, on page 583
- MAC Authentication Failover to 802.1X Authentication, on page 588
- Configuring 802.11w, on page 589

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 the 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.
- WLAN WEP is not supported in Cisco Aironet 1810w Access Points.

- 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.
- A WLAN configured with TKIP support will not be enabled on an RM3000AC module.

- Static WEP (not supported on Wave 2 APs)
- WPA2+WPA3
- Enhanced Open

Configuring Static WEP Keys (CLI)

Controllers can control static WEP keys across access points. Use these commands to configure static WEP for WLANs:

- Disable the 802.1X encryption by entering this command:

  config wlan security 802.1X *disable wlan_id*

- Configure 40/64-bit or 104/128-bit WEP keys by entering this command:

  config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} **key** *key_index*

  - Use the **40** or **104** option to specify 40/64-bit or 104/128-bit encryption. The default setting is 104/128.
  - Use the **hex** or **ascii** option to specify the character format for the WEP key.
  - Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F) or five printable ASCII characters for 40-bit/64-bit WEP keys or enter 26 hexadecimal or 13 ASCII characters for 104-bit/128-bit keys.
  - Enter a key index (sometimes called a *key slot*). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).

Configuring Dynamic 802.1X Keys and Authorization (CLI)

Controllers can control 802.1X dynamic WEP keys using Extensible Authentication Protocol (EAP) across access points and support 802.1X dynamic key settings for WLANs.

Note To use LEAP with lightweight access points and wireless clients, make sure to choose **Cisco-Aironet** as the RADIUS server type when configuring the CiscoSecure Access Control Server (ACS).

- Check the security settings of each WLAN by entering this command:

  show wlan *wlan_id*

  The default security setting for new WLANs is 802.1X with dynamic keys enabled. To maintain robust Layer 2 security, leave 802.1X configured on your WLANs.

- Disable or enable the 802.1X authentication by entering this command:

  config wlan security 802.1X {**enable** | **disable**} *wlan_id*

After you enable 802.1X authentication, the controller sends EAP authentication packets between the wireless client and the authentication server. This command allows all EAP-type packets to be sent to and from the controller.

Note The controller performs both web authentication and 802.1X authentication in the same WLAN. The clients are initially authenticated with 802.1X. After a successful authentication, the client must provide the web authentication credentials. After a successful web authentication, the client is moved to the run state.

- Change the 802.1X encryption level for a WLAN by entering this command:

  config wlan security 802.1X encryption *wlan_id* **[0 | 40 | 104]**

  - Use the **0** option to specify no 802.1X encryption.
  - Use the **40** option to specify 40/64-bit encryption.
  - Use the **104** option to specify 104/128-bit encryption. (This is the default encryption setting.)

Configuring 802.11r BSS Fast Transition

Restrictions for 802.11r Fast Transition

- This feature is not supported on mesh access points.
- For APs in FlexConnect mode:
  - 802.11r Fast Transition is supported in central and locally switched WLANs.
  - This feature is not supported for the WLANs enabled for local authentication.
  - 802.11r client association is not supported on access points in standalone mode.
  - 802.11r fast roaming is not supported on access points in standalone mode.
  - 802.11r fast roaming between local authentication and central authentication WLAN is not supported.
  - 802.11r fast roaming works only if the APs are in the same FlexConnect group.
- This feature is not supported on Linux-based APs such as Cisco 600 Series OfficeExtend Access Points.
- 802.11r fast roaming is not supported if the client uses Over-the-DS preauthentication in standalone mode.
- EAP LEAP method is not supported. WAN link latency prevents association time to a maximum of 2 seconds.
- The service from standalone AP to client is only supported until the session timer expires.
- TSpec is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.

- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The Cisco WLC handles 802.11r Fast Transition authentication request during roaming for both Over-the-Air and Over-the-DS methods.
- This feature is supported on open and WPA2 configured WLANs.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs.

  Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).
- Fast Transition resource request protocol is not supported because clients do not support this protocol. Also, the resource request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.
- Non-802.11r capable devices will not be able to associate with FT-enabled WLAN.
- 802.11r FT + PMF is not recommended.
- 802.11r FT Over-the-Air roaming is recommended for FlexConnect deployments.
- In a default FlexGroup scenario, fast roaming is not supported.

802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.

802.11r provides two methods of roaming:

- Over-the-Air
- Over-the-DS (Distribution System)

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

How a Client Roams

For a client to move from its current AP to a target AP using the FT protocols, the message exchanges are performed using one of the following two methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-DS—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller.

Figure 40: Message Exchanges when Over the Air client roaming is configured

This figure shows the sequence of message exchanges that occur when Over the Air client roaming is configured.

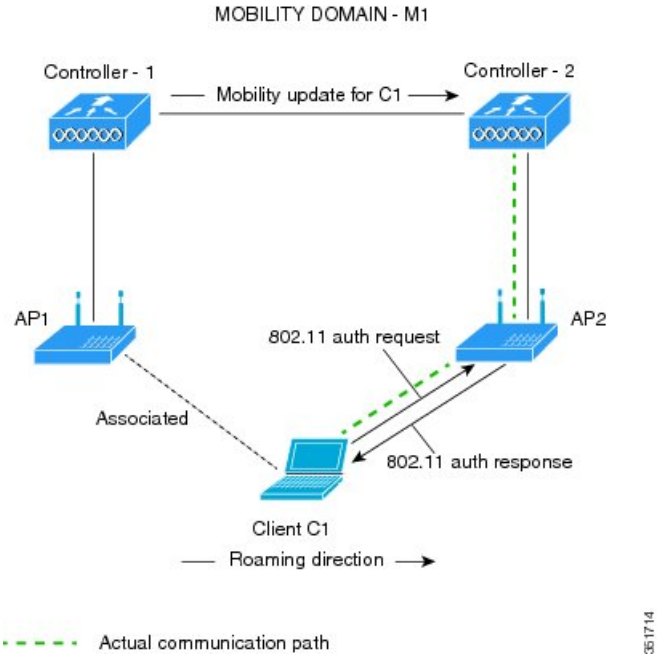
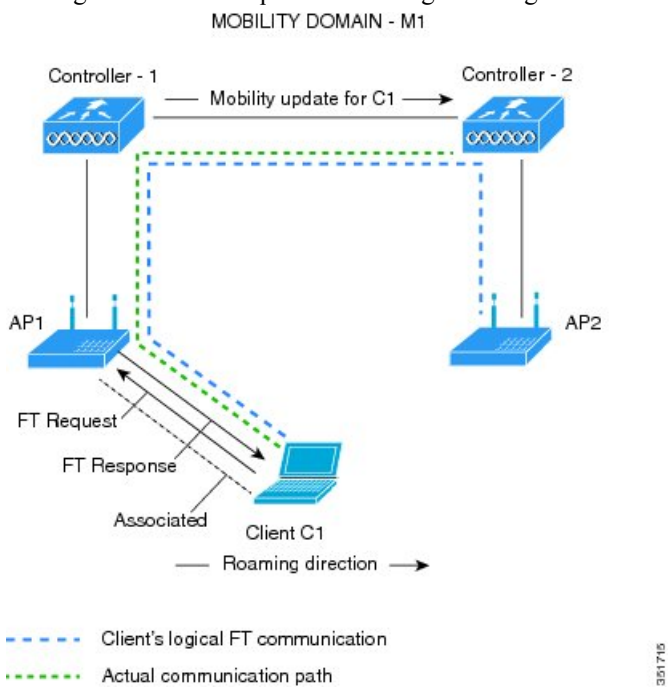


Figure 41: Message Exchanges when Over the DS client roaming is configured

This figure shows the sequence of message exchanges that occur when Over the DS client roaming is configured.



This section contains the following subsections:

Configuring 802.11r Fast Transition (GUI)

Step 1 Choose **WLANs** to open the **WLANs** window.

Step 2 Click a WLAN ID to open the **WLANs > Edit** window.

Step 3 Choose **Security** > **Layer 2** tab.

Step 4 From the **Layer 2 Security** drop-down list, choose **WPA+WPA2**.

The Authentication Key Management parameters for Fast Transition are displayed.

Step 5 From the **Fast Transition** drop-down list, choose Fast Transition on the WLAN.

Step 6 Check or uncheck the **Over the DS** check box to enable or disable Fast Transition over a distributed system.

This option is available only if you enable Fast Transition or if Fast Transition is adaptive.

To use 802.11r Fast Transition, Over-the-Air and Over-the-DS must be disabled.

Step 7 In the **Reassociation Timeout** field, enter the number of seconds after which the reassociation attempt of a client to an AP should time out. The valid range is 1 to 100 seconds.

Note This option is available only if you enable Fast Transition.

Step 8 Under Authentication Key Management, choose **FT 802.1X** or **FT PSK**. Check or uncheck the corresponding check boxes to enable or disable the keys. If you check the **FT PSK** check box, from the PSK Format drop-down list, choose **ASCII** or **Hex** and enter the key value.

Note When Fast Transition adaptive is enabled, you can use only **802.1X** and **PSK AKM.**.

Step 9 From the **WPA gtk-randomize State** drop-down list, choose **Enable** or **Disable** to configure the Wi-Fi Protected Access (WPA) group temporal key (GTK) randomize state.

Step 10 Click **Apply** to save your settings.

Configuring 802.11r Fast Transition (CLI)

Step 1 To enable or disable 802.11r fast transition parameters, use the **config wlan security ft** {**enable** | **disable**} *wlan-id* command.

Step 2 To enable or disable 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** {**enable** | **disable**} *wlan-id* command.

The Client devices normally prefer fast transition over-the-ds if the capability is advertised in the WLAN. To force a client to perform fast transition over-the-air, disable fast transition over-the-ds.

Step 3 To enable or disable the authentication key management for fast transition using preshared keys (PSK), use the **config wlan security wpa akm ft psk** {**enable** | **disable**} *wlan-id* command.

By default, the authentication key management using PSK is disabled.

Step 4 To enable or disable authentication key management for adaptive using PSK, use the **config wlan security wpa akm psk** {**enable** | **disable**} *wlan-id* command.

Step 5 To enable or disable authentication key management for fast transition using 802.1X, use the **config wlan security wpa akm ft-802.1X** {**enable** | **disable**} *wlan-id* command.

By default, authentication key management using 802.1X is enabled.

Step 6 To enable or disable authentication key management for adaptive using 802.1x, use the **config wlan security wpa akm 802.1x** {**enable** | **disable**} *wlan-id* command.

Note When Fast Transition adaptive is enabled, you can use only 802.1X and PSK AKM.

Step 7 To enable or disable 802.11r fast transition reassociation timeout, use the **config wlan security ft reassociation-timeout** *timeout-in-seconds wlan-id* command.

The valid range is 1 to 100 seconds. The default value of reassociation timeout is 20 seconds.

Step 8 To view the fast transition configuration on a WLAN, use the **show wlan** *wlan-id* command.

Step 9 To view the fast transition configuration on a client, use the **show client detail** *client-mac* command.

Note This command is relevant only for a connected or connecting client station (STA).

Step 10 To enable or disable debugging of fast transition events, use the **debug ft events** {**enable** | **disable**} command.

Troubleshooting 802.11r BSS Fast Transition

Symptom	Resolution
Non-802.11r legacy clients are no longer connecting.	Check if the WLAN has FT enabled. If so, non-FT WLAN will need to be created.
When configuring WLAN, the FT setup options are not shown.	Check if WPA2 is being used (802.1x / PSK). FT is supported only on WPA2 and OPEN SSIDs.
802.11r clients appear to reauthenticate when they do a Layer 2 roam to a new controller.	Check if the reassociation timeout has been lowered from the default of 20 by navigating to **WLANs** > *WLAN Name* > **Security** > **Layer 2** on the controller GUI.

MAC Authentication Failover to 802.1X Authentication

You can configure the controller to start 802.1X authentication when MAC authentication with static WEP for the client fails. If the RADIUS server rejects an access request from a client instead of deauthenticating the client, the controller can force the client to undergo an 802.1X authentication. If the client fails the 802.1X authentication too, then the client is deauthenticated.

If MAC authentication is successful and the client requests for an 802.1X authentication, the client has to pass the 802.1X authentication to be allowed to send data traffic. If the client does not choose an 802.1X authentication, the client is declared to be authenticated if the client passes the MAC authentication.

Note WLAN with **WPA2 + 802.1X + WebAuth with WebAuth** on MAC failure is not supported.

This section contains the following subsections:

Configuring MAC Authentication Failover to 802.1x Authentication (GUI)

Step 1 Choose **WLANs** > **WLAN ID** to open the WLANs > Edit page.
Step 2 In the **Security** tab, click the **Layer 2** tab.
Step 3 Select the **MAC Filtering** check box.
Step 4 Select the **Mac Auth or Dot1x** check box.

Configuring MAC Authentication Failover to 802.1X Authentication (CLI)

To configure MAC authentication failover to 802.1X authentication, enter this command:

config wlan security 802.1X on-macfilter-failure {**enable** | **disable**} *wlan-id*

Configuring 802.11w

Restrictions for 802.11w

- Cisco's legacy Management Frame Protection is not related to the 802.11w standard that is implemented in the 7.4 release.
- The 802.11w standard is supported on all 802.11n capable APs from Cisco WLC release 7.5.
- The 802.11w standard is supported on Cisco 2504, 5508, 8510, and WiSM2 WLCs.

  The 802.11w standard is not supported on Flex 7510 WLC and WLC.
- When 802.11w is set to optional and the keys are set, the AKM suite still shows 802.11w as disabled; this is a Wi-Fi limitation.
- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- PMF is not supported in Cisco Aironet 1810, 1815, 1832, 1852, 1542, and 1800 series APs in FlexConnect mode prior to Release 8.9.

802.11w

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Control and management frames such as authentication/deauthentication, association/disassociation, beacons, and probes are used by wireless clients to select an AP and to initiate a session for network services.

Unlike data traffic which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to tear down a session between a client and AP.

The 802.11w standard for Management Frame Protection is implemented in the 7.4 release.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Management Frame Protection (PMF) service. These include Disassociation, Deauthentication, and Robust Action frames.

Management frames that are considered as robust action and therefore protected are the following:

- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement

- Fast BSS Transition
- SA Query
- Protected Dual of Public Action
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following occur:

- Client protection is added by the AP adding cryptographic protection (by including the MIC information element) to deauthentication and disassociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) teardown protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

This section contains the following subsections:

Configuring 802.11w (GUI)

Step 1 Choose **WLANs** > WLAN ID to open the WLANs > Edit page.

Step 2 In the **Security** tab, choose the **Layer 2** security tab.

Step 3 From the Layer 2 Security drop-down list, choose **WPA+WPA2**.

The 802.11w IGTK Key is derived using the 4-way handshake, which means that it can only be used on WLANs that are configured for WPA2 security at Layer 2.

Note WPA2 is mandatory and encryption type must be AES. TKIP is not valid.

Step 4 Choose the PMF state from the drop-down list

The following options are available:

- **Disabled**—Disables 802.11w MFP protection on a WLAN
- **Optional**—To be used if the client supports 802.11w.
- **Required**—Ensures that the clients that do not support 802.11w cannot associate with the WLAN.

Step 5 If you choose the PMF state as either **Optional** or **Required**, do the following:

a) In the Comeback Timer box, enter the association comeback interval in milliseconds. It is the time within which the access point reassociates with the client after a valid security association.
b) In the SA Query Timeout box, enter the maximum time before an Security Association (SA) query times out.

Step 6 In the Authentication Key Management section, follow these steps:

a) Select or unselect the **PMF 802.1X** check box to configure the 802.1X authentication for the protection of management frames.
b) Select or unselect the **PMF PSK** check box to configure the preshared keys for PMF. Choose the PSK format as either ASCII or Hexadecimal and enter the PSK.

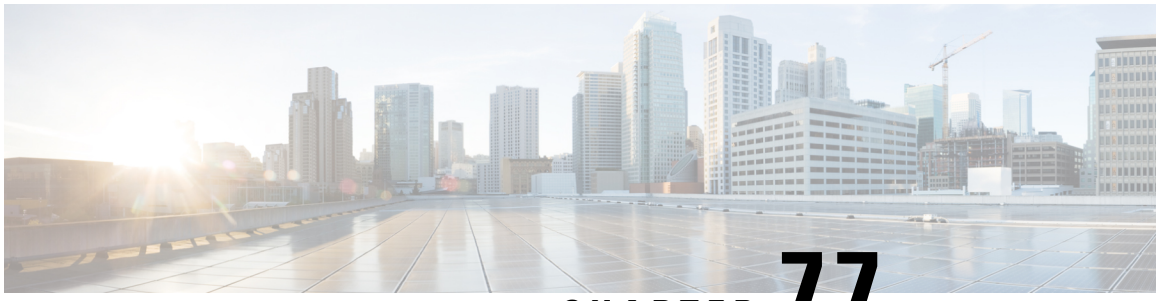
Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Configuring 802.11w (CLI)

Procedure

- Configure the 802.1X authentication for PMF by entering this command:
  config wlan security wpa akm pmf 802.1x {**enable** | **disable**} *wlan-id*
- Configure the preshared key support for PMF by entering this command:
  config wlan security wpa akm pmf psk {**enable** | **disable**} *wlan-id*
- If not done, configure a preshared key for a WLAN by entering this command:
  config wlan security wpa akm psk set-key {*ascii* | *hex*} *psk wlan-id*
- Configure protected management frames by entering this command:
  config wlan security pmf {**disable** | **optional** | **required**} *wlan-id*
- Configure the association comeback time settings by entering this command:
  config wlan security pmf association-comeback *timeout-in-seconds wlan-id*
- Configure the SA query retry timeout settings by entering this command:
  config wlan security pmf saquery-retrytimeout *timeout-in-milliseconds wlan-id*
- See the 802.11w configuration status for a WLAN by entering this command:
  show wlan *wlan-id*
- Configure the debugging of PMF by entering this command:
  debug pmf events {**enable** | **disable**}



CHAPTER 77

Configuring a WLAN for Static WEP

- Restrictions for Configuring Static WEP, on page 593
- WLAN for Static WEP, on page 593
- Configuring WPA1+WPA2, on page 595

Restrictions for Configuring Static WEP

- The OEAP 600 series does not support fast roaming for clients. Dual mode voice clients will experience reduced call quality when they roam between the two spectrums on OEAP602 access point. We recommend that you configure voice devices to only connect on one band, either 2.4 GHz or 5 GHz.
- 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 client functionality. Clients must support CCXv4 or v5 in order to use CCKM. For more information about CCX, see the Configuring Cisco Client Extensions section.
- In a unified architecture where multiple VLAN clients are supported for a WGB, you also need to configure encryption cipher suite and WEP keys globally, when the WEP encryption is enabled on the WGB. Otherwise, multicast traffic for wired VLAN clients fail.

WLAN for Static WEP

You can configure up to four WLANs to support static WEP keys. Follow these guidelines when configuring a WLAN for static WEP:

- When you configure static WEP as the Layer 2 security policy, no other security policies can be specified. That is, you cannot configure web authentication. However, when you configure static WEP as the Layer 2 security policy, you can configure web authentication.

Note Dynamic WEP encryption method is not supported. The last release to support this method was Release 7.0 (7.0.240.0 and later 7.0 releases).

WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA1 and WPA2 use 802.1X for authenticated key management by default. However, these options are also available:

- 802.1X—The standard for wireless LAN security, as defined by IEEE, is called 802.1X for 802.11, or simply 802.1X. An access point that supports 802.1X acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network. If 802.1X is selected, only 802.1X clients are supported.
- PSK—When you choose PSK (also known as WPA preshared key or WPA passphrase), you need to configure a preshared key (or a passphrase). This key is used as the pairwise master key (PMK) between the clients and the authentication server.
- CCKM—Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature. If CCKM is selected, only CCKM clients are supported.

  When CCKM is enabled, the behavior of access points differs from the controller's for fast roaming in the following ways:

  - If an association request sent by a client has CCKM enabled in a Robust Secure Network Information Element (RSN IE) but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.
  - If an association request sent by a client has CCKM enabled in RSN IE but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then AP does a full authentication. The access point does not use PMKID sent with the association request when CCKM is enabled in RSN IE.

- 802.1X+CCKM—During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and CCKM fast secure roaming, CCKM-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+CCKM is considered optional CCKM because both CCKM and non-CCKM clients are supported when this option is selected.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/CCKM/ 802.1X+CCKM information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two ciphers, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

This section contains the following subsections:

Configuring WPA1+WPA2

Configuring WPA1+WPA2 (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** page.

Step 3 Choose the **Security** and **Layer 2** tabs to open the **WLANs > Edit (Security > Layer 2)** page.

Step 4 Choose **WPA+WPA2** from the Layer 2 Security drop-down list.

Step 5 Under WPA+WPA2 Parameters, select the **WPA Policy** check box to enable WPA1, select the **WPA2 Policy** check box to enable WPA2, or select both check boxes to enable both WPA1 and WPA2.

Note The default value is disabled for both WPA1 and WPA2. If you leave both WPA1 and WPA2 disabled, the access points advertise in their beacons and probe responses information elements only for the authentication key management method that you choose in Step 7.

Step 6 Select the **AES** check box to enable AES data encryption or the **TKIP** check box to enable TKIP data encryption for WPA1, WPA2, or both. The default values are TKIP for WPA1 and AES for WPA2.

Step 7 Choose one of the following key management methods from the Auth Key Mgmt drop-down list: **802.1X**, **CCKM**, **PSK**, or **802.1X+CCKM**.

Note Cisco OEAP 600 does not support CCKM. You must choose either 802.1X or PSK.

Note For Cisco OEAP 600, the TKIP and AES security encryption settings must be identical for WPA and WPA2.

Step 8 If you chose PSK in Step 7, choose **ASCII** or **HEX** from the PSK Format drop-down list and then enter a preshared key in the blank text box. WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Note The PSK parameter is a set-only parameter. The value set for the PSK key is not visible to the user for security reasons. For example, if you selected HEX as the key format when setting the PSK key, and later when you view the parameters of this WLAN, the value shown is the default value. The default is ASCII.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring WPA1+WPA2 (CLI)

Step 1 Disable the WLAN by entering this command:

config wlan disable *wlan_id*

Step 2 Enable or disable WPA for the WLAN by entering this command:

config wlan security wpa {**enable** | **disable**} *wlan_id*

Step 3 Enable or disable WPA1 for the WLAN by entering this command:

config wlan security wpa wpa1 {**enable** | **disable**} *wlan_id*

Step 4 Enable or disable WPA2 for the WLAN by entering this command:

config wlan security wpa wpa2 {**enable** | **disable**} *wlan_id*

Step 5 Enable or disable AES or TKIP data encryption for WPA1 or WPA2 by entering one of these commands:

- **config wlan security wpa wpa1 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*
- **config wlan security wpa wpa2 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

The default values are TKIP for WPA1 and AES for WPA2.

Note You can enable or disable TKIP encryption only using the CLI. Configuring TKIP encryption is not supported in GUI.

When you have VLAN configuration on WGB, you need to configure the encryption cipher mode and keys for a particular VLAN, for example, **encryption vlan 80 mode ciphers tkip**. Then, you need configure the encryption cipher mode globally on the multicast interface by entering the following command: **encryption mode ciphers tkip**.

Step 6 Enable or disable 802.1X, PSK, or CCKM authenticated key management by entering this command:

config wlan security wpa akm {**802.1X** | **psk** | **cckm**} {**enable** | disable} *wlan_id*

The default value is 802.1X.

Step 7 If you enabled PSK in *Step 6*, enter this command to specify a preshared key:

config wlan security wpa akm psk set-key {**ascii** | **hex**} *psk-key wlan_id*

WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Step 8 Enable or disable authentication key management suite for fast transition by entering this command:

config wlan security wpa akm ft {**802.1X** | **psk**} {**enable** | **disable**} *wlan_id*

Note You can now choose between the PSK and the fast transition PSK as the AKM suite.

Step 9 Enable or disable randomization of group temporal keys (GTK) between AP and clients by entering this command:

config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

Step 10 If you enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with CCKM authenticated key management, the PMK cache lifetime timer is used to trigger reauthentication with the client when necessary. The timer is based on the timeout value received from the AAA server or the WLAN session timeout setting. To see the amount of time remaining before the timer expires, enter this command:

show pmk-cache all

If you enabled WPA2 with 802.1X authenticated key management, the controller supports both opportunistic PMKID caching and sticky (or non-opportunistic) PMKID caching. In sticky PMKID caching (SKC), the client stores multiple PMKIDs, a different PMKID for every AP it associates with. Opportunistic PMKID caching (OKC) stores only one PMKID per client. By default, the controller supports OKC.

Step 11 Enable the WLAN by entering this command:

config wlan enable wlan_id

Step 12 Save your settings by entering this command:

save config

CHAPTER 78

Configuring Sticky Key Caching

- Sticky Key Caching, on page 599
- Restrictions for Sticky Key Caching, on page 599
- Configuring Sticky Key Caching (CLI), on page 600

Sticky Key Caching

The controller supports sticky key caching (SKC). With sticky key caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client.

In SKC, the client stores each Pairwise Master Key ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

This section contains the following subsections:

Restrictions for Sticky Key Caching

- The controller supports SKC for up to eight APs per client. If a client roams to more than 8 APs per session, the old APs are removed to store the newly cached entries when the client roams. We recommend that you do not use SKC for large scale deployments.
- SKC works only on WPA2-enabled WLANs.
- SKC does not work across controllers in a mobility group.
- SKC works only on local mode APs.

Configuring Sticky Key Caching (CLI)

Step 1 Disable the WLAN by entering this command:

config wlan disable *wlan_id*

Step 2 Enable sticky key caching by entering this command:

config wlan security wpa wpa2 cache sticky enable *wlan_id*

By default, SKC is disabled and opportunistic key caching (OKC) is enabled.

Note SKC works only on WPA2 enabled WLANs.

You can check if SKC is enabled by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

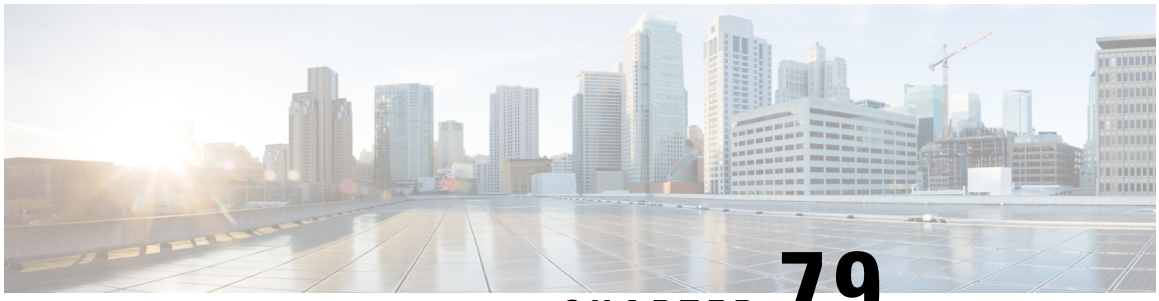
```
WLAN Identifier.................................. 2
Profile Name..................................... new
Network Name (SSID).............................. new
Status........................................... Disabled
MAC Filtering.................................... Disabled
Security
   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
      Auth Key Management
         802.1x.................................. Disabled
         PSK..................................... Enabled
         CCKM.................................... Disabled
         FT(802.11r)............................. Disabled
         FT-PSK(802.11r)......................... Disabled
     SKC Cache Support.......................... Enabled
      FT Reassociation Timeout................... 20
      FT Over-The-Air mode....................... Enabled
      FT Over-The-Ds mode........................ Enabled
CCKM tsf Tolerance............................... 1000
   Wi-Fi Direct policy configured................ Disabled
   EAP-Passthrough............................... Disabled
```

Step 3 Enable the WLAN by entering this command:

config wlan enable *wlan_id*

Step 4 Save your settings by entering this command:

save config



CHAPTER 79

Configuring CKIP

- Cisco Key Integrity Protocol , on page 603
- Configuring CKIP (GUI), on page 604
- Configuring CKIP (CLI), on page 604

Cisco Key Integrity Protocol

Cisco Key Integrity Protocol (CKIP) is a Cisco-proprietary security protocol for encrypting 802.11 media. CKIP improves 802.11 security in infrastructure mode using key permutation, a message integrity check (MIC), and a message sequence number. For this feature to operate correctly, you must enable Aironet information elements (IEs) for the WLAN.

A lightweight access point advertises support for CKIP in beacon and probe response packets by adding an Aironet IE and setting one or both of the CKIP negotiation bits (key permutation and multi-modular hash message integrity check [MMH MIC]). Key permutation is a data encryption technique that uses the basic encryption key and the current initialization vector (IV) to create a new key. MMH MIC prevents bit-flip attacks on encrypted packets by using a hash function to compute message integrity code.

The CKIP settings specified in a WLAN are mandatory for any client attempting to associate. If the WLAN is configured for both CKIP key permutation and MMH MIC, the client must support both. If the WLAN is configured for only one of these features, the client must support only the CKIP feature.

CKIP requires that 5-byte and 13-byte encryption keys be expanded to 16-byte keys. The algorithm to perform key expansion occurs at the access point. The key is appended to itself repeatedly until the length reaches 16 bytes. All lightweight access points support CKIP.

Note CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a WLAN that is configured for CKIP. We recommend that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

Configuring CKIP (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Choose the **Advanced** tab.

Step 4 Select the **Aironet IE** check box to enable Aironet IEs for this WLAN and click **Apply**.

Step 5 Choose the **General** tab.

Step 6 Unselect the **Status** check box, if selected, to disable this WLAN and click **Apply**.

Step 7 Choose the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page.

Step 8 Choose **CKIP** from the Layer 2 Security drop-down list.

Step 9 Under CKIP Parameters, choose the length of the CKIP encryption key from the Key Size drop-down list.The range is Not Set, 40 bits, or 104 bits and the default is Not Set.

Step 10 Choose the number to be assigned to this key from the Key Index drop-down list. You can configure up to four keys.

Step 11 From the Key Format drop-down list, choose **ASCII** or **HEX** and then enter an encryption key in the Encryption Key text box. 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.

Step 12 Select the **MMH Mode** check box to enable **MMH MIC** data protection for this WLAN. The default value is disabled (or unselected).

Step 13 Select the **Key Permutation** check box to enable this form of CKIP data protection. The default value is disabled (or unselected).

Step 14 Click **Apply** to commit your changes.

Step 15 Choose the **General** tab.

Step 16 Select the **Status** check box to enable this WLAN.

Step 17 Click **Apply** to commit your changes.

Step 18 Click **Save Configuration** to save your changes.

Configuring CKIP (CLI)

Step 1 Disable the WLAN by entering this command:

config wlan disable *wlan_id*

Step 2 Enable Aironet IEs for this WLAN by entering this command:

config wlan ccx aironet-ie enable *wlan_id*

Step 3 Enable or disable CKIP for the WLAN by entering this command:

config wlan security ckip {**enable** | **disable**} *wlan_id*

Step 4 Specify a CKIP encryption key for the WLAN by entering this command:

config wlan security ckip akm psk set-key *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key_index*

Step 5 Enable or disable CKIP MMH MIC for the WLAN by entering this command:

config wlan security ckip mmh-mic {**enable** | **disable**} *wlan_id*

Step 6 Enable or disable CKIP key permutation for the WLAN by entering this command:

config wlan security ckip kp {**enable** | **disable**} *wlan_id*

Step 7 Enable the WLAN by entering this command:

config wlan enable wlan_id

Step 8 Save your settings by entering this command:

save config

CHAPTER 80

Configuring Layer 3 Security

• Configuring Layer 3 Security Using Web Authentication, on page 607

Configuring Layer 3 Security Using Web Authentication

Prerequisites for Configuring Web Authentication on a WLAN

- To initiate HTTP/HTTPS web authentication redirection, use HTTP URL or HTTPS URL.
- If the CPU ACLs are configured to block HTTP / HTTPS traffic, after the successful web login authentication, there could be a failure in the redirection page.
- Before enabling web authentication, make sure that all proxy servers are configured for ports other than port 53.
- When you enable web authentication for a WLAN, a message appears indicating that the controller forwards DNS traffic to and from wireless clients prior to authentication. We recommend that you have a firewall or intrusion detection system (IDS) behind your guest VLAN to regulate DNS traffic and to prevent and detect any DNS tunneling attacks.
- If the web authentication is enabled on the WLAN and you also have the CPU ACL rules, the client-based web authentication rules take higher precedence as long as the client is unauthenticated (in the webAuth_Reqd state). Once the client goes to the RUN state, the CPU ACL rules get applied. Therefore, if the CPU ACL rules are enabled in the controller, an allow rule for the virtual interface IP is required (in any direction) with the following conditions:
    - When the CPU ACL does not have an allow ACL rule for both directions.
    - When an allow ALL rule exists, but also a DENY rule for port 443 or 80 of higher precedence.
- The allow rule for the virtual IP should be for TCP protocol and port 80 (if secureweb is disabled) or port 443 (if secureweb is enabled). This process is required to allow client's access to the virtual interface IP address, post successful authentication when the CPU ACL rules are in place.

Restrictions for Configuring Web Authentication on a WLAN

- Web authentication is supported only with these Layer 2 security policies: open authentication, open authentication+WEP, and WPA-PSK. With the 7.4 release, web authentication is supported for use with 802.1X.
- Special charecters are not supported in the username field for web-authentication.
- When clients connect to a WebAuth SSID and a preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.

  You can select the following identity stores to authenticate web-auth user, under **WLANs > Security > AAA servers > Authentication priority** order for web-auth user section:

  - Local
  - RADIUS
  - LDAP

  If multiple identity stores are selected, then the controller checks each identity store in the list, in the order specified, from top to bottom, until authentication for the user succeeds. The authentication fails, if the controller reaches the end of the list and user remains un-authenticated in any of the identity stores.

Information About Web Authentication

WLANs can use web authentication only if VPN passthrough is not enabled on the controller. Web authentication is simple to set up and use and can be used with SSL to improve the overall security of the WLAN.

Configuring Web Authentication

Configuring Web Authentication (GUI)

Step 1 Choose **WLANs** to open the WLANs page.
Step 2 Click the ID number of the WLAN for which you want to configure web authentication. The **WLANs > Edit** page appears.
Step 3 Choose the **Security** and **Layer 3** tabs to open the **WLANs > Edit (Security > Layer 3)** page.
Step 4 Select the **Web Policy** check box.
Step 5 Make sure that the **Authentication** option is selected.
Step 6 Click **Apply** to commit your changes.
Step 7 Click **Save Configuration** to save your settings.

Configuring Web Authentication (CLI)

Step 1 Enable or disable web authentication on a particular WLAN by entering this command:

config wlan security web-auth {**enable** | **disable**} *wlan_id*

Step 2 Release the guest user IP address when the web authentication policy timer expires and prevent the guest user from acquiring an IP address for 3 minutes by entering this command:

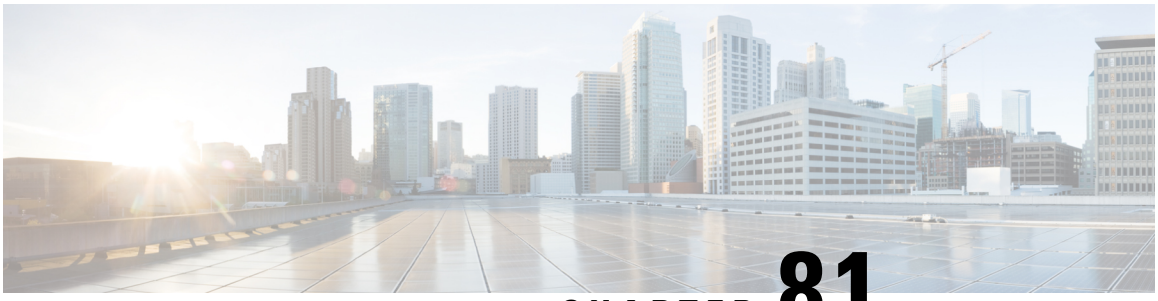
config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

The default value is disabled. This command is applicable when you configure the internal DHCP scope on the controller. By default, when the web authentication timer expires for a guest user, the user can immediately reassociate to the same IP address before another guest user can acquire it. If there are many guest users or limited IP addresses in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the web authentication policy timer expires and the guest user is excluded from acquiring an IP address for 3 minutes. The IP address is available for another guest user to use. After 3 minutes, the excluded guest user can reassociate and acquire an IP address, if available.

Step 3 See the status of web authentication by entering this command:

show wlan *wlan_id*



CHAPTER 81

Configuring Captive Bypassing

- Captive Bypassing, on page 611
- Configuring Captive Bypassing (CLI), on page 612

Captive Bypassing

WISPr is a draft protocol that enables users to roam between different wireless service providers. Some devices (For example, Apple iOS devices) have a mechanism using which they can determine if the device is connected to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used for the device to automatically open a web browser when a direct connection to the internet is not possible. This enables the user to provide his credentials to access the internet. The actual authentication is done in the background every time the device connects to a new SSID.

This HTTP request triggers a web authentication interception in the controller as any other page requests are performed by a wireless client. This interception leads to a web authentication process, which will be completed normally. If the web authentication is being used with any of the controller splash page features (URL provided by a configured RADIUS server), the splash page may never be displayed because the WISPr requests are made at very short intervals, and as soon as one of the queries is able to reach the designated server, any web redirection or splash page display process that is performed in the background is terminated, and the device processes the page request, thus breaking the splash page functionality.

For example, Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to http://www.apple.com/library/test/success.html for Apple IOS version 6 and older, and to several possible target URLs for Apple IOS version 7 and later. If a response is received, then the Internet access is assumed to be available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an ISE captive portal. The controller prevents this pseudo-browser from popping up.

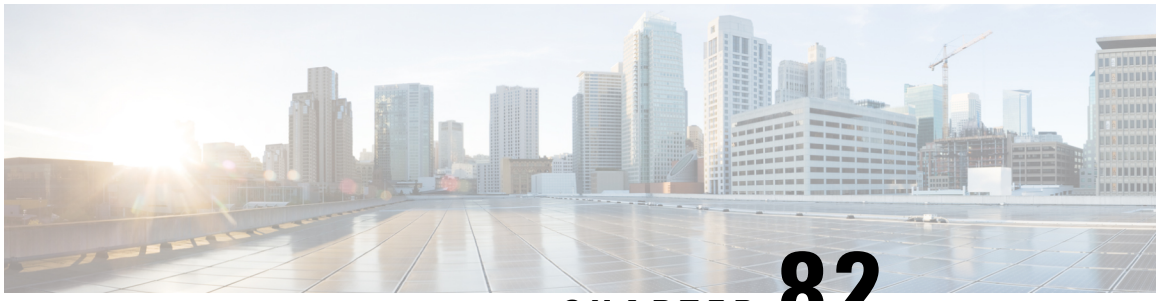
You can now configure the controller to bypass WISPr detection process, so the web authentication interception is only done when a user requests a web page leading to splash page load in user context, without the WISPr detection being performed in the background.

This section contains the following subsections:

Configuring Captive Bypassing (CLI)

Use these commands to configure captive bypassing:

- **config network web-auth captive-bypass** {**enable** | **disable**}—Enables or disables the controller to support bypass of captive portals at the network level.
- **show network summary**—Displays the status for the WISPr protocol detection feature.



CHAPTER 82

Configuring a Fallback Policy with MAC Filtering and Web Authentication

- Fallback Policy with MAC Filtering and Web Authentication, on page 613
- Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI), on page 613
- Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI), on page 614

Fallback Policy with MAC Filtering and Web Authentication

You can configure a fallback policy mechanism that combines Layer 2 and Layer 3 security. In a scenario where you have both MAC filtering and web authentication implemented, when a client tries to connect to a WLAN using the MAC filter (RADIUS server), if the client fails the authentication, you can configure the authentication to fall back to web authentication. When a client passes the MAC filter authentication, the web authentication is skipped and the client is connected to the WLAN. With this feature, you can avoid disassociations based on only a MAC filter authentication failure.

Restrictions

- MAC filtering does not support passthrough web-authentication. It supports only username and password for web-authentication.

Mobility is not supported for SSIDs with security type configured for Webauth on MAC filter failure.

This section contains the following subsections:

Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI)

Note Before configuring a fallback policy, you must have MAC filtering enabled.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure the fallback policy for web authentication. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page.

Step 4 From the Layer 3 Security drop-down list, choose **None.**

Step 5 Select the **Web Policy** check box.

Note The controller forwards DNS traffic to and from wireless clients prior to authentication.

The following options are displayed:

- Authentication
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- On MAC Filter Failure

Step 6 Click **On MAC Filter Failure**.

Step 7 Click **Apply** to commit your changes.

Step 8 Click **Save Configuration** to save your settings.

Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI)

Note Before configuring a fallback policy, you must have MAC filtering enabled.

Step 1 Enable or disable web authentication on a particular WLAN by entering this command:

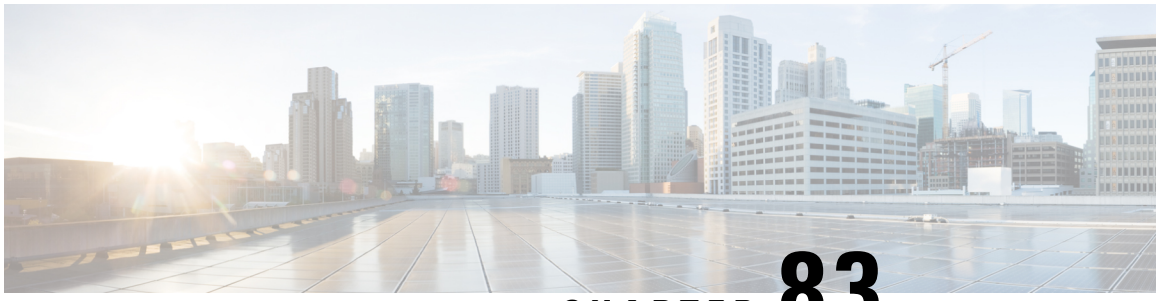
config wlan security web-auth on-macfilter-failure *wlan-id*

Step 2 See the web authentication status by entering this command:

show wlan *wlan_id*

```
FT Over-The-Ds mode.............................. Enabled
CKIP ..................................... Disabled
   IP Security.................................... Disabled
   IP Security Passthru........................... Disabled
   Web Based Authentication....................... Enabled-On-MACFilter-Failure
        ACL.......................................... Unconfigured
        Web Authentication server precedence:
        1.............................................. local
        2.............................................. radius
```

```
3.............................................. ldap
```



CHAPTER 83

Assigning a QoS Profile to a WLAN

- QoS Profiles, on page 617
- Assigning a QoS Profile to a WLAN (GUI), on page 618
- Assigning a QoS Profile to a WLAN (CLI), on page 619

QoS Profiles

Cisco UWN solution WLANs support four levels of QoS: Platinum/Voice, Gold/Video, Silver/Best Effort (default), and Bronze/Background. You can configure the voice traffic WLAN to use Platinum QoS, assign the low-bandwidth WLAN to use Bronze QoS, and assign all other traffic between the remaining QoS levels.

The WLAN QoS level defines a specific 802.11e user priority (UP) for over-the-air traffic. This UP is used to derive the over-the-wire priorities for non-WMM traffic, and it also acts as the ceiling when managing WMM traffic with various levels of priorities.

The wireless rate limits can be defined on both upstream and downstream traffic. Rate limits can be defined per SSID and/or specified as a maximum rate limit for all clients. These rate limits can be individually configured.

The access point uses this QoS-profile-specific UP in accordance with the values in the following table to derive the IP DSCP value that is visible on the wired LAN.

Table 21: Access Point QoS Translation Values

AVVID Traffic Type	AVVID IP DSCP	QoS Profile	AVVID 802.1p	IEEE 802.11e UP
Network control	56 (CS7)	Platinum	7	7
Inter-network control (CAPWAP control, 802.11 management)	48 (CS6)	Platinum	6	7
Voice	46 (EF)	Platinum	5	6
Interactive video	34 (AF41)	Gold	4	5
Mission critical	26 (AF31)	Gold	3	4
Transactional	18 (AF21)	Silver	2	3

AVVID Traffic Type	AVVID IP DSCP	QoS Profile	AVVID 802.1p	IEEE 802.11e UP
Bulk data	10 (AF11)	Bronze	1	2
Best effort	0 (BE)	Silver	0	0
Scavenger	2	Bronze	0	1

Note The IEEE 802.11e UP value for DSCP values that are not mentioned in the table is calculated by considering 3 MSB bits of DSCP.

For example, the IEEE 802.11e UP value for DSCP 32 (100 000 in binary), would be the decimal equivalent of the MSB (100) which is 4. The 802.11e UP value of DSCP 32 is 4.

This section contains the following subsections:

Assigning a QoS Profile to a WLAN (GUI)

Before you begin

If you have not already done so, configure one or more QoS profiles using the instructions in the Configuring QoS Profiles (GUI) section.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to which you want to assign a QoS profile.

Step 3 When the **WLANs > Edit** page appears, choose the **QoS** tab.

Step 4 From the **Quality of Service (QoS)** drop-down list, choose one of the following:

- **Platinum** (**voice**)
- **Gold (video)**
- **Silver (best effort)**
- **Bronze** (**background**)

Note Silver (best effort) is the default value.

Step 5 To define the data rates on a per-user basis, do the following:

a) Define the average data rate TCP traffic per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic in the WLANs.

c) Define the average real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.
d) Define the peak real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic in the WLANs.

Step 6 To define the data rates on a per-SSID basis, do the following:

a) Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.
b) Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Ensure that you configure the average data rate before you configure the burst data rate.

c) Define the average real-time rate for UDP traffic per user by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

d) Define the peak real-time rate for UDP traffic per user by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 7 Save the configuration.

Assigning a QoS Profile to a WLAN (CLI)

If you have not already done so, configure one or more QoS profiles using the instructions in the Configuring QoS Profiles (CLI) section.

Step 1 Assign a QoS profile to a WLAN by entering this command:

config wlan qos *wlan_id* {**bronze** | **silver** | **gold** | **platinum**}

Silver is the default value.

Step 2 To override QoS profile rate limit parameters, enter this command:

config wlan override-rate-limit *wlan-id* {**average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 3 Enter the **save config** command.

Step 4 Verify that you have properly assigned the QoS profile to the WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist.................................... Disabled
Session Timeout.................................. 0
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... 1.100.163.24
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
...
```

CHAPTER 84

Configuring QoS Enhanced BSS

- Prerequisites for Using QoS Enhanced BSS on Cisco 7921 and 7920 Wireless IP Phones, on page 621
- Restrictions for QoS Enhanced BSS, on page 622
- QoS Enhanced BSS, on page 622
- Configuring QBSS (GUI), on page 623
- Configuring QBSS (CLI), on page 623

Prerequisites for Using QoS Enhanced BSS on Cisco 7921 and 7920 Wireless IP Phones

Follow these guidelines to use Cisco 7921 and 7920 Wireless IP Phones with controllers:

- Aggressive load balancing must be disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11b dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The 7921 or 7920 phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
- Both the 7921 and 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7921 or 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7921 or 7920.
- For standalone 7921 phones, load-based CAC must be enabled, and the WMM Policy must be set to Required on the WLAN.
- The controller supports traffic classification (TCLAS) coming from 7921 phones using firmware version 1.1.1. This feature ensures proper classification of voice streams to the 7921 phones.
- When using a 7921 phone with the 802.11a radio of a 1242 series access point, set the 24-Mbps data rate to Supported and choose a lower Mandatory data rate (such as 12 Mbps). Otherwise, the phone might experience poor voice quality.

Restrictions for QoS Enhanced BSS

- The OEAP 600 Series access points do not support CAC.
- QBSS is disabled by default.
- 7920 phones are non-WMM phones with limited CAC functionality. The phones look at the channel utilization of the access point to which they are associated and compare that to a threshold that is beaconed by the access point. If the channel utilization is less than the threshold, the 7920 places a call. In contrast, 7921 phones are full-fledged WMM phones that use traffic specifications (TSPECs) to gain access to the voice queue before placing a phone call. The 7921 phones work well with load-based CAC, which uses the percentage of the channel set aside for voice and tries to limit the calls accordingly.

  Because 7921 phones support WMM and 7920 phones do not, capacity and voice quality problems can arise if you do not properly configure both phones when they are used in a mixed environment. To enable both 7921 and 7920 phones to co-exist on the same network, make sure that load-based CAC and 7920 AP CAC are both enabled on the controller and the WMM Policy is set to Allowed. These settings become particularly important if you have many more 7920 users than 7921 users.
- We recommend that aggressive load balancing always be turned off either through the controller GUI or CLI in any wireless network that is supporting voice, regardless of vendor. When aggressive load balancing is turned on, voice clients can hear an audible artifact when roaming, if the handset is refused at its first reassociation attempt.

QoS Enhanced BSS

The QoS Enhanced Basis Service Set (QBSS) information element (IE) enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7921 or 7920 phone uses the QBSS value to determine if they should associate to another access point. You can enable QBSS in these two modes:

- Wi-Fi Multimedia (WMM) mode, which supports devices that meet the 802.11E QBSS standard (such as Cisco 7921 IP Phones)
- 7920 support mode, which supports Cisco 7920 IP Phones on your 802.11b/g network

  The 7920 support mode has two options:

  - Support for 7920 phones that require call admission control (CAC) to be configured on and advertised by the client device (these are typically older 7920 phones)
  - Support for 7920 phones that require CAC to be configured on and advertised by the access point (these are typically newer 7920 phones)

    When access point-controlled CAC is enabled, the access point sends out a Cisco proprietary CAC Information Element (IE) and does not send out the standard QBSS IE.

This section contains the following subsections:

Configuring QBSS (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure WMM mode.

Step 3 When the **WLANs > Edit** page appears, choose the **QoS** tab to open the **WLANs > Edit (Qos)** page.

Step 4 From the WMM Policy drop-down list, choose one of the following options, depending on whether you want to enable WMM mode for 7921 phones and other devices that meet the WMM standard:

- **Disabled**—Disables WMM on the WLAN. This is the default value.
- **Allowed**—Allows client devices to use WMM on the WLAN.
- **Required**—Requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 5 Select the **7920 AP CAC** check box if you want to enable 7920 support mode for phones that require access point-controlled CAC. The default value is unselected.

Step 6 Select the **7920 Client CAC** check box if you want to enable 7920 support mode for phones that require client-controlled CAC. The default value is unselected.

Note You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Step 7 Click **Apply** to commit your changes.

Step 8 Click **Save Configuration** to save your changes.

Configuring QBSS (CLI)

Step 1 Determine the ID number of the WLAN to which you want to add QBSS support by entering this command:

show wlan summary

Step 2 Disable the WLAN by entering this command:

config wlan disable *wlan_id*

Step 3 Configure WMM mode for 7921 phones and other devices that meet the WMM standard by entering this command:

config wlan wmm {**disabled** | **allowed** | **required**} *wlan_id*

where

- **disabled** disables WMM mode on the WLAN.
- **allowed** allows client devices to use WMM on the WLAN.
- **required** requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 4 Enable or disable 7920 support mode for phones that require client-controlled CAC by entering this command:

config wlan 7920-support client-cac-limit {**enable** | **disable**} *wlan_id*

Note You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Step 5 Enable or disable 7920 support mode for phones that require access point-controlled CAC by entering this command:

config wlan 7920-support ap-cac-limit {**enable** | **disable**} *wlan_id*

Step 6 Reenable the WLAN by entering this command:

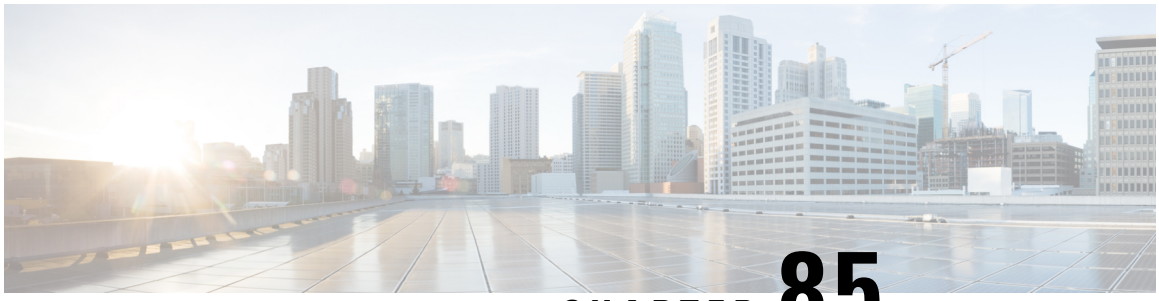
config wlan enable *wlan_id*

Step 7 Save your changes by entering this command:

save config

Step 8 Verify that the WLAN is enabled and the Dot11-Phone Mode (7920) text box is configured for compact mode by entering this command:

show wlan *wlan_id*



CHAPTER 85

Configuring Media Session Snooping and Reporting

- Media Session Snooping and Reporting, on page 625
- Restrictions for Media Session Snooping and Reporting, on page 625
- Configuring Media Session Snooping (GUI), on page 626
- Configuring Media Session Snooping (CLI), on page 626

Media Session Snooping and Reporting

This feature enables access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) voice calls and then report them to the controller and Cisco Prime Infrastructure. You can enable or disable Voice over IP (VoIP) snooping and reporting for each WLAN.

When you enable VoIP Media Session Aware (MSA) snooping, the access point radios that advertise this WLAN look for SIP voice packets that comply with SIP RFC 3261. They do not look for non-RFC 3261-compliant SIP voice packets or Skinny Call Control Protocol (SCCP) voice packets. Any SIP packets destined to or originating from port number 5060 (the standard SIP signaling port) are considered for further inspection. The access points track when Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, are already on an active call, or are in the process of ending a call. Upstream packet classification for both client types occurs at the access point. Downstream packet classification occurs at the controller for WMM clients and at the access point for non-WMM clients. The access points notify the controller and Cisco Prime Infrastructure of any major call events, such as call establishment, termination, and failure.

The controller provides detailed information for VoIP MSA calls. For failed calls, the controller generates a trap log with a timestamp and the reason for failure (in the GUI) and an error code (in the CLI) to aid in troubleshooting. For successful calls, the controller shows the number and duration of calls for usage tracking purposes. Cisco Prime Infrastructure displays failed VoIP call information in the Events page.

This section contains the following subsections:

Restrictions for Media Session Snooping and Reporting

Controller software release 6.0 or later releases support Voice over IP (VoIP) Media Session Aware (MSA) snooping and reporting.

Configuring Media Session Snooping (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure media session snooping.

Step 3 On the **WLANs > Edit** page, click the **Advanced** tab.

Step 4 Under Voice, select the **Media Session Snooping** check box to enable media session snooping or unselect it to disable this feature. The default value is unselected.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Step 7 See the VoIP statistics for your access point radios as follows:

a) Choose **Monitor** > **Access Points** > **Radios** > **802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

b) Scroll to the right and click the **Detail** link for the access point for which you want to view VoIP statistics. The **Radio > Statistics** page appears.

The VoIP Stats section shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the controller.

Step 8 Choose **Management** > **SNMP** > **Trap Logs** to see the traps generated for failed calls. The Trap Logs page appears.

For example, log 0 in the figure shows that a call failed. The log provides the date and time of the call, a description of the failure, and the reason why the failure occurred.

Configuring Media Session Snooping (CLI)

Step 1 Enable or disable VoIP snooping for a particular WLAN by entering this command:

config wlan call-snoop {**enable** | **disable**} *wlan_id*

Step 2 Save your changes by entering this command:

save config

Step 3 See the status of media session snooping on a particular WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wpa2-psk
Network Name (SSID).............................. wpa2-psk
Status........................................... Enabled
...
 FlexConnect Local Switching...................... Disabled
```

```
    FlexConnect Learn IP Address..................... Enabled
    Infrastructure MFP protection.............. Enabled (Global Infrastructure MFP
Disabled)
 Client MFP..................................... Optional
    Tkip MIC Countermeasure Hold-down Timer....... 60
Call Snooping.................................. Enabled
```

Step 4 See the call information for an MSA client when media session snooping is enabled and the call is active by entering this command:

show call-control client callInfo *client_MAC_address*

Information similar to the following appears:

```
Uplink IP/port..................................... 192.11.1.71 / 23870
Downlonk IP/port................................... 192.12.1.47 / 2070
UP................................................. 6
Calling Party...................................... sip:1054
Called Party....................................... sip:1000
Call ID............................................ 58635b00-850161b7-14853-1501a8
Number of calls for given client is.............. 1
```

Step 5 See the metrics for successful calls or the traps generated for failed calls by entering this command:

show call-control ap {**802.11a** | **802.11b**} *Cisco_AP* {**metrics** | **traps**}

Information similar to the following appears when you enter **show call-control ap** {**802.11a** | **802.11b**} *Cisco_AP* **metrics**:

```
Total Call Duration in Seconds................... 120
Number of Calls.................................. 10
```

Information similar to the following appears when you enter **show call-control ap** {**802.11a** | **802.11b**} *Cisco_AP* **traps**:

```
Number of traps sent in one min.................. 2
Last SIP error code.............................. 404
Last sent trap timestamp..................... Jun 20 10:05:06
```

To aid in troubleshooting, the output of this command shows an error code for any failed calls. This table explains the possible error codes for failed calls.

Table 22: Error Codes for Failed VoIP Calls

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.

Error Code	Integer	Description
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.
405	methodNotallowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.
406	notAcceptabl	The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header text box sent in the request.
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	The server could not produce a response within a suitable amount of time, if it could not determine the location of the user in time.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.

Error Code	Integer	Description
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header text box.
480	temporarilyNotAvailable	The callee's end system was contacted successfully, but the callee is currently unavailable.
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header text box with the value zero.
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	The callee's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	notImplemented	The server does not support the functionality required to fulfill the request.
502	badGateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.

Error Code	Integer	Description
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

Note If you experience any problems with media session snooping, enter the **debug call-control** {**all** | **event**} {**enable** | **disable**} command to debug all media session snooping messages or events.

CHAPTER 86

Configuring Key Telephone System-Based CAC

- Restrictions for Key Telephone System-Based CAC, on page 631
- Key Telephone System-Based CAC, on page 631
- Configuring KTS-based CAC (GUI), on page 632
- Configuring KTS-based CAC (CLI), on page 632

Restrictions for Key Telephone System-Based CAC

- The controller ignores the SSID Capability Check Request message from the clients.
- Preferred call is not supported for KTS CAC clients.
- Reason code 17 is not supported in intercontroller roaming scenarios.
- To make the KTS-based CAC feature functional, ensure that you do the following:
  - Enable WMM on the WLAN
  - Enable ACM at the radio level
  - Enable processing of TSPEC inactivity timeout at the radio level
- All RLAN clients are disconnected when Call Admission Control (CAC) is enabled or disabled to apply policies.

Key Telephone System-Based CAC

Key Telephone System-based CAC is a protocol that is used in NEC MH240 wireless IP telephones. You can configure the controller to support CAC on KTS-based SIP clients, to process bandwidth request message from such clients, to allocate the required bandwidth on the AP radio, and to handle other messages that are part of the protocol.

When a call is initiated, the KTS-based CAC client sends a Bandwidth Request message to which the controller responds with a Bandwidth Confirm message indicating whether the bandwidth is allocated or not. The call is allowed only if the bandwidth is available. If the client roams from one AP to another, the client sends another Bandwidth Request message to the controller.

Bandwidth allocation depends on the median time calculated using the data rate from the Bandwidth Request message and the packetization interval. For KTS-based CAC clients, the G.711 codec with 20 milliseconds as the packetization interval is used to compute the medium time.

The controller releases the bandwidth after it receives the bandwidth release message from the client. When the client roams to another AP, the controller releases the bandwidth on the previous AP and allocates bandwidth on the new AP, in both intracontroller and intercontroller roaming scenarios. The controller releases the bandwidth if the client is dissociated or if there is inactivity for 120 seconds. The controller does not inform the client when the bandwidth is released for the client due to inactivity or dissociation of the client.

This section contains the following subsections:

Configuring KTS-based CAC (GUI)

Before you begin

To enable KTS-based CAC for a WLAN, ensure that you do the following:

- Set the QoS profile for the WLAN to Platinum.
- Set the WLAN in disabled state.
- Set the FlexConnect Local Switching in disabled state for the WLAN (On the WLANs > Edit page, click the **Advanced** tab and uncheck the **FlexConnect Local Switching** check box).

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure the KTS-based CAC policy.

Step 3 On the **WLANs > Edit** page, click the **Advanced** tab.

Step 4 Under Voice, check or uncheck the **KTS based CAC Policy** check box to enable or disable KTS-based CAC for the WLAN.

Step 5 Save the configuration.

Configuring KTS-based CAC (CLI)

Before you begin

To enable KTS-based CAC for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:

  config wlan qos *wlan-id* **platinum**

- Disable the WLAN by entering the following command:

  config wlan disable *wlan-id*

- Disable FlexConnect Local Switching for the WLAN by entering the following command:

  config wlan flexconnect local-switching *wlan-id* **disable**

Step 1 To enable KTS-based CAC for a WLAN, enter the following command:

config wlan kts-cac enable *wlan-id*

Step 2 To enable the functioning of the KTS-based CAC feature, ensure you do the following:

a) Enable WMM on the WLAN by entering the following command:

config wlan wmm allow *wlan-id*

b) Enable ACM at the radio level by entering the following command:

config 802.11a cac voice acm enable

c) Enable the processing of the TSPEC inactivity timeout at the radio level by entering the following command:

config 802.11a cac voice tspec-inactivity-timeout enable

Related Commands

- To see whether the client supports KTS-based CAC, enter the following command:

  show client detail *client-mac-address*

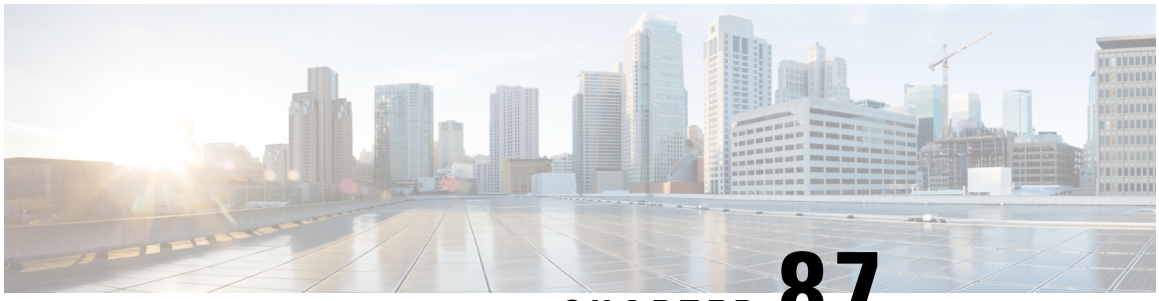
  Information similar to the following appears:

```
Client MAC Address.............................. 00:60:b9:0d:ef:26
Client Username ................................ N/A
AP MAC Address.................................. 58:bc:27:93:79:90

QoS Level....................................... Platinum
802.1P Priority Tag............................. disabled
KTS CAC Capability.............................. Yes
WMM Support..................................... Enabled
Power Save...................................... ON
```

- To troubleshoot issues with KTS-based CAC, enter the following command:

  debug cac kts enable

- To troubleshoot other issues related to CAC, enter the following commands:
  - **debug cac event enable**
  - **debug call-control all enable**



CHAPTER 87

Configuring Reanchoring of Roaming Voice Clients

- Restrictions for Configuring Reanchoring of Roaming Voice Clients, on page 635
- Information About Reanchoring of Roaming Voice Clients, on page 635
- Configuring Reanchoring of Roaming Voice Clients (GUI), on page 636
- Configuring Reanchoring of Roaming Voice Clients (CLI), on page 636

Restrictions for Configuring Reanchoring of Roaming Voice Clients

- The ongoing data session might be affected due to disassociation and then reassociation.
- This feature is supported for TSPEC-based calls and non-TSPEC SIP-based calls only when you enable the admission control.
- This feature is not recommended for use on Cisco 792x phones.

Information About Reanchoring of Roaming Voice Clients

You can allow voice clients to get anchored on the best suited and nearest available controller, which is useful when intercontroller roaming occurs. By using this feature, you can avoid the use of tunnels to carry traffic between the foreign controller and the anchor controller and remove unnecessary traffic from the network.

The ongoing call during roaming is not affected and can continue without any problem. The traffic passes through proper tunnels that are established between the foreign controller and the anchor controller. Disassociation occurs only after the call ends, and then the client then gets reassociated to a new controller.

Note You can reanchor roaming of voice clients for each WLAN.

Configuring Reanchoring of Roaming Voice Clients (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure reanchoring of roaming voice clients.

Step 3 When the WLANs > Edit page appears, choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4 In the Voice area select the **Re-anchor Roamed Clients** check box.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring Reanchoring of Roaming Voice Clients (CLI)

Step 1 Enable or disable reanchoring of roaming voice clients for a particular WLAN by entering this command:

config wlan roamed-voice-client re-anchor {enable | disable} *wlan id*

Step 2 Save your changes by entering this command:

save config

Step 3 See the status of reanchoring roaming voice client on a particular WLAN by entering this command:

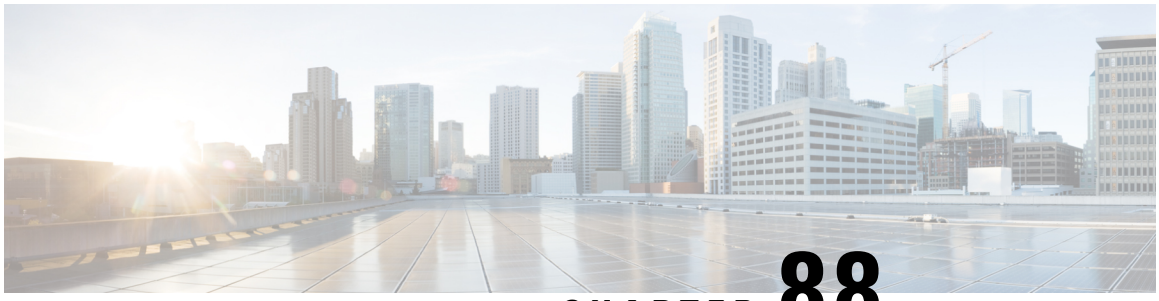
show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wpa2-psk
Network Name (SSID).............................. wpa2-psk
Status........................................... Enabled
...
Call Snooping.................................... Enabled
Roamed Call Re-Anchor Policy..................... Enabled
Band Select...................................... Disabled
Load Balancing................................... Disabled
```

Step 4 Save your changes by entering this command:

save config



CHAPTER 88

Configuring Seamless IPv6 Mobility

- Prerequisites for Configuring IPv6 Mobility, on page 637
- Restrictions on Configuring IPv6 Mobility, on page 637
- IPv6 Client Mobility, on page 638
- Configuring IPv6 Globally, on page 638
- Configuring RA Guard for IPv6 Clients, on page 639
- Configuring RA Throttling for IPv6 Clients, on page 640
- Configuring IPv6 Neighbor Discovery Caching, on page 641

Prerequisites for Configuring IPv6 Mobility

- Up to eight client addresses can be tracked per client.
- To allow stateful DHCPv6 IP addressing to operate properly, you must have a switch or router that supports the DHCP for IPv6 feature that is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

To support the seamless IPv6 Mobility, you might need to configure the following:

- Configuring RA Guard for IPv6 Clients
- Configuring RA Throttling for IPv6 Clients
- Configuring IPv6 Neighbor Discovery Caching

Restrictions on Configuring IPv6 Mobility

- The Dynamic VLAN function for IPv6 is not supported.
- Roaming of IPv6 clients that are associated with a WLAN that is mapped to an untagged interface to another WLAN that is mapped to a tagged interface is not supported.
- The controllers that have the same mobility group, same VLAN ID, and different IPv4 and IPv6 subnets, generate different IPv6 router advertisements. WLAN on these WLCs is assigned to the same dynamic interface with the same VLAN ID on all the controllers. The client receives correct IPv4 address; however it receives a router advertisement from the different subnets that reach the other controllers. There could be issue of no traffic from the client, because the first given IPv6 address to the client does not match to

the subnet for the IPv4 address. To resolve this, make sure if performing Layer 3 roams between controllers that the client is assigned to different VLANs.

- IPv6 is not supported in Flex local switching with AAA override VLAN.
- IPv6 ping from controller to a client is not supported if the client is in the management subnet.
- In Cisco 2504 WLC with directly connected APs, client IPv6 is not supported. (CSCvf51290)
- Controller sends all application IPv6 traffic to the gateway even if the host is in the same subnet. The gateway forwards the traffic to the host in the same subnet. If the gateway is a Cisco ASA, by default, the Cisco ASA drops traffic sent by the controller to the gateway, if traffic has to be sent to the same subnet. This is because traffic ingress and egress interface is the same. To allow Cisco ASA to forward this traffic, use the **same-security-traffic permit intra-interface** command in Cisco ASA. For more information, see https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/vpn/asa-vpn-cli/vpn-params.html#56144.

IPv6 Client Mobility

Internet Protocol version 6 (IPv6) is the next-generation network layer Internet protocol intended to replace version 4 (IPv4) in the TCP/IP suite of protocols. This new version increases the Internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, which provide significantly more addresses than the 32-bit IPv4 addresses.

To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network. The controllers keep track of IPv6 clients by intercepting the ICMPv6 messages to provide seamless mobility and protect the network from network attacks. The ICMPv6 packets are converted from multicast to unicast and delivered individually per client. This process allows more control. Specific clients can receive specific Neighbor Discovery and Router Advertisement packets, which ensures correct IPv6 addressing and avoids unnecessary multicast traffic.

The configuration for IPv6 mobility is the same as IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The controllers must be part of the same mobility group. Both IPv4 and IPv6 client mobility are enabled by default.

Configuring IPv6 Globally

Configuring IPv6 Globally (GUI)

Step 1 Choose **Controller** > **General**.

Step 2 From the Global IPv6 Config drop-down list, choose **Enabled** or **Disabled**.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Configuring IPv6 Globally (CLI)

Procedure

	Command or Action	Purpose
Step 1	Enable or disable IPv6 globally by entering this command:	**config ipv6** {**enable** | **disable**}

Configuring RA Guard for IPv6 Clients

RA Guard

IPv6 clients configure IPv6 addresses and populate their router tables based on IPv6 Router Advertisement (RA) packets. The RA Guard feature is similar to the RA guard feature of wired networks. RA Guard increases the security of the IPv6 network by dropping the unwanted or rogue RA packets that come from wireless clients. If this feature is not configured, malicious IPv6 clients could announce themselves as the router for the network, which would take higher precedence over legitimate IPv6 routers.

RA Guard occurs at the controller. You can configure the controller to drop RA messages at the access point or at the controller. By default, RA Guard is configured at the access point and also enabled in the controller. All IPv6 RA messages are dropped, which protects other wireless clients and upstream wired network from malicious IPv6 clients.

Note

- IPv6 RA guard feature works on wireless clients only. This feature does not work on wired guest access (GA).
- RA guard is also supported in FlexConnect local switching mode.

This section contains the following subsections:

Configuring RA Guard (GUI)

Step 1 Choose **Controller > IPv6 > RA Guard** to open the IPv6 RA Guard page. By default the IPv6 RA Guard on AP is enabled.

Step 2 From the drop-down list, choose **Disable** to disable RA Guard. The controller also displays the clients that have been identified as sending RA packets.

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

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

Configuring RA Guard (CLI)

Procedure

	Command or Action	Purpose
Step 1	Configure RA Guard by entering this command:	**config ipv6 ra-guard ap** {**enable** | **disable**}

Configuring RA Throttling for IPv6 Clients

RA Throttling

RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, then an RA is sent back to the client. This is allowed through the controller and unicasted to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

This section contains the following subsections:

Configuring RA Throttling (GUI)

Step 1 Choose **Controller > IPv6 > RA Throttle Policy** page. By default the IPv6 RA Throttle Policy is disabled. Unselect the check box to disable RA throttle policy.

Step 2 Configure the following parameters:

- **Throttle period**—The period of time for throttling. RA throttling takes place only after the Max Through limit is reached for the VLAN or the Allow At-Most value is reached for a particular router. The range is from 10 seconds to 86400 seconds. The default is 600 seconds.
- **Max Through**—The maximum number of RA packets on a VLAN that can be sent before throttling takes place. The No Limit option allows an unlimited number of RA packets through with no throttling. The range is from 0 to 256 RA packets. The default is 10 RA packets.
- **Interval Option**—This option allows the controller to act differently based on the RFC 3775 value set in IPv6 RA packets.
  - **Passthrough**— Allows any RA messages with the RFC 3775 interval option to go through without throttling.
  - **Ignore**—Causes the RA throttle to treat packets with the interval option as a regular RA and subject to throttling if in effect.
  - **Throttle**—Causes the RA packets with the interval option to always be subject to rate limiting.
- **Allow At-least**—The minimum number of RA packets per router that can be sent as multicast before throttling takes place. The range is from 0 to 32 RA packets.

- **Allow At-most**—The maximum number of RA packets per router that can be sent as multicast before throttling takes place. The No Limit option allows an unlimited number of RA packets through the router. The range is from 0 to 256 RA packets.

  Note When RA throttling occurs, only the first IPv6 capable router is allowed through. For networks that have multiple IPv6 prefixes being served by different routers, you should disable RA throttling.

Step 3 Save the configuration.

Configuring the RA Throttle Policy (CLI)

Configure the RA throttle policy by entering this command:

config ipv6 neigbhor-binding ra-throttle {**allow at-least** *at-least-value* | **enable** | **disable** | **interval-option** { **ignore** | **passthrough** | **throttle**} | **max-through** {**max-through-value** | **no-limit**}}

Configuring IPv6 Neighbor Discovery Caching

IPv6 Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4.

At any given time, only eight IPv6 addresses are supported per client. When the ninth IPv6 address is encountered, the controller removes the oldest stale entry and accommodates the latest one.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery packets that do not comply are dropped. The neighbor binding table in the controller track each IPv6 address and its associated MAC address. Clients are expired from the table according to Neighbor Binding timers.

This section contains the following subsections:

Configuring Neighbor Binding (GUI)

Step 1 Choose **Controller > IPv6 > Neighbor Binding** page.

Step 2 Configure the following:

- Down–Lifetime—Specifies how long IPv6 cache entries are kept if the interface goes down. The range is from 0 to 86400 seconds.
- Reachable–Lifetime—Specifies how long IPv6 addresses are active. The range is from 0 to 86400 seconds.
- Stale–Lifetime—Specifies how long to keep IPv6 addresses in the cache. The range is from 0 to 86400 seconds.

Step 3 Enable or disable the Unknown Address Multicast NS Forwarding.

Step 4 Enable or disable NA Multicast Forwarding.

If you enable NA Multicast Forwarding, all unsolicited multicast NA from Wired/Wireless is not forwarded to Wireless.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring Neighbor Binding (CLI)

Procedure

- Configure the neighbor binding parameters by entering this command:

  config ipv6 neighbor-binding timers {**down-lifetime** | **reachable-lifetime** | **stale-lifetime**} {**enable** | **disable**}

- Configure the Unknown Address Multicast NS Forwarding by entering this command:

  config ipv6 ns-mcast-fwd {**enable** | **disable**}

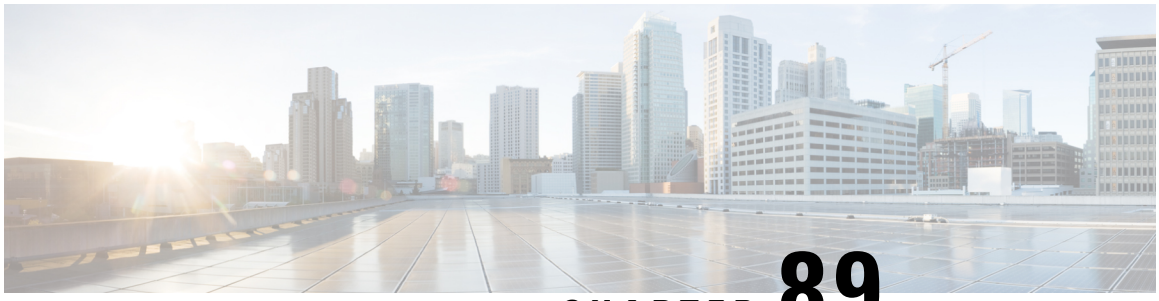
- Configure NA Multicast Forwarding by entering this command:

  config ipv6 na-mcast-fwd {**enable** | **disable**}

  If you enable NA Multicast Forwarding, all unsolicited multicast NA from Wired/Wireless is not forwarded to Wireless.

- See the status of neighbor binding data that are configured on the controller by entering this command:

  show ipv6 neighbor-binding summary



CHAPTER 89

Configuring Cisco Client Extensions

- Prerequisites for Configuring Cisco Client Extensions, on page 643
- Guidelines and Restrictions for Configuring Cisco Client Extensions, on page 643
- Cisco Client Extensions, on page 644
- Configuring CCX Aironet IEs (GUI), on page 644
- Viewing a Client's CCX Version (GUI), on page 644
- Configuring CCX Aironet IEs (CLI), on page 644
- Viewing a Client's CCX Version (CLI), on page 645

Prerequisites for Configuring Cisco Client Extensions

- The software supports CCX versions 1 through 5, which enables controllers 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 controller 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 controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Guidelines and Restrictions for Configuring Cisco Client Extensions

- CCX is not supported on Cisco OEAP 600 access points and all elements related to CCX are not supported.
- Cisco OEAP 600 do not support Cisco Aironet IEs.

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.

For more information about CCX Lite, see
http://www.cisco.com/c/en/us/products/wireless/compatible-extensions.html

This section contains the following subsections:

Configuring CCX Aironet IEs (GUI)

Step 1 Choose **WLANs** to open the **WLANs** page.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** page.

Step 3 Choose the **Advanced** tab to open the **WLANs > Edit (Advanced tab)** page.

Step 4 Select the Aironet IE check box if you want to enable support for Aironet IEs for this WLAN. Otherwise, unselect this check box. The default value is enabled (or selected).

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Viewing a Client's CCX Version (GUI)

A client device sends its CCX version in association request packets to the access point. The controller then stores the client's CCX version in its database and uses it to limit the features for this client. For example, if a client supports CCX version 2, the controller does not allow the client to use CCX version 4 features.

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client device to open the Clients > Detail page.

The CCX Version text box shows the CCX version supported by this client device. *Not Supported* appears if the client does not support CCX.

Step 3 Click **Back** to return to the previous screen.

Step 4 Repeat this procedure to view the CCX version supported by any other client devices.

Configuring CCX Aironet IEs (CLI)

Use this command to configure CCX Aironet IEs:

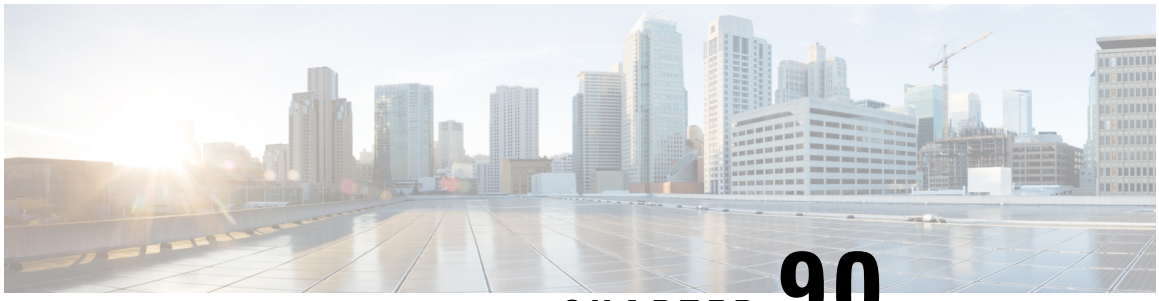
config wlan ccx aironet-ie {**enable** | **disable**} *wlan_id*

The default value is enabled.

Viewing a Client's CCX Version (CLI)

See the CCX version supported by a particular client device using the controller CLI by entering this command:

show client detail *client_mac*



CHAPTER 90

Configuring Remote LANs

- Prerequisites for Configuring Remote LANs, on page 647
- Restrictions for Configuring Remote LANs, on page 647
- Remote LANs, on page 647
- Configuring a Remote LAN (GUI), on page 648
- Configuring a Remote LAN (CLI), on page 649

Prerequisites for Configuring Remote LANs

- You must remove all remote LANs from a controller's configuration before moving to a release that does not support the remote LAN functionality. The remote LAN changes to a WLAN in earlier releases, which could cause an undesirable or unsecured WLAN being broadcast on the wireless network. Remote LAN is only supported in release 7.0.116.0 and later.
- Remote LAN can be applied on a dedicated LAN port on a Cisco Aironet 600 Series OEAP.

Restrictions for Configuring Remote LANs

- Only four clients can connect to a Cisco Aironet 600 Series OEAP through a remote LAN port. This number does not affect the fifteen WLAN limit imposed for the controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.
- It is not possible to configure 802.1X on remote LANs through the controller GUI; configuration only through CLI is supported.

Remote LANs

This section describes how to configure remote LANs.

Prerequisites

- You must remove all remote LANs from a controller's configuration before moving to a release that does not support the remote LAN functionality. The remote LAN changes to a WLAN in earlier releases, which could cause an undesirable or unsecured WLAN being broadcast on the wireless network. Remote LAN is only supported in release 7.0.116.0 and later.
- Remote LAN can be applied on a dedicated LAN port on a Cisco Aironet 600 Series OEAP.

Restrictions

- Only four clients can connect to a Cisco Aironet 600 Series OEAP through a remote LAN port. This number does not affect the fifteen WLAN limit imposed for the controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.
- It is not possible to configure 802.1X on remote LANs through the controller GUI; configuration only through CLI is supported.

This section contains the following subsections:

Configuring a Remote LAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

This page lists all of the WLANs and remote LANs currently configured on the controller. For each WLAN, you can see its WLAN/remote LAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs/Remote LANs appears in the upper right-hand corner of the page. If the list of WLANs/Remote LANs spans multiple pages, you can access these pages by clicking the page number links.

Note If you want to delete a Remote LAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove**, or select the check box to the left of the row, choose **Remove Selected** from the drop-down list, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the remote LAN is removed from any access point group to which it is assigned and from the access point's radio.

Step 2 Create a new Remote-LAN by choosing **Create New** from the drop-down list and clicking **Go**. The WLANs > New page appears.

Step 3 From the Type drop-down list, choose **Remote LAN** to create a remote LAN.

Step 4 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this Remote WLAN. The profile name must be unique.

Step 5 From the WLAN ID drop-down list, choose the ID number for this WLAN.

Step 6 Click **Apply** to commit your changes. The **WLANs > Edit** page appears.

Note You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

Step 7 Use the parameters on the General, Security, and Advanced tabs to configure this remote LAN. See the sections in the rest of this chapter for instructions on configuring specific features.

Step 8 On the General tab, select the **Status** check box to enable this remote LAN. Be sure to leave it unselected until you have finished making configuration changes to the remote LAN.

Note You can also enable or disable remote LANs from the WLANs page by selecting the check boxes to the left of the IDs that you want to enable or disable, choosing **Enable Selected** or **Disable Selected** from the drop-down list, and clicking **Go**.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring a Remote LAN (CLI)

Procedure

- See the current configuration of the remote LAN by entering this command:

  show remote-lan *remote-lan-id*

- Enable or disable remote LAN by entering this command:

  config remote-lan {**enable** | **disable**} *remote-lan-id*

- Enable or disable 802.1X authentication for remote LAN by entering this command:

  config remote-lan security 802.1X {**enable** | **disable**} *remote-lan-id*

Note The encryption on a remote LAN is always “none.”

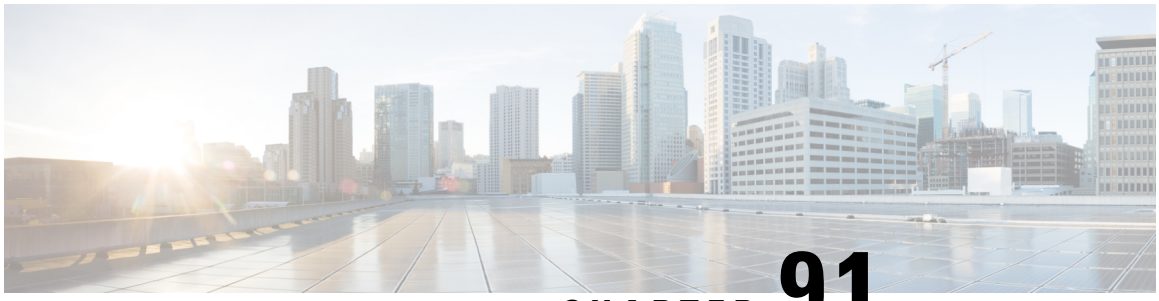
- Enable or disable local EAP with the controller as an authentication server by entering this command:

  config remote-lan local-auth enable *profile-name remote-lan-id*

- If you are using an external AAA authentication server, use the following command:

  config remote-lan radius_server auth {**add** | **delete**} *remote-lan-id server id*

  config remote-lan radius_server auth {**add** | **delete**} *remote-lan-id*



CHAPTER 91

AP Groups

- Access Point Groups, on page 651
- 802.1Q-in-Q VLAN Tagging, on page 656

Access Point Groups

After you create up to 512 WLANs on the controller, 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 controller. 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.

This section contains the following subsections:

Prerequisites for Configuring AP Groups

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

- 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.

AP Groups Supported on Controller Platforms

This table lists the AP groups supported on various controller platforms:

Controller Platform	AP Groups Supported
Cisco 2504 WLC	50
Cisco 5508 WLC	500
Cisco Virtual Wireless Controller	200
Cisco 7510 WLC	6000

Controller Platform	AP Groups Supported
Cisco 8510 WLC	6000
Cisco WiSM2	1000

Restrictions on 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 controller, 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.

- The OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the 600 Series access point to an AP group. The support for two WLANs and one remote LAN still applies to the AP group If the 600 Series OEAP is in the default group, the WLAN/remote LAN ids must be lower than 8.

- All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

  Note A controller with OfficeExtend access points in an access point group publishes up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

- We recommend that you configure all Flex+Bridge APs in a mesh tree (in the same sector) in the same AP group and the same FlexConnect group, to inherit the WLAN-VLAN mappings properly.

- Whenever you add a new WLAN to an AP group, radio reset occurs and if any client is in connected state, the client is deauthenticated and is required to reconnect. We recommend that you add or modify the WLAN configuration of an AP group only during maintenance windows to avoid outages.

- The number of AP groups that you can configure cannot be more than the number of ap-count licenses on controller. For example, if your controller has 5 ap-count licenses, the maximum number of AP groups that you can configure is 5, including the default AP group.

- If you add a WLAN to a custom AP group whose interface mapping is the same as the global WLAN-level interface mapping, interface override does not occur in the AP group for the WLAN.

Later, if you change the interface mapping at a global WLAN level, the change is applied to the AP group level mappings for the WLAN and for all the AP groups to which the WLAN belongs.

Workaround: If you want a different interface mapping for the WLAN at AP group level, you can remove the WLAN from the AP group and add it back with the desired interface.

Configuring Access Point Groups

Step 1 Configure the appropriate dynamic interfaces and map them to the desired VLANs.

For example, to implement the network described in the Information About Access Point Groups section, create dynamic interfaces for VLANs 61, 62, and 63 on the controller. See the Configuring Dynamic Interfaces section for information about how to configure dynamic interfaces.

Step 2 Create the access point groups. See the Creating Access Point Groups section.

Step 3 Create a RF profile. See the Creating an RF Profile section.

Step 4 Assign access points to the appropriate access point groups. See the Creating Access Point Groups section.

Step 5 Apply the RF profile on the AP groups. See the Applying RF Profile to AP Groups section.

Creating Access Point Groups (GUI)

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page.

This page lists all the access point groups currently created on the controller. By default, all access points belong to the default access point group "default-group," unless you assign them to other access point groups.

Note The controller creates a default access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it nor delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the controller with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.

Step 2 Click **Add Group** to create a new access point group. The Add New AP Group section appears at the top of the page.

Step 3 In the **AP Group Name** text box, enter the group's name.

Step 4 In the **Description** text box, enter the group's description.

Step 5 In the **NAS-ID** text box, enter the network access server identifier for the AP group.

Step 6 Click **Add**. The newly created access point group appears in the list of access point groups on the AP Groups page.

Note If you ever want to delete this group, hover your cursor over the blue drop-down arrow for the group and choose **Remove**. An error message appears if you try to delete an access point group that is used by at least one access point. Before deleting an access point group in controller software release 6.0 or later releases, move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases.

Step 7 Click the name of the group to edit this new group. The **AP Groups > Edit (General)** page appears.

Step 8 Change the description of this access point group by entering the new text in the AP Group Description text box and click **Apply**.

Step 9 Choose the **WLANs** tab to open the **AP Groups > Edit (WLANs)** page. This page lists the WLANs that are currently assigned to this access point group.

Step 10 Click **Add New** to assign a WLAN to this access point group. The Add New section appears at the top of the page.

Step 11 From the WLAN SSID drop-down list, choose the SSID of the WLAN.

Step 12 From the **Interface Name** drop-down list, choose the interface to which you want to map the access point group. Choose the quarantine VLAN if you plan to enable network admission control (NAC) out-of-band support.

Note The interface name in the default-group access point group matches the WLAN interface.

Step 13 Select the **SNMP NAC State** check box to enable NAC out-of-band support for this access point group. To disable NAC out-of-band support, leave the check box unselected, which is the default value.

Step 14 Click **Add** to add this WLAN to the access point group. This WLAN appears in the list of WLANs that are assigned to this access point group.

Note If you ever want to remove this WLAN from the access point group, hover your cursor over the blue drop-down arrow for the WLAN and choose **Remove**.

Step 15 Repeat *Step 10* through *Step 14* to add any additional WLANs to this access point group.

Step 16 Choose the **APs** tab to assign access points to this access point group. The AP Groups > Edit (APs) page lists the access points that are currently assigned to this group as well as any access points that are available to be added to the group. If an access point is not currently assigned to a group, its group name appears as “default-group”.

Step 17 Select the check box to the left of the access point name and click **Add APs** to add an access point to this access point group. The access point, after it is reloaded, appears in the list of access points currently in this access point group. The AP has to be reloaded if the AP has to be moved from one group to another.

Note To select all of the available access points at once, select the **AP Name** check box. All of the access points are then selected.

Note If you ever want to remove an access point from the group, select the check box to the left of the access point name and click **Remove APs**. To select all of the access points at once, select the **AP Name** check box. All of the access points are then removed from this group.

Note If you ever want to change the access point group to which an access point belongs, choose **Wireless** > **Access Points** > **All APs** > *ap_name* > **Advanced** tab, choose the name of another access point group from the **AP Group Name** drop-down list, and click **Apply**.

Step 18 In the **802.11u** tab, do the following:

a) Choose a HotSpot group that groups similar HotSpot venues.
b) Choose a venue type that is based on the HotSpot venue group that you choose.
c) To add a new venue, click Add New Venue and enter the language name that is used at the venue and the venue name that is associated with the basic service set (BSS). This name is used in cases where the SSID does not provide enough information about the venue.
d) Select the operating class(es) for the AP group.
e) Click **Apply**.

Step 19 Click **Save Configuration**.

Creating Access Point Groups (CLI)

Step 1 Create an access point group by entering this command:

config wlan apgroup add *group_name*

Note To delete an access point group, enter the **config wlan apgroup delete** *group_name command*. An error message appears if you try to delete an access point group that is used by at least one access point. Before deleting an access point group in controller software release 6.0 or later releases, move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the access points in a group, enter the **show wlan apgroups** command. To move the access points to another group, enter the **config ap group-name** *group_name Cisco_AP* command.

Step 2 Add a description to an access point group by entering this command:

config wlan apgroup description *group_name description*

Step 3 Assign a WLAN to an access point group by entering this command:

config wlan apgroup interface-mapping add *group_name wlan_id interface_name*

Note To remove a WLAN from an access point group, enter the **config wlan apgroup interface-mapping delete** *group_name wlan_id* command.

Step 4 Enable or disable NAC out-of-band support for this access point group by entering this command:

config wlan apgroup nac {**enable** | **disable**}*group_name wlan_id*

Step 5 Configure a WLAN radio policy on the access point group by entering this command:

config wlan apgroup wlan-radio-policy *apgroup_name wlan_id* {**802.11a-only** | **802.11bg** | **802.11g-only** | **all**}

Note With Release 8.0, you can store the WLAN radio policy configuration for an AP group upon a configuration upload or a download.

Step 6 Assign an access point to an access point group by entering this command:

config ap group-name *group_name Cisco_AP*

Note To remove an access point from an access point group, reenter this command and assign the access point to another group.

Step 7 To configure HotSpot for the AP group, enter this command:

config wlan apgroup hotspot {**venue** | **operating-class**}

Step 8 Save your changes by entering this command:

save config

Viewing Access Point Groups (CLI)

To view information about or to troubleshoot access point groups, use these commands:

- See a list of all access point groups on the controller by entering this command:

  show wlan apgroups

- See the BSSIDs for each WLAN assigned to an access point group by entering this command:

  show ap wlan {**802.11a** | **802.11b**} *Cisco_AP*

- See the number of WLANs enabled for an access point group by entering this command:

  show ap config {**802.11a** | **802.11b**} *Cisco_AP*

- Enable or disable debugging of access point groups by entering this command:

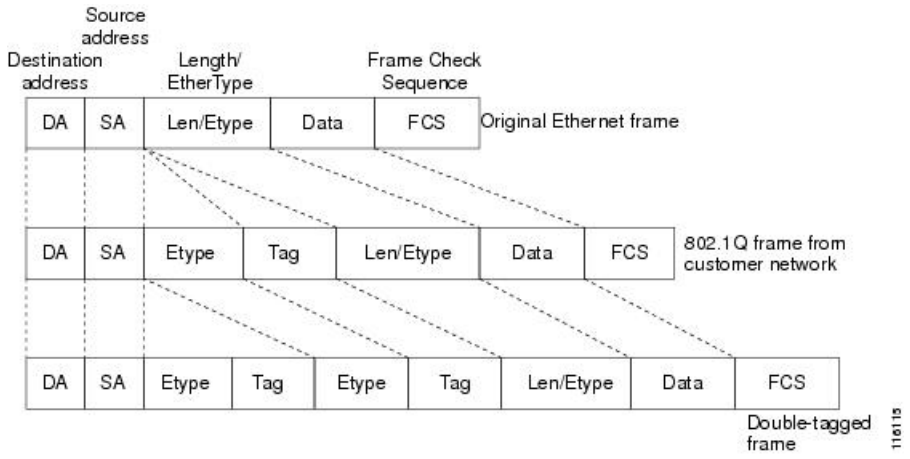
  debug group {**enable** | **disable**}

802.1Q-in-Q VLAN Tagging

Assigning a unique range of VLAN IDs to each client can exceed the limit of 4096 VLANs. The 802.1Q-in-Q VLAN tag feature encapsulates the 802.1Q VLAN tagging within another 802.1Q VLAN tag. The outer tag is assigned according to the AP group, and the inner VLAN ID is assigned dynamically by the AAA server.

Using the 802.1Q-in-Q feature you can use a single VLAN to support multiple VLANs. With the 802.1Q-in-Q feature you can preserve VLAN IDs and segregate traffic of different VLANs. The figure below shows the untagged, 802.1Q-tagged, and 802.1Q-in-Q tagged Ethernet frames.

Figure 42: Untagged 802.1Q-Tagged and 802.1Q-in-Q Tagged Ethernet Frames



This section contains the following subsections:

Restrictions for 802.1Q-in-Q VLAN Tagging

- You cannot enable multicast until you disable IGMP snooping.

- 802.1Q-in-Q VLAN tagging is supported only on Layer 2 and Layer 3 intra-Controller roaming, and Layer 2 inter-Controller roaming. Layer 3 inter-Controller roaming is not supported.
- 0x8100 is the only supported value for the EtherType field of the 802.1Q-in-Q Ethernet frame.
- You can enable 802.1Q-in-Q VLAN tagging only on centrally switched packets.
- You can enable only IPv4 DHCP packets and not IPv6 DHCP packets for 802.1Q-in-Q VLAN tagging.
- The IETF attribute which is a tunnel-type is required to override the C-VLAN.
- C-VLAN can be set with tunnel-private-group-ID /tunnel-type and tunnel-private-group-id.

Configuring 802.1Q-in-Q VLAN Tagging (GUI)

Step 1 Choose **WLANs** > **Advanced > AP Groups** to open the AP Groups page.

Step 2 Click an AP group Name to open the corresponding AP Group > Edit page.

Step 3 Click the **General** tab to configure the 802.1Q-in-Q VLAN tagging details.

Step 4 Select the **Enable Client Traffic QinQ** check box to enable 802.1Q-in-Q VLAN tagging for the AP group.

Step 5 Select the **Enable DHCPv4 QinQ** check box to enable 802.1Q-in-Q VLAN tagging of IPv4 DHCP packets in the AP group.

Step 6 In the **QinQ Service VLAN ID** text box, enter the VLAN ID for 802.1Q-in-Q VLAN tagging.

Step 7 Click **Apply**.

Configuring 802.1Q-in-Q VLAN Tagging (CLI)

Step 1 Enable or disable 802.1Q-in-Q VLAN tagging for an AP group by entering this command:

config wlan apgroup qinq tagging client-traffic *apgroup_name* {**enable** | **disable**}

By default, 802.1Q-in-Q tagging of client traffic for an AP group is disabled.

Step 2 Configure the service VLAN for the AP group by entering this command:

config wlan apgroup qinq service-vlan *apgroup_name vlan_id*

Step 3 Enable or disable IPv4 DHCP packets of the client traffic in the AP group by entering this command::

config wlan apgroup qinq tagging dhcp-v4 *apgroup_name* {**enable** | **disable**}

Note You must enable 802.1Q-in-Q tagging of client traffic before you enable 802.1Q-in-Q tagging of DHCPv4 traffic.

By default, 802.1Q-in-Q tagging of DHCPv4 traffic for an AP group is disabled.

Step 4 Enable or disable 802.1Q-in-Q VLAN tagging for EAP for Global System for Mobile Communications (GSM) Subscriber Identity Module (EAP-SIM) or EAP for Authentication and Key Agreement-authenticated client traffic in the AP group by entering this command:

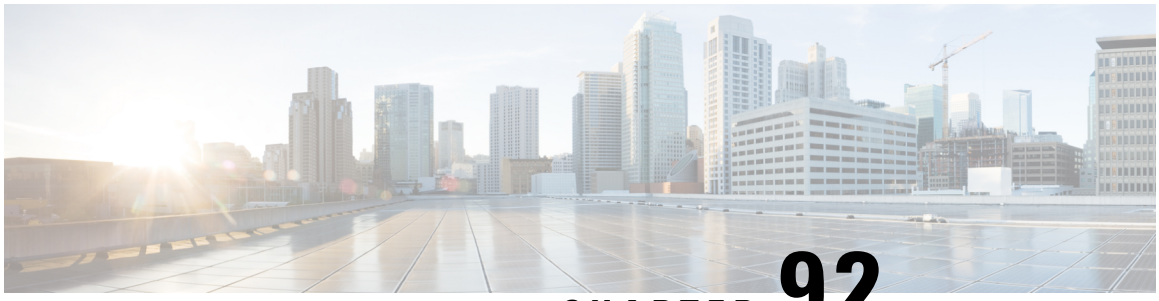
config wlan apgroup qinq tagging eap-sim-aka *apgroup_name* {**enable** | **disable**}

When you enable 802.1Q-in-Q tagging of client traffic, the 802.1Q-in-Q tagging of EAP for Authentication and Key Agreement (EAP-AKA) and EAP-SIM traffic is enabled.

Step 5 Verify if 802.1Q-in-Q VLAN tagging is enabled by entering this command:

show wlan apgroups

```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups..................... 5


Site Name..................................... CT_builing1
Site Description.............................. APs for CT Building1
Venue Group Code.............................. Unspecified
Venue Type Code............................... Unspecified

NAS-identifier................................ CTB1
Client Traffic QinQ Enable.................... TRUE
DHCPv4 QinQ Enable............................ TRUE
AP Operating Class............................ Not-configured
```



CHAPTER 92

Configuring RF Profiles

- Prerequisites for Configuring RF Profiles, on page 659
- Restrictions on Configuring RF Profiles, on page 659
- RF Profiles, on page 660
- Configuring an RF Profile (GUI), on page 662
- Configuring an RF Profile (CLI), on page 663
- Applying an RF Profile to AP Groups (GUI), on page 665
- Applying RF Profiles to AP Groups (CLI), on page 665

Prerequisites for Configuring RF Profiles

Once you create an AP group and apply RF profiles or modify an existing AP group, the new settings are in effect and the following rules become effective:

- The same RF profile must be applied and present on every controller of the AP group or the action will fail for that controller.
- You can assign the same RF profile to more than one AP group.

Restrictions on Configuring RF Profiles

- Once you create an AP group and apply RF profiles or modify an existing AP group, the new settings are in effect and the following rules become effective:
  - AP that has a custom power setting applied for AP power is not in global mode configuration, an RF profile has no effect on this AP. For RF profiling to work, all APs must have their channel and power managed by RRM.
  - Within the AP group, changing the assignment of an RF profile on either band causes the AP to reboot.
  - Once you assign an RF profile to an AP group, you cannot make changes to that RF profile. You must change the AP group RF profile settings to none in order to change the RF profile and then add it back to the AP group. You can also work around this restriction by disabling the network that will be affected by the changes that you will be making either for 802.11a or 802.11b.
  - You cannot delete an AP group that has APs assigned to it.

- You cannot delete an RF profile that is applied to an AP group.

- If you enable Out of Box, save the configuration, and then reboot the Cisco WLC, the status of Out of Box is changed to disabled state. This behavior is observed in Cisco WiSM2, Cisco 5508 WLC, and Cisco 2504 WLC. The workaround is to enable Out of Box again after you reboot the Cisco WLC.

RF Profiles

RF Profiles allows you to tune groups of APs that share a common coverage zone together and selectively change how RRM will operates the APs within that coverage zone.

For example, a university might deploy a high density of APs in an area where a high number of users will congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage.

Using RF profiles and AP groups allows you to optimize the RF settings for AP groups that operate in different environments or coverage zones. RF profiles are created for the 802.11 radios. RF profiles are applied to all APs that belong to an AP group, where all APs in that group will have the same profile settings.

The RF profile gives you the control over the data rates and power (TPC) values.

Note The application of an RF profile does not change the AP's status in RRM. It is still in global configuration mode controlled by RRM.

To address high-density complex RF topologies, the following configurations are available:

- High Density Configurations—The following configurations are available to fine tune RF environments in a dense wireless network:
  - Client limit per WLAN or radio—Maximum number of clients that can communicate with the AP in a high-density environment.
  - Client trap threshold—Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller and Cisco Prime Infrastructure.
- Stadium Vision Configurations—You can configure the following parameter:
  - Multicast data rates—Configurable data rate for multicast traffic based on the RF condition of an AP.
- Out-of-Box AP Configurations—To create an Out-of-Box AP group that consists of newly installed access points that belong to the default AP group. When you enable this feature:
- • Newly installed access points (assigned to the 'default-group' AP group by default) are automatically assigned to the Out-of-Box AP group upon associating with the controller, and their radios are administratively disabled. This eliminates any RF instability caused by the new access points.
  - When Out-of-Box is enabled, default-group APs currently associated with the controller remain in the default group until they reassociate with the controller.

- All default-group APs that subsequently associate with the controller (existing APs on the same controller that have dropped and reassociated, or APs from another controller) are placed in the Out-of-Box AP group.

Note When removing APs from the Out-of-Box AP group for production use, we recommend that you assign the APs to a custom AP group to prevent inadvertently having them revert to the Out-of-Box AP group.

- Special RF profiles are created per 802.11 band. These RF profiles have default settings for all the existing RF parameters and additional new configurations.

Note When you disable this feature after you enable it, only subscription of new APs to the Out of Box AP group stops. All APs that are subscribed to the Out of Box AP Group remain in this AP group. The network administrators can move such APs to the default group or a custom AP group upon network convergence.

- Band Select Configurations— Band Select addresses client distribution between the 2.4-GHz and 5-GHz bands by first understanding the client capabilities to verify whether a client can associate on both 2.4-GHz and 5-GHz spectrum. Enabling band select on a WLAN forces the AP to do probe suppression on the 2.4-GHz band that ultimately moves dual band clients to 5-GHz spectrum. You can configure the following band select parameters per AP Group:
  - Probe response—Probe responses to clients that you can enable or disable.
  - Probe Cycle Count—Probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client.
  - Cycle Threshold—Time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle.
  - Suppression Expire—Expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression.
  - Dual Band Expire—Expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression.
  - Client RSSI—Minimum RSSI for a client to respond to a probe.
- Load Balancing Configurations—Load balancing maintains fair distribution of clients across APs. You can configure the following parameters:
  - Window—Load balancing sets client association limits by enforcing a client window size. For example, if the window size is defined as 3, assuming fair client distribution across the floor area, then an AP should have no more than 3 clients associated with it than the group average.
  - Denial—The denial count sets the maximum number of association denials during load balancing.
- Coverage Hole Mitigation Configurations—You can configure the following parameters:

- Data RSSI—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.
- Voice RSSI—Minimum receive signal strength indication (RSSI) value for voice packets received by the access point.
- Coverage Exception—Percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. If an access point has more number of such clients than the configured coverage level it triggers a coverage hole event.
- Coverage Level—Minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold to trigger a coverage hole exception.

Configuring an RF Profile (GUI)

Step 1 Choose **Wireless** > **RF Profiles** to open the RF profiles page.

Step 2 To configure the out-of-box status for all RF profiles, select or unselect the **Enable Out Of Box** check box.

Step 3 Click **New**.

Step 4 Enter the RF Profile Name and choose the radio band.

Step 5 Click **Apply** to configure the customizations of power and data rate parameters.

Step 6 In the **General** tab, enter the description for the RF profile in the Description text box.

Step 7 In the **802.11** tab, configure the data rates to be applied to the APs of this profile.

Step 8 In the **RRM** tab, do the following:

a) In the TPC area, configure the Maximum and Minimum Power Level Assignment, that is the maximum and minimum power that the APs in this RF profile are allowed to use.

b) In the TPC area, configure a custom TPC power threshold for either Version1 or Version 2 of TPC.

Note Only one version of TPC can be operable for RRM on a given controller Version 1 and Version 2 are not interoperable within the same RF profile. If you select a threshold value for TPCv2 and it is not in the chosen TPC algorithm for the RF profile, this value will be ignored.

c) In the Coverage Hole Detection area, configure the voice and data RSSI.

d) In the Coverage Exception text box, enter the number for clients.

e) In the Coverage Level text box, enter the percentage.

f) In the High-Speed Roam area, select the HSR mode **Enabled** check box to optimize high-speed roaming.

g) In the High-Speed Roam area, enter the neighbor timeout factor.

Step 9 In the **High Density** tab, do the following:

a) In the High Density Parameters area, enter the maximum number of clients to be allowed per AP radio and the client trap threshold value.

b) In the Multicast Parameters area, choose the data rates from the Multicast Data Rates drop-down list.

Step 10 In the **Client Distribution** tab, do the following:

a) In the Load Balancing area, enter the client window size and the denial count.

The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing window + client associations on AP with the lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

The denial count sets the maximum number of association denials during load balancing.

b) In the Band Select area, select or unselect the **Probe Response** check box.

Note The Band Select configurations are available only for the 802.11b/g RF profiles.

c) In the Cycle Count text box, enter a value that sets the number of suppression cycles for a new client. The default count is 2.
d) In the Cycle Threshold text box, enter a time period in milliseconds that determines the time threshold during which new probe requests from a client from a new scanning cycle. The default cycle threshold is 200 milliseconds.
e) In the Suppression Expire text box, enter a time period after which the 802.11 b/g clients become new and are subject to probe response suppression.
f) In the Dual Band Expire text box, enter a time period after which the dual band clients become new and are subject to probe response suppression.
g) In the Client RSSI text box, enter the minimum RSSI for a client to respond to a probe.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Configuring an RF Profile (CLI)

Step 1 To configure the out-of-box status for all RF profiles, enter this command:

config rf-profile out-of-box {**enable** | **disable**}

Step 2 To create or delete an RF profile, enter this command:

config rf-profile {**create** {**802.11a** | **802.11b**} | **delete**} *profile-name*

Step 3 To specify a description for the RF profile, enter this command:

config rf-profile description *text profile-name*

Step 4 To configure the data rates to be applied to the APs of this profile, enter this command:

config rf-profile data-rates {**802.11a** | **802.11b**} {**disabled** | **mandatory** | **supported**} *rate profile-name*

Step 5 To configure the maximum and minimum power level assignment, that is the maximum and minimum power that the APs in this RF profile are allowed to use, enter this command:

config rf-profile {**tx-power-max** | **tx-power-min**} *power-value profile-name*

Step 6 To configure a custom TPC power threshold for either Version1 or Version 2 of TPC, enter this command:

config rf-profile {**tx-power-control-thresh-v1** | **tx-power-control-thresh-v2**} *power-threshold profile-name*

Step 7 To configure the coverage hole detection parameters:

a) To configure the coverage data, enter this command:

config rf-profile coverage data *value-in-dBm profile-name*

b) To configure the minimum client coverage exception level, enter this command:

config rf-profile coverage exception *clients profile-name*

c) To configure the coverage exception level percentage, enter this command:

config rf-profile coverage level *percentage-value profile-name*

d) To configure the coverage of voice, enter this command:

config rf-profile coverage voice *value-in-dBm profile-name*

Step 8 To configure the maximum number of clients to be allowed per AP radio, enter this command:

config rf-profile max-clients *num-of-clients profile-name*

Step 9 To configure the client trap threshold value, enter this command:

config rf-profile client-trap-threshold *threshold-value profile-name*

Step 10 To configure multicast, enter this command:

config rf-profile multicast data-rate *rate profile-name*

Step 11 To configure load balancing, enter this command:

config rf-profile load-balancing {**window** *num-of-clients* | **denial** *value*} *profile-name*

Step 12 To configure band select:

a) To configure the band select cycle count, enter this command:

config rf-profile band-select cycle-count *max-num-of-cycles profile-name*

b) To configure the cycle threshold, enter this command:

config rf-profile band-select cycle-threshold *time-in-milliseconds profile-name*

c) To configure the expiry of the band select, enter this command:

config rf-profile band-select expire {**dual-band** | **suppression**} *time-in-seconds profile-name*

d) To configure the probe response, enter this command:

config rf-profile band-select probe-response {**enable** | **disable**} *profile-name*

e) To configure the minimum RSSI for a client to respond to a probe, enter this command:

config rf-profile band-select client-rssi *value-in-dBm profile-name*

Step 13 Configure the 802.11n only mode for an access point group base by entering this command:

config rf-profile 11n-client-only {**enable** | **disable**} *rf-profile-name*

In the 802.11n only mode, the access point broadcasts support for 802.11n speeds. Only 802.11n clients are allowed to associate with the access point

Applying an RF Profile to AP Groups (GUI)

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page.

Step 2 Click the AP Group Name to open the AP Group > Edit page.

Step 3 Click the **RF Profile** tab to configure the RF profile details. You can choose an RF profile for each band (802.11a/802.11b) or you can choose just one or none to apply to this group.

Note Until you choose the APs and add them to the new group, no configurations are applied. You can save the new configuration as is, but no profiles are applied. Once you choose the APs to move the AP group, the process of moving the APs into the new group reboots the APs and the configurations for the RF profiles are applied to the APs in that AP group.

Step 4 Click the **APs** tab and choose the APs to add to the AP group.

Step 5 Click **Add APs** to add the selected APs to the AP group. A warning message displays that the AP group will reboot the APs will rejoin the controller.

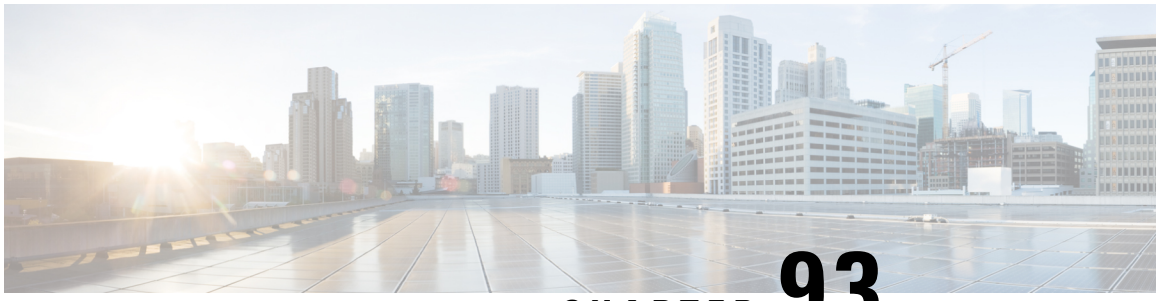
Note APs cannot belong to two AP groups at once.

Step 6 Click **Apply**. The APs are added to the AP Group.

Applying RF Profiles to AP Groups (CLI)

Procedure

	Command or Action	Purpose
Step 1	Apply RF profiles to AP groups by entering this command:	**config wlan apgroup profile-mapping** {**add** | **delete**} *ap-group-name rf-profile-name*



CHAPTER 93

Configuring Web Redirect with 8021.X Authentication

- Web Redirect with 802.1X Authentication, on page 667
- Configuring the RADIUS Server (GUI), on page 668
- Configuring Web Redirect, on page 669
- Disabling Accounting Servers per WLAN (GUI), on page 670
- Disabling Coverage Hole Detection per WLAN, on page 670

Web Redirect with 802.1X Authentication

You can configure a WLAN to redirect a user to a particular web page after 802.1X authentication has completed successfully. You can configure the web redirect to give the user partial or full access to the network.

This section contains the following subsections:

Conditional Web Redirect

If you enable conditional web redirect, the user can be conditionally redirected to a particular web page after 802.1X authentication has completed successfully. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server. Conditions might include the user's password reaching expiration or the user needing to pay his or her bill for continued usage.

If the RADIUS server returns the Cisco AV-pair "url-redirect," then the user is redirected to the specified URL upon opening a browser. If the server also returns the Cisco AV-pair "url-redirect-acl," the specified access control list (ACL) is installed as a preauthentication ACL for this client. The client is not considered fully authorized at this point and can only pass traffic allowed by the preauthentication ACL.

After the client completes a particular operation at the specified URL (for example, changing a password or paying a bill), the client must reauthenticate. When the RADIUS server does not return a "url-redirect," the client is considered fully authorized and allowed to pass traffic.

Note The conditional web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security.

After you configure the RADIUS server, you can then configure the conditional web redirect on the controller using either the controller GUI or CLI.

Splash Page Web Redirect

If you enable splash page web redirect, the user is redirected to a particular web page after 802.1X authentication has completed successfully. After the redirect, the user has full access to the network. You can specify the redirect page on your RADIUS server and the corresponding ACL to allow access to this server in "url-redirect-acl". If the RADIUS server returns the Cisco AV-pair “url-redirect,” then the user is redirected to the specified URL upon opening a browser. The client is considered fully authorized at this point and is allowed to pass traffic, even if the RADIUS server does not return a “url-redirect.”

Note The splash page web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security with 802.1x key management. Preshared key management is not supported with any Layer 2 security method.

Suppose there are backend applications running on the wireless clients and they use HTTP or HTTPS port for their communication. If the applications start communicating before the actual web page is opened, the redirect functionality does not work with web passthrough.

After you configure the RADIUS server, you can then configure the splash page web redirect on the controller using either the controller GUI or CLI.

Configuring the RADIUS Server (GUI)

Note These instructions are specific to the CiscoSecure ACS; however, they should be similar to those for other RADIUS servers.

Step 1 From the CiscoSecure ACS main menu, choose **Group Setup**.

Step 2 Click **Edit Settings**.

Step 3 From the Jump To drop-down list, choose **RADIUS (Cisco IOS/PIX 6.0)**.

Step 4 Select the **[009\001] cisco-av-pair** check box.

Step 5 Enter the following Cisco AV-pairs in the [009\001] cisco-av-pair edit box to specify the URL to which the user is redirected and, if configuring conditional web redirect, the conditions under which the redirect takes place, respectively:

url-redirect=http://url

url-redirect-acl=acl_name

Configuring Web Redirect

Configuring Web Redirect (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page.

Step 4 From the Layer 2 Security drop-down list, choose **802.1X** or **WPA+WPA2**.

Step 5 Set any additional parameters for 802.1X or WPA+WPA2.

Step 6 Choose the **Layer 3** tab to open the WLANs > Edit (Security > Layer 3) page.

Step 7 From the Layer 3 Security drop-down list, choose **None**.

Step 8 Check the **Web Policy** check box.

Step 9 Choose one of the following options to enable conditional or splash page web redirect: **Conditional Web Redirect** or **Splash Page Web Redirect**. The default value is disabled for both parameters.

Step 10 If the user is to be redirected to a site external to the controller, choose the ACL that was configured on your RADIUS server from the Preauthentication ACL drop-down list.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Configuring Web Redirect (CLI)

Step 1 Enable or disable conditional web redirect by entering this command:

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Step 2 Enable or disable splash page web redirect by entering this command:

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Step 3 Save your settings by entering this command:

save config

Step 4 See the status of the web redirect features for a particular WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
```

```
Conditional Web Redirect..................... Disabled
Splash-Page Web Redirect..................... Enabled
...
```

Disabling Accounting Servers per WLAN (GUI)

Note Disabling accounting servers disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to be modified. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page.

Step 4 Unselect the **Enabled** check box for the Accounting Servers.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Disabling Coverage Hole Detection per WLAN

Note Coverage hole detection is enabled globally on the controller.

Note You can disable coverage hole detection on a per-WLAN basis. When you disable coverage hole detection on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.

This section contains the following subsections:

Disabling Coverage Hole Detection on a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the profile name of the WLAN to be modified. The WLANs > Edit page appears.

Step 3 Choose the **Advanced** tab to display the WLANs > Edit (Advanced) page.

Step 4 Uncheck the **Coverage Hole Detection Enabled** check box.

Note OEAP 600 Series Access Points do not support coverage hole detection.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Disabling Coverage Hole Detection on a WLAN (CLI)

Step 1 Disable coverage hole detection on a by entering this command:

config wlan chd *wlan-id* **disable**

Note OEAP 600 Series Access Points do not support coverage hole detection.

Step 2 Save your settings by entering this command:

save config

Step 3 See the coverage hole detection status for a particular WLAN by entering this command:

show wlan *wlan-id*

Information similar to the following appears:

```
WLAN Identifier.................................. 2
Profile Name..................................... wlan2
Network Name (SSID).............................. 2
. . .
CHD per WLAN..................................... Disabled
```

CHAPTER 94

Configuring NAC Out-of-Band Integration

- Prerequisites for NAC Out Of Band, on page 673
- Restrictions for NAC Out of Band, on page 674
- NAC Out-of-Band Integration, on page 674
- Configuring NAC Out-of-Band Integration (GUI), on page 675
- Configuring NAC Out-of-Band Integration (CLI), on page 677

Prerequisites for NAC Out Of Band

- CCA software release 4.5 or later releases is required for NAC out-of-band integration.
- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface that is configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN if they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
- For a posture reassessment that is based on a session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.
- When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. After the session timeout expires for WLANs that use web authentication, clients deauthenticate from the controller and must perform posture validation again.
- All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

Note See the Cisco NAC appliance configuration guides for configuration instructions at http://www.cisco.com/c/en/us/support/security/nac-appliance-clean-access/products-installation-and-configuration-guides-list.html.

- If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.
- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Multiple NAC appliances might need to be deployed.
- If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.
- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Multiple NAC appliances might need to be deployed.
- In controller software releases prior to 5.1, the controller integrates with the NAC appliance only in in-band mode, where the NAC appliance must remain in the data path. For in-band mode, a NAC appliance is required at each authentication location (such as at each branch or for each controller), and all traffic must traverse the NAC enforcement point. In controller software release 5.1 or later releases, the controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.

Restrictions for NAC Out of Band

- NAC out-of-band integration is not supported for use with the WLAN AAA override feature.
- In controller software releases prior to 5.1, the controller integrates with the NAC appliance only in in-band mode, where the NAC appliance must remain in the data path. For in-band mode, a NAC appliance is required at each authentication location (such as at each branch or for each controller), and all traffic must traverse the NAC enforcement point. In controller software release 5.1 or later releases, the controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.

NAC Out-of-Band Integration

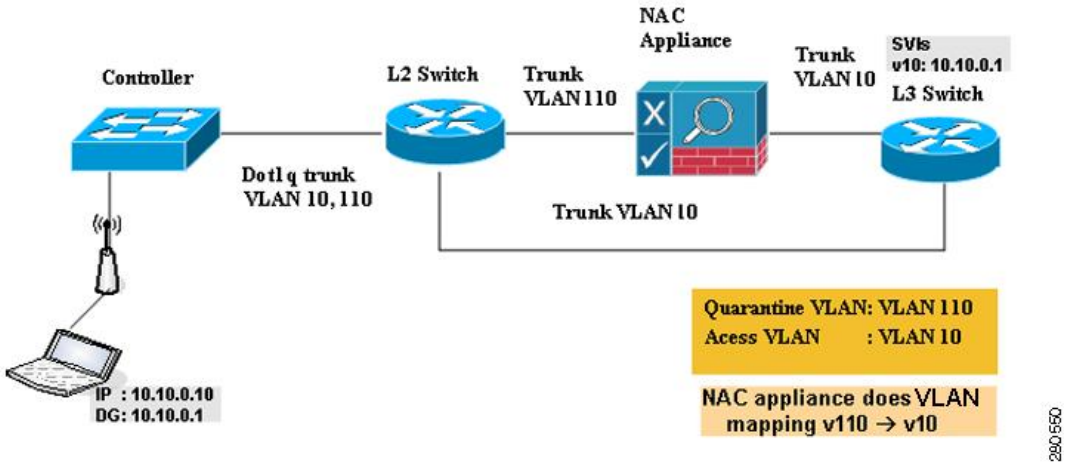
The Cisco NAC Appliance, also known as Cisco Clean Access (CCA), is a network admission control (NAC) product that enables network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. NAC identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network.

The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

To implement the NAC out-of-band feature on the controller, you must enable NAC support on the WLAN or guest LAN and then map this WLAN or guest LAN to an interface that is configured with a quarantine VLAN (untrusted VLAN) and an access VLAN (trusted VLAN). When a client associates and completes Layer 2 authentication, the client obtains an IP address from the access VLAN subnet, but the client state is Quarantine. While deploying the NAC out-of-band feature, be sure that the quarantine VLAN is allowed only between the Layer 2 switch on which the controller is connected and the NAC appliance and that the NAC appliance is configured with a unique quarantine-to-access VLAN mapping. Client traffic passes into the quarantine VLAN, which is trunked to the NAC appliance. After posture validation is completed, the client is prompted to take remedial action. After cleaning is completed, the NAC appliance updates the controller to change the client state from Quarantine to Access.

Figure 43: Example of NAC Out-of-Band Integration

The link between the controller and the switch is configured as a trunk, enabling the quarantine VLAN (110) and the access VLAN (10). On the Layer 2 switch, the quarantine traffic is trunked to the NAC appliance while the access VLAN traffic goes directly to the Layer 3 switch. Traffic that reaches the quarantine VLAN on the NAC appliance is mapped to the access VLAN based on a static mapping configuration.



This section contains the following subsections:

Configuring NAC Out-of-Band Integration (GUI)

Step 1 Configure the quarantine VLAN for a dynamic interface as follows:

a) Choose **Controller** > **Interfaces** to open the Interfaces page.
b) Click **New** to create a new dynamic interface.
c) In the Interface Name text box, enter a name for this interface, such as “quarantine.”
d) In the VLAN ID text box, enter a nonzero value for the access VLAN ID, such as “10.”
e) Click **Apply** to commit your changes. The **Interfaces > Edit** page appears.
f) Select the **Quarantine** check box and enter a nonzero value for the quarantine VLAN ID, such as “110.”

Note We recommend that you configure unique quarantine VLANs throughout your network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in the same subnet, it is mandatory to have the same quarantine VLAN if there is only one NAC appliance in the network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in different subnets, it is mandatory to have different quarantine VLANs if there is only one NAC appliance in the network.

g) Configure any remaining text boxes for this interface, such as the IP address, netmask, and default gateway.
h) Click **Apply** to save your changes.

Step 2 Configure NAC out-of-band support on a WLAN or guest LAN as follows:

a) Choose **WLANs** to open the WLANs page.
b) Click the ID number of the desired WLAN or guest LAN. The WLANs > Edit page appears.
c) Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.
d) Configure NAC out-of-band support for this WLAN or guest LAN by selecting the **NAC State** check box. To disable NAC out-of-band support, leave the check box unselected, which is the default value.
e) Click **Apply** to commit your changes.

Step 3 Configure NAC out-of-band support for a specific access point group as follows:

a) Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page.
b) Click the name of the desired access point group.
c) Choose the **WLANs** tab to open the AP Groups > Edit (WLANs) page.
d) Click **Add New** to assign a WLAN to this access point group. The Add New section appears at the top of the page.
e) From the WLAN SSID drop-down list, choose the SSID of the WLAN.
f) From the Interface Name drop-down list, choose the interface to which you want to map the access point group. Choose the quarantine VLAN if you plan to enable NAC out-of-band support.
g) To enable NAC out-of-band support for this access point group, select the **NAC State** check box. To disable NAC out-of-band support, leave the check box unselected, which is the default value.
h) Click **Add** to add this WLAN to the access point group. This WLAN appears in the list of WLANs assigned to this access point group.

Note If you ever want to remove this WLAN from the access point group, hover your cursor over the blue drop-down arrow for the WLAN and choose **Remove**.

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

Step 5 See the current state of the client (Quarantine or Access) as follows:

a) Choose **Monitor** > **Clients** to open the Clients page.
b) Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears under the Security Information section.

Note The client state appears as “Invalid” if the client is probing, has not yet associated to a WLAN, or cannot complete Layer 2 authentication.

Configuring NAC Out-of-Band Integration (CLI)

Step 1 Configure the quarantine VLAN for a dynamic interface by entering this command:

config interface quarantine vlan *interface_name vlan_id*

Note You must configure a unique quarantine VLAN for each interface on the controller.

To disable the quarantine VLAN on an interface, enter *0* for the VLAN ID.

Step 2 Enable or disable NAC out-of-band support for a WLAN or guest LAN by entering this command:

config {**wlan** | **guest-lan**} **nac** {**enable** | **disable**} {*wlan_id* | *guest_lan_id*}

Step 3 Enable or disable NAC out-of-band support for a specific access point group by entering this command:

config wlan apgroup nac {**enable** | **disable**} *group_name wlan_id*

Step 4 Save your changes by entering this command:

save config

Step 5 See the configuration of a WLAN or guest LAN, including the NAC state by entering this command:

show {**wlan** *wlan_ id* | **guest-lan** *guest_lan_id*}

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wlan
Network Name (SSID).............................. wlan
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control

  NAC-State...................................... Enabled
  Quarantine VLAN............................ 110
...
```

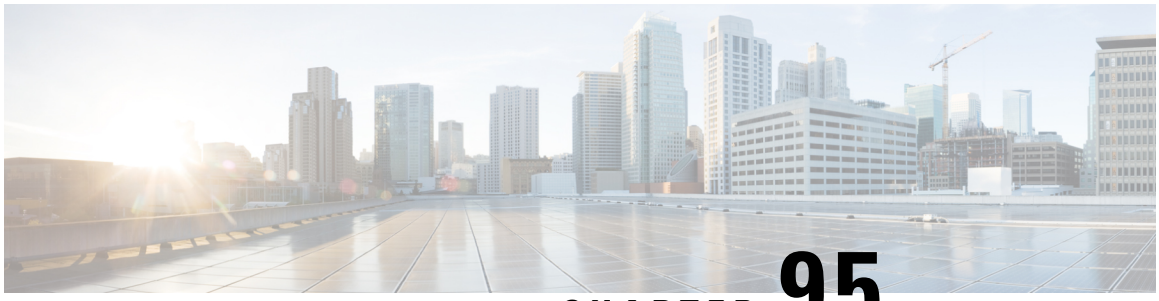
Step 6 See the current state of the client (either Quarantine or Access) by entering this command:

show client detailed *client_mac*

Information similar to the following appears:

```
Client's NAC state.............................. QUARANTINE
```

Note The client state appears as "Invalid" if the client is probing, has not yet associated to a WLAN, or cannot complete Layer 2 authentication.



CHAPTER 95

Configuring Passive Clients

- Restrictions for Passive Clients, on page 679
- Passive Clients, on page 679
- Configuring Passive Clients (GUI), on page 680
- Configuring Passive Clients (CLI), on page 681

Restrictions for Passive Clients

- The interface associated to the WLAN must have a VLAN tagging.
- GARP forwarding must to be enabled using the **show advanced hotspot** command.

Note Client ARP forwarding will not work if any one of the two scenarios, mentioned above, is not configured.

- The passive client feature is not supported with the AP groups and FlexConnect centrally switched WLANs.

Passive Clients

Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.

Wireless LAN controllers currently act as a proxy for ARP requests. Upon receiving an ARP request, the controller responds with an ARP response instead of passing the request directly to the client. This scenario has two advantages:

- The upstream device that sends out the ARP request to the client will not know where the client is located.
- Power for battery-operated devices such as mobile phones and printers is preserved because they do not have to respond to every ARP requests.

Since the wireless controller does not have any IP related information about passive clients, it cannot respond to any ARP requests. The current behavior does not allow the transfer of ARP requests to passive clients. Any application that tries to access a passive client will fail.

The passive client feature enables the ARP requests and responses to be exchanged between wired and wireless clients. This feature when enabled, allows the controller to pass ARP requests from wired to wireless clients until the desired wireless client gets to the RUN state.

Note For FlexConnect APs with locally switched WLANs, passive client feature enables the broadcast of ARP requests and the APs respond on behalf of the client.

This section contains the following subsections:

Configuring Passive Clients (GUI)

Before you begin

To configure passive clients, you must enable multicast-multicast or multicast-unicast mode.

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

Step 2 From **the AP Multicast Mode** drop-down list, choose **Multicast**. The **Multicast Group Address** text box is displayed.

Step 3 In the **Multicast Group Address** text box, enter the IP address of the multicast group.

Step 4 Click **Apply**.

Step 5 Enable global multicast mode as follows:

a) Choose **Controller** > **Multicast**.

b) Check the **Enable Global Multicast Mode** check box.

Enabling the Multicast-Multicast Mode (GUI)

Before you begin

To configure passive clients, you must enable multicast-multicast or multicast-unicast mode.

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

Step 2 Choose one of the following options from the **AP Multicast Mode** drop-down list:

- **Unicast**—Configures the controller to use the unicast method to send multicast packets. This is the default value.
- **Multicast**—Configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.

Step 3 From the **AP Multicast Mode** drop-down list, choose **Multicast**. The **Multicast Group Address** text box is displayed.

Note It is not possible to configure the AP multicast mode for Cisco Flex 7510 WLCs because only unicast is supported.

Step 4 In the **Multicast Group Address** text box, enter the IP address of the multicast group.

Step 5 Click **Apply**.

Step 6 Enable global multicast mode as follows:

a) Choose **Controller** > **Multicast**.

b) Check the **Enable Global Multicast Mode** check box.

Enabling the Global Multicast Mode on Controllers (GUI)

Step 1 Choose **Controller** > **Multicast** to open the Multicast page.

Note The Enable IGMP Snooping text box is highlighted only when you enable the Enable Global Multicast mode. The IGMP Timeout (seconds) text box is highlighted only when you enable the Enable IGMP Snooping text box.

Step 2 Select the **Enable Global Multicast Mode** check box to enable the multicast mode. This step configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.

Note It is not possible to configure Global Multicast Mode for Cisco Flex 7510 WLCs.

Step 3 Select the **Enable IGMP Snooping** check box to enable the IGMP snooping. The default value is disabled.

Step 4 In the IGMP Timeout text box to set the IGMP timeout, enter a value between 30 and 7200 seconds.

Step 5 Click **Apply** to commit your changes.

Enabling the Passive Client Feature on the Controller (GUI)

Step 1 Choose **WLANs** > **WLANs** > **WLAN ID** to open the WLANs > Edit page. By default, the General tab is displayed.

Step 2 Choose the **Advanced** tab.

Step 3 Select the **Passive Client** check box to enable the passive client feature.

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

Configuring Passive Clients (CLI)

Step 1 Enable multicasting on the controller by entering this command:

config network multicast global enable

The default value is disabled.

Step 2 Configure the controller to use multicast to send multicast to an access point by entering this command:

config network multicast mode multicast *multicast_group_IP_address*

Step 3 Configure passive client on a wireless LAN by entering this command:

config wlan passive-client {**enable** | **disable**} *wlan_id*

Step 4 Configure a WLAN by entering this command:

config wlan

Step 5 Save your changes by entering this command:

save config

Step 6 Display the passive client information on a particular WLAN by entering this command:

show wlan *2*

Step 7 Verify if the passive client is associated correctly with the AP and if the passive client has moved into the DHCP required state at the controller by entering this command:

debug client *mac_address*

Step 8 Display the detailed information for a client by entering this command:

show client detail *mac_address*

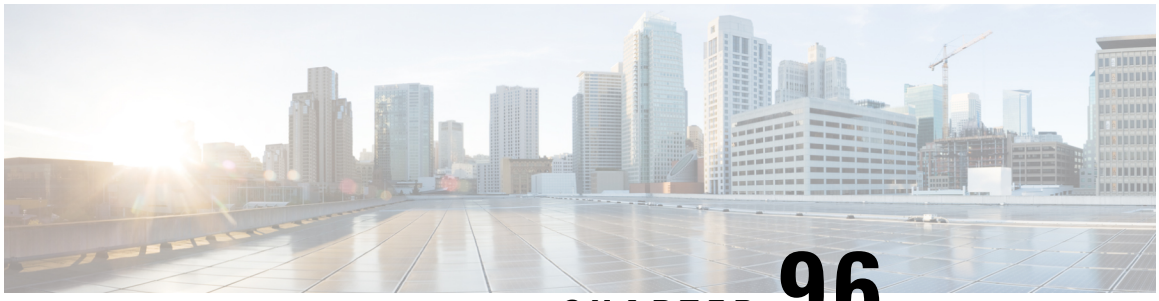
Step 9 Check if the client moves into the run state, when a wired client tries to contact the client by entering this command:

debug client *mac_address*

Step 10 Configure and check if the ARP request is forwarded from the wired side to the wireless side by entering this command:

debug arp all enable

Note Cisco WLC detects duplicate IP addresses based on the ARP table, and not based on the VLAN information. If two clients in different VLANs are using the same IP address, Cisco WLC reports IP conflict and sends GARP. This is not limited to two wired clients, but also for a wired client and a wireless client.



CHAPTER 96

Configuring Client Profiling

- Prerequisites for Configuring Client Profiling, on page 683
- Restrictions for Configuring Client Profiling, on page 684
- Client Profiling, on page 684
- Configuring Client Profiling, on page 685

Prerequisites for Configuring Client Profiling

- By default, client profiling will be disabled on all WLANs.
- Client profiling is supported on access points that are in Local mode and FlexConnect mode.
- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.
- Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.
- The type of DHCP server used does not affect client profiling.
- If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.
- The client is identified based on the MAC address sent in the Accounting request packet.
- Only a MAC address should be sent as calling station ID in accounting packets when profiling is enabled.
- To enable client profiling, you must enable the DHCP required flag and disable the local authentication flag.
- Client profiling uses pre-existing profiles in the controller.
- Profiling for Wireless clients are done based on MAC OUI, DHCP, HTTP User agent.

Note DHCP is required for DHCP profiling and Webauth for HTTP user agent.

Restrictions for Configuring Client Profiling

- Profiling is not supported for clients in the following scenarios:
  - Clients associating with FlexConnect mode APs in Standalone mode.
  - Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
  - Wired clients behind the WGB will not be profiled and policy action will not be done.
- With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.
- While the controller parses the DHCP profiling information every time the client sends a request, the profiling information is sent to ISE only once.
- Custom profiles cannot be created for this release.
- This release contains 88 pre-existing policies where CLI is check only except if you create a policy.
- When local profiling is enabled radius profiling is not allowed on a particular WLAN.
- Only the first policy rule that matches is applied.
- Only 16 policies per WLAN can be configured and globally 16 policies can be allowed.
- Policy action is done only after L2/L3 authentication is complete or when the device sends http traffic and gets the device profiled. Profiling and policing actions will happen more than once per client.
- If AAA override is enabled and if you get any AAA attributes from the AAA server other than role type, configured policy does not apply since the AAA override attributes have a higher precedence.
- For Apple devices, the version and operating system information is displayed only for iPhone 7 and later models and iPads introduced in 2017 and later, provided the WLAN is not open. The version and operating system information is not displayed for older devices.

Client Profiling

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form. Local Client profiling (DHCP and HTTP) is enabled at WLAN level. Clients on the WLANS will be profiled as soon as profling is enabled.

Controller has been enhanced with some of these following capabilities:

- Controller does profiling of devices based on protocols like HTTP, DHCP, etc. to identify the end devices on the network.
- You can configure device-based policies and enforce per user or per device end points, and policies applicable per device.
- Controller displays statistics based on per user or per device end points, and policies applicable per device.

Profiling can be based on:

- Role, defining the user type or the user group to which the user belongs.
- Device type, such as Windows machine, Smart Phone, iPad, iPhone, Android, etc.
- Username/ password pair.
- Location, based on the AP group to which the endpoint is connected
- Time of the day, based on what time of the day the endpoint is allowed on the network.
- EAP type, to check what EAP method the client uses to get connected.

Policing is decided based on a profile which are:

- VLAN
- QoS Level
- ACL
- Session timeout value

This section contains the following subsections:

Configuring Client Profiling

Configuring Client Profiling (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID. The WLANs > Edit page appears.

Step 3 Click the **Advanced** tab.

Step 4 In the RADIUS and Local Client Profiling area, do the following:

a) To profile clients based on DHCP, select the **DHCP Profiling** check box.

b) To profile clients based on HTTP, select the **HTTP Profiling** check box.

You can configure client profiling in both RADIUS mode and Local mode on the WLAN.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring Client Profiling (CLI)

- Enable or disable client profiling for a WLAN based on DHCP by entering this command:

  config wlan profiling radius dhcp {**enable** | **disable**} *wlan-id*

- Enable or disable client profiling in RADIUS mode for a WLAN based on HTTP, DHCP, or both by entering this command:

  config wlan profiling radius {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

  Note Use the **all** parameter to configure client profiling based on both DHCP and HTTP.

- Enable or disable client profiling in Local mode for a WLAN based on HTTP, DHCP, or both by entering this command:

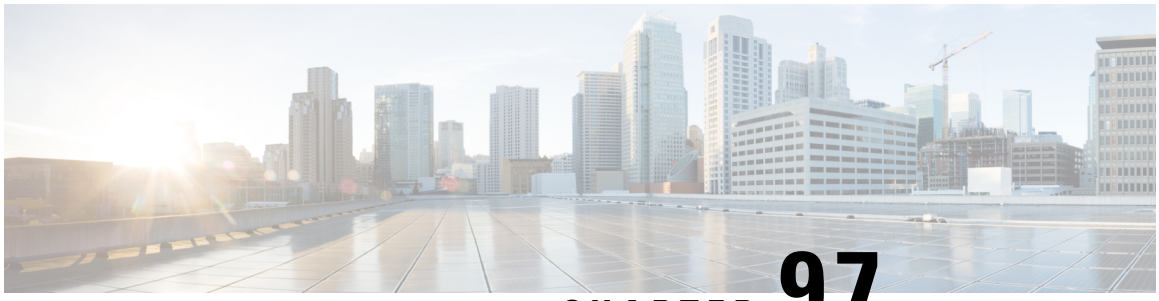
  config wlan profiling local {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

- To see the status of client profiling on a WLAN, enter the following command:

  show wlan *wlan-id*

- To enable or disable debugging of client profiling, enter the following command:

  debug profiling {**enable** | **disable**}



CHAPTER 97

Configuring Per-WLAN RADIUS Source Support

- Prerequisites for Per-WLAN RADIUS Source Support, on page 687
- Per-WLAN RADIUS Source Support, on page 687
- Configuring Per-WLAN RADIUS Source Support (CLI), on page 688
- Monitoring the Status of Per-WLAN RADIUS Source Support (CLI), on page 688

Prerequisites for Per-WLAN RADIUS Source Support

- You must implement appropriate rule filtering on the new identity for the authentication server (RADIUS) because the controller sources traffic only from the selected interface.

Per-WLAN RADIUS Source Support

The controller sources RADIUS traffic from the IP address of its management interface unless the configured RADIUS server exists on a VLAN accessible via one of the controller Dynamic interfaces. If a RADIUS server is reachable via a controller Dynamic interface, RADIUS requests to this specific RADIUS server will be sourced from the controller via the corresponding Dynamic interface.

By default, RADIUS packets sourced from the controller will set the NAS-IP-Address attribute to that of the management interface's IP Address, regardless of the packet's source IP Address (Management or Dynamic, depending on topology).

When you enable per-WLAN RADIUS source support (Radius Server Overwrite interface) the NAS-IP-Address attribute is overwritten by the controller to reflect the sourced interface. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the controller 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.

To filter WLANs, 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.

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.

This section contains the following subsections:

Configuring Per-WLAN RADIUS Source Support (CLI)

Step 1 Enter the **config wlan disable** *wlan-id* command to disable the WLAN.

Step 2 Enter the following command to enable or disable the per-WLAN RADIUS source support:

config wlan radius_server overwrite-interface {**enable** | **disable**} *wlan-id*

Note When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN. When disabled, the controller uses the management interface as the identity in the NAS-IP-Address attribute. If the RADIUS server is on a directly connected dynamic interface, the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used. In all cases, the NAS-IP-Address attribute remains the management interface, unless the feature is enabled.

Step 3 Enable either an AP group's interface or a WLAN's interface for RADIUS packet routing by entering these commands:

- AP group's interface—**config wlan radius_server overwrite-interface apgroup** *wlan-id*
- WLAN's interface—**config wlan radius_server overwrite-interface wlan** *wlan-id*

Note Valid WLAN ID range is between 1 and 16.

Step 4 Enter the **config wlan enable** *wlan-id* command to enable the WLAN.

Note You can filter requests on the RADIUS server side using CiscoSecure ACS. You can filter (accept or reject) a request depending on the NAS-IP-Address attribute through a Network Access Restrictions rule. The filtering to be used is the CLI/DNIS filtering.

Monitoring the Status of Per-WLAN RADIUS Source Support (CLI)

To see if the feature is enabled or disabled, enter the following command:

show wlan *wlan-id*

Example

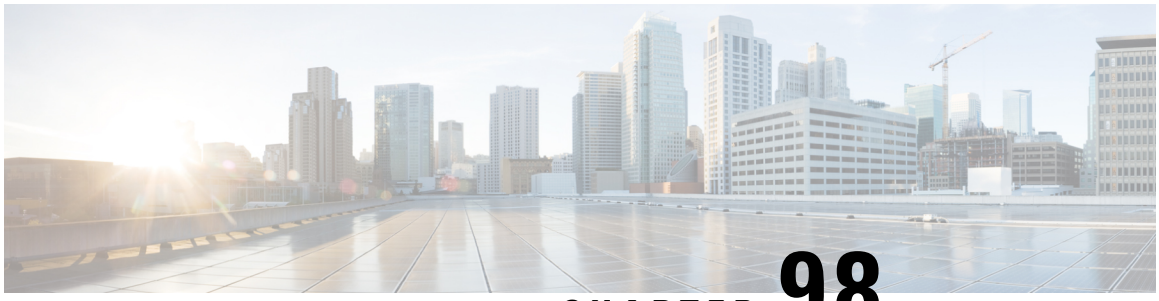
The following example shows that the per-WLAN RADIUS source support is enabled on WLAN 1.

show wlan *1*

Information similar to the following is displayed:

```
WLAN Identifier.................................. 4
Profile Name..................................... example
Network Name (SSID).............................. example
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control
```

```
...
Radius Servers
   Authentication.............................. Global Servers
   Accounting.................................. Global Servers
   Overwrite Sending Interface................. Enabled
Local EAP Authentication........................ Disabled
```



CHAPTER 98

Configuring Mobile Concierge

- Mobile Concierge, on page 691
- Configuring 802.11u Mobility Services Advertisement Protocol, on page 694
- Configuring 802.11u HotSpot, on page 695

Mobile Concierge

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

Configuring Mobile Concierge (802.11u)

Configuring Mobile Concierge (802.11u) (GUI)

Step 1 Choose **WLAN** to open the WLANs page.

Step 2 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the 802.11u parameters and select 802.11u. The 802.11u page appears.

Step 3 Select the **802.11u Status** check box to enable 802.11u on the WLAN.

Step 4 In the 802.11u General Parameters area, do the following:

a) Select the **Internet Access** check box to enable this WLAN to provide Internet services.

b) From the Network Type drop-down list, choose the network type that best describes the 802.11u you want to configure on this WLAN.

c) From the Network Auth Type drop-down list, choose the authentication type that you want to configure for the 802.11u parameters on this network.

d) In the HESSID box, enter the homogenous extended service set identifier (HESSID) value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

e) If the IP address is in the IPv4 format, then from the IPv4 Type drop-down list, choose the IPv4 address type.

f) From the IPv6 Type drop-down list, choose whether you want to make the IPv6 address type available or not.

Step 5 In the OUI List area, do the following:

a) In the OUI text box, enter the Organizationally Unique Identifier, which can be a hexadecimal number represented in 3 or 5 bytes (6 or 10 characters). For example, AABBDF.

b) Select the **Is Beacon** check box to enable the OUI beacon responses.

Note You can have a maximum of 3 OUIs with this field enabled.

c) From the OUI Index drop-down list, choose a value from 1 to 32. The default is 1.

d) Click **Add** to add the OUI entry to the WLAN.

To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 6 In the Domain List area, do the following:

a) In the Domain Name box, enter the domain name that is operating in the WLAN.

b) From the Domain Index drop-down list, choose an index for the domain name from 1 to 32. The default is 1.

c) Click **Add** to add the domain entry to the WLAN.

To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 7 In the Realm List area, do the following:

a) In the Realm text box, enter the realm name that you can assign to the WLAN.

b) From the Realm Index drop-down list, choose an index for the realm from 1 to 32. The default is 1.

c) Click **Add** to add the domain entry to this WLAN.

To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 8 In the Cellular Network Information List area, do the following:

a) In the Country Code text box, enter the 3-character mobile country code.

b) From the CellularIndex drop-down list, choose a value between 1 and 32. The default is 1.

c) In the Network Code text box, enter the character network code. The network code can be 2 or 3 characters.

d) Click **Add** to add the cellular network information to the WLAN.

To remove this entry, hover your mouse pointer over the blue drop-down image and select **Remove**.

Step 9 Click **Apply**.

Configuring Mobile Concierge (802.11u) (CLI)

Procedure

- To enable or disable 802.11u on a WLAN, enter this command:

  config wlan hotspot dot11u {**enable** | **disable**} *wlan-id*

- To add or delete information about a third generation partnership project's cellular network, enter this command:

  config wlan hotspot dot11u 3gpp-info {**add** *index mobile-country-code network-code wlan-id* | **delete** *index wlan-id*}

- To configure the domain name for the entity operating in the 802.11u network, enter this command:

  config wlan hotspot dot11u domain {{{**add** | **modify**} *wlan-id domain-index domain-name*} | {**delete** *wlan-id domain-index*}}

- To configure a homogenous extended service set identifier (HESSID) value for a WLAN, enter this command:

  config wlan hotspot dot11u hessid *hessid wlan-id*

  The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

- To configure the IP address availability type for the IPv4 and IPv6 IP addresses on the WLAN, enter this command:

  config wlan hotspot dot11u ipaddr-type *ipv4-type ipv6-type wlan-id*

- To configure the network authentication type, enter this command:

  config wlan hotspot dot11u auth-type *network-auth wlan-id*

- To configure the Roaming Consortium OI list, enter this command:

  config wlan hotspot dot11u roam-oi {{{**add** | **modify**} *wlan-id oi-index oi is-beacon*} | {**delete** *wlan-id oi-index*}}

- To configure the 802.11u network type and internet access, enter this command:

  config wlan hotspot dot11u network-type *wlan-id network-type internet-access*

- To configure the realm for the WLAN, enter this command:

  config wlan hotspot dot11u nai-realm {{{**add** | **modify**} *realm-name wlan-id realm-index realm-name* | {**delete** *realm-name wlan-id realm-index*}}

- To configure the authentication method for the realm, enter this command:

  config wlan hotspot dot11u nai-realm {**add** | **modify**} **auth-method** *wlan-id realm-index eap-index auth-index auth-method auth-parameter*

- To delete the authentication method for the realm, enter this command:

  config wlan hotspot dot11u nai-realm delete auth-method *wlan-id realm-index eap-index auth-index*

- To configure the extensible authentication protocol (EAP) method for the realm, enter this command:

  config wlan hotpspot dot11u nai-realm {**add** | **modify**} **eap-method** *wlan-id realm-index eap-index eap-method*

- To delete the EAP method for the realm, enter this command:

  config wlan hotspot dot11u nai-realm delete eap-method *wlan-id realm-index eap-index*

Configuring 802.11u Mobility Services Advertisement Protocol

802.11u MSAP

MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers.

Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.

This section contains the following subsections:

Configuring 802.11u MSAP (GUI)

Step 1 Choose **WLAN** to open the WLANs page.

Step 2 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the MSAP parameters and select **Service Advertisements**. The Service Advertisement page appears.

Step 3 Enable the service advertisements.

Step 4 Enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.

Step 5 Click **Apply**.

Configuring MSAP (CLI)

Procedure

- To enable or disable MSAP on a WLAN, enter this command:

  config wlan hotspot msap {**enable** | **disable**} *wlan-id*

- To assign a server ID, enter this command:

  config wlan hotspot msap server-id *server-id wlan-id*

Configuring 802.11u HotSpot

Information About 802.11u HotSpot

This feature, which enables IEEE 802.11 devices to interwork with external networks, is typically found in hotspots or other public networks irrespective of whether the service is subscription based or free.

The interworking service aids network discovery and selection, enabling information transfer from external networks. It provides information to the stations about the networks prior to association. Interworking not only helps users within the home, enterprise, and public access, but also assists manufacturers and operators to provide common components and services for IEEE 802.11 customers. These services are configured on a per WLAN basis on the controller.

Note The Downstream Group-Addressed Forwarding (DGAF) bit in the Hotspot 2.0 IE will not be updated automatically until you disable and enable the WLAN.

Configuring 802.11u HotSpot (GUI)

Step 1 Choose **WLAN** to open the **WLANs** window.

Step 2 Hover your mouse over the blue drop-down arrow that corresponds to the desired WLAN on which you want to configure the HotSpot parameters and choose **HotSpot**. The **WLAN > HotSpot 2.0** page is displayed.

Step 3 On the **WLAN > HotSpot 2.0** window, enable HotSpot2.

Step 4 To set the WAN link parameters, perform the following tasks:

a) From the **WAN Link Status** drop-down list, choose the status. The default is the Not Configured status.
b) From the **WAN Symmetric Link Status** drop-down list, choose the status as either **Different** or **Same**.
c) Enter the **WAN Downlink and Uplink** speeds. The maximum value is 4,294,967,295 kbps.

Step 5 In the **Operator Name List** area, perform the following tasks:

a) In the **Operator Name** text box, enter the name of the 802.11 operator.
b) From the **Operator index** drop-down list, choose an index value between 1 and 32 for the operator.
c) In the **Language Code** field, enter an ISO-14962-1997-encoded string defining the language. This string is a three-character language code.
d) Click **Add** to add the operator details.

The operator details are displayed in a tabular form. To remove an operator, hover your mouse pointer over the blue drop-down arrow and choose **Remove**.

Step 6 In the **Port Config List** area, perform the following tasks:

a) From the **IP Protocol** drop-down list, choose the IP protocol that you want to enable.
b) From the **Port No** drop-down list, choose the port number that is enabled on the WLAN.
c) From the **Status** drop-down list, choose the status of the port.
d) From the **Index** drop-down list, choose an index value for the port configuration.
e) Click **Add** to add the port configuration parameters.

To remove a port configuration list, hover your mouse over the blue drop-down arrow and choose **Remove**.

Step 7 Click **Apply**.

Configuring HotSpot 2.0 (CLI)

Note The character '?' is not supported in the value part of the commands.

Procedure

- To enable or disable HotSpot2 on a WLAN, enter this command:

  config wlan hotspot hs2 {**enable** | **disable**}

- To configure the operator name on a WLAN, enter this command:

  config wlan hotspot hs2 operator-name {**add** | **modify**} *wlan-id index operator-name lang-code*

  The following options are available:

  - *wlan-id*—The WLAN ID on which you want to configure the operator-name.
  - *index*—The operator index of the operator. The range is 1 to 32.
  - *operator-name*—The name of the 802.11an operator.
  - *lang-code*—The language used. An ISO-14962-1997 encoded string defining the language. This string is a three character language code. Enter the first three letters of the language in English (For example: eng for English).

    Tip Press the **tab** key after entering a keyword or argument to get a list of valid values for the command.

- To delete the operator name, enter this command:

  config wlan hotspot hs2 operator-name delete *wlan-id index*

- To configure the port configuration parameters, enter this command:

  config wlan hotspot hs2 port-config {**add** | **modify**} *wlan-id index ip-protocol port-number*

- To delete a port configuration, enter this command:

  config wlan hotspot hs2 port-config delete *wlan-id index*

- To configure the WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics *wlan-id link-status symet-link downlink-speed uplink-speed*

  The values are as follows:

  - *link-status*—The link status. The valid range is 1 to 3.

- *symet-link*—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
- *downlink-speed*—The downlink speed. The maximum value is 4,194,304 kbps.
- *uplink-speed*—The uplink speed. The maximum value is 4,194,304 kbps.

- To clear all HotSpot configurations, enter this command:

  config wlan hotspot clear-all *wlan-id*

- To configure the Access Network Query Protocol (ANQP) 4-way messaging, enter this command:

  config advanced hotspot anqp-4way {**enable** | **disable** | **threshold** *value*}

- To configure the ANQP comeback delay value in terms of TUs, enter this command:

  config advanced hotspot cmbk-delay *value*

- To configure the gratuitous ARP (GARP) forwarding to wireless networks, enter this command:

  config advanced hotspot garp {**enable** | **disable**}

- To limit the number of GAS request action frames to be sent to the controller by an AP in a given interval, enter this command:

  config advanced hotspot gas-limit {**enable** *num-of-GAS-required interval* | **disable**}

Configuring Access Points for HotSpot2 (GUI)

When HotSpot2 is configured, the access points that are part of the network must be configured to support HotSpot2.

Step 1 Click **Wireless > All APs** to open the All APs page.

Step 2 Click the **AP Name** link to configure the HotSpot parameters on the desired access point. The AP Details page appears.

Step 3 Under the General Tab, configure the following parameters:

- **Venue Group**—The venue category that this access point belongs to. The following options are available:
  - **Unspecified**
  - **Assembly**
  - **Business**
  - **Educational**
  - **Factory and Industrial**
  - **Institutional**
  - **Mercantile**
  - **Residential**
  - **Storage**
  - **Utility and Misc**

- **Vehicular**
- **Outdoor**

- **Venue Type**—Depending on the venue category selected above, the venue type drop-down list displays options for the venue type.
- **Venue Name**—Venue name that you can provide to the access point. This name is associated with the BSS. This is used in cases where the SSID does not provide enough information about the venue.
- **Language**—The language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (For example, eng for English).

Step 4 Click **Apply**.

Configuring Access Points for HotSpot2 (CLI)

- **config ap venue add** *venue-name venue-group venue-type lang-code ap-name*–Adds the venue details to the access point indicating support for HotSpot2.

  The values are as follows:

  - *venue-name*—Name of the venue where this access point is located.
  - *venue-group*—Category of the venue. See the following table.
  - *venue-type*—Type of the venue. Depending on the venue-group chosen, select the venue type. See the following table.
  - *lang-code*—The language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (For example: eng for English)
  - *ap-name*—Access point name.

  Tip Press the **tab** key after entering a keyword or argument to get a list of valid values for the command.

- **config ap venue delete** *ap-name*—Deletes the venue related information from the access point.

Table 23: Venue Group Mapping

Venue Group Name	Value	Venue Type for Group
UNSPECIFIED	0	

Venue Group Name	Value	Venue Type for Group
ASSEMBLY	1	• 0—UNSPECIFIED ASSEMBLY • 1—ARENA • 2—STADIUM • 3—PASSENGER TERMINAL (E.G., AIRPORT, BUS, FERRY, TRAIN STATION) • 4—AMPHITHEATER • 5—AMUSEMENT PARK • 6—PLACE OF WORSHIP • 7—CONVENTION CENTER • 8—LIBRARY • 9—MUSEUM • 10—RESTAURANT • 11—THEATER • 12—BAR • 13—COFFEE SHOP • 14—ZOO OR AQUARIUM • 15—EMERGENCY COORDINATION CENTER
BUSINESS	2	• 0—UNSPECIFIED BUSINESS • 1—DOCTOR OR DENTIST OFFICE • 2—BANK • 3—FIRE STATION • 4—POLICE STATION • 6—POST OFFICE • 7—PROFESSIONAL OFFICE • 8—RESEARCH AND DEVELOPMENT FACILITY • 9—ATTORNEY OFFICE
EDUCATIONAL	3	• 0—UNSPECIFIED EDUCATIONAL • 1—SCHOOL, PRIMARY • 2—SCHOOL, SECONDARY • 3—UNIVERSITY OR COLLEGE

Venue Group Name	Value	Venue Type for Group
FACTORY-INDUSTRIAL	4	• 0—UNSPECIFIED FACTORY AND INDUSTRIAL • 1—FACTORY
INSTITUTIONAL	5	• 0—UNSPECIFIED INSTITUTIONAL • 1—HOSPITAL • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.) • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER • 4—GROUP HOME • 5—PRISON OR JAIL
MERCANTILE	6	• 0—UNSPECIFIED MERCANTILE • 1—RETAIL STORE • 2—GROCERY MARKET • 3—AUTOMOTIVE SERVICE STATION • 4—SHOPPING MALL • 5—GAS STATION
RESIDENTIAL	7	• 0—UNSPECIFIED RESIDENTIAL • 1—PRIVATE RESIDENCE • 2—HOTEL OR MOTEL • 3—DORMITORY • 4—BOARDING HOUSE
STORAGE	8	UNSPECIFIED STORAGE
UTILITY-MISC	9	0—UNSPECIFIED UTILITY AND MISCELLANEOUS

Venue Group Name	Value	Venue Type for Group
VEHICULAR	10	• 0—UNSPECIFIED VEHICULAR • 1—AUTOMOBILE OR TRUCK • 2—AIRPLANE • 3—BUS • 4—FERRY • 5—SHIP OR BOAT • 6—TRAIN • 7—MOTOR BIKE
OUTDOOR	11	• 0—UNSPECIFIED OUTDOOR • 1—MUNI-MESH NETWORK • 2—CITY PARK • 3—REST AREA • 4—TRAFFIC CONTROL • 5—BUS STOP • 6—KIOSK

Downloading the Icon File (CLI)

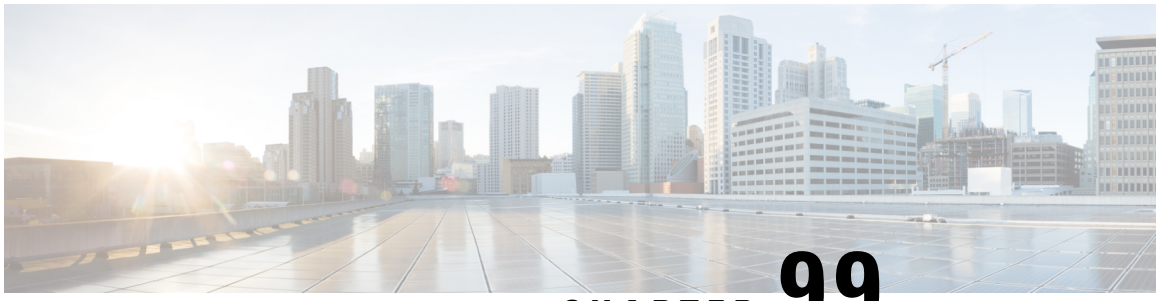
You can configure unique icons of the service providers to be displayed on the client devices. You can download these icon files to the Cisco WLC for the icon files to be sent through a gas message and displayed on the client devices. This feature enhances the user interface on the client devices wherein users can differentiate between service providers based on the icons displayed.

Step 1 Save the icon file on an TFTP, SFTP, or an FTP server.

Step 2 Download the icon file to the Cisco WLC by entering these commands:

a) **transfer download datatype icon**

b) **transfer download start**



CHAPTER 99

Configuring Assisted Roaming

- Restrictions for Assisted Roaming, on page 703
- Assisted Roaming, on page 703
- Configuring Assisted Roaming (CLI), on page 704

Restrictions for Assisted Roaming

- This feature must be implemented only if you are using one controller. The assisted roaming feature is not supported across multiple controllers.
- This feature is supported only on 802.11n capable indoor access points. For a single band configuration, a maximum of 6 neighbors are visible in a neighbor list. For dual band configuration, a maximum of 12 neighbors are visible.
- You can configure assisted roaming only using the controller CLI. Configuration using the controller GUI is not supported.

Assisted Roaming

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning.

The assisted roaming feature is based on an intelligent and client optimized neighbor list.

Unlike the Cisco Client Extension (CCX) neighbor list, the 802.11k neighbor list is generated dynamically on-demand and is not maintained on the controller. The 802.11k neighbor list is based on the location of the clients without requiring the mobility services engine (MSE). Two clients on the same controller but different APs can have different neighbor lists delivered depending on their individual relationship with the surrounding APs.

By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, a switch exists that allows 802.11k to return neighbors in both bands.

Clients send requests for neighbor lists only after associating with the APs that advertize the RRM (Radio Resource Management) capability information element (IE) in the beacon. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

Assembling and Optimizing the Neighbor List

When the controller receives a request for an 802.11k neighbor list, the following occurs:

1. The controller searches the RRM neighbor table for a list of neighbors on the same band as the AP with which the client is currently associated with.
2. The controller checks the neighbors according to the RSSI (Received Signal Strength Indication) between the APs, the current location of the present AP, the floor information of the neighboring AP from Cisco Prime Infrastructure, and roaming history information on the controller to reduce the list of neighbors to six per band. The list is optimized for APs on the same floor.

Assisted Roaming for Non-802.11k Clients

It is also possible to optimize roaming for non-802.11k clients. You can generate a prediction neighbor list for each client without the client requiring to send an 802.11k neighbor list request. When this is enabled on a WLAN, after each successful client association/reassociation, the same neighbor list optimization is applied on the non-802.11k client to generate the neighbor list and store the list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by different neighbors. Because clients usually probe before any association or reassociation, this list is constructed with the most updated probe data and predicts the next AP that the client is likely to roam to.

We discourage clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

Similar to aggressive load balancing, there is a switch to turn on the assisted roaming feature both on a per-WLAN basis and globally. The following options are available:

- Denial count—Maximum number of times a client is refused association.
- Prediction threshold—Minimum number of entries required in the prediction list for the assisted roaming feature to be activated.

Because both load balancing and assisted roaming are designed to influence the AP that a client associates with, it is not possible to enable both the options at the same time on a WLAN.

This section contains the following subsections:

Configuring Assisted Roaming (CLI)

Procedure

- Configure an 802.11k neighbor list for a WLAN by entering this command:

  config wlan assisted-roaming neighbor-list {**enable** | **disable**} *wlan-id*

- Configure neighbor floor label bias by entering this command:

  config assisted-roaming floor-bias *dBm*

- Configure a dual-band 802.11k neighbor list for a WLAN by entering this command:

  config wlan assisted-roaming dual-list {**enable** | **disable**} *wlan-id*

Note Default is the band which the client is using to associate.

- Configure Assisted Roaming Prediction List feature for a WLAN by entering this command:

  config wlan assisted-roaming prediction {**enable** | **disable**} *wlan-id*

Note A warning message is displayed and load balancing is disabled for the WLAN if load balancing is already enabled for the WLAN.

- Configure the minimum number of predicted APs required for the prediction list feature to be activated by entering this command:

  config assisted-roaming prediction-minimum *count*

Note If the number of APs in the prediction assigned to a client is less than the number that you specify, the assisted roaming feature will not apply on this roam.

- Configure the maximum number of times a client can be denied association if the association request that is sent to an AP does not match any AP in the prediction list by entering this command:

  config assisted-roaming denial-maximum *count*

- Debug a client for assisted roaming by entering this command:

  debug mac addr *client-mac-addr*

- Configure debugging of all of 802.11k events by entering this command:

  debug 11k all {**enable** | **disable**}

- Configure debugging of neighbor details by entering this command:

  debug 11k detail {**enable** | **disable**}

- Configure debugging of 802.11k errors by entering this command:

  debug 11k errors {**enable** | **disable**}

- Verify if the neighbor requests are being received by entering this command:

  debug 11k events {**enable** | **disable**}

- Configure debugging of the roaming history of clients by entering this command:

  debug 11k history {**enable** | **disable**}

- Configure debugging of 802.11k optimizations by entering this command:

  debug 11k optimization {**enable** | **disable**}

- Get details of the client-roaming parameters that are to be imported for offline simulation by entering this command:

debug 11k simulation {**enable** | **disable**}

PART VI

Lightweight Access Points

- Using Access Point Communication Protocols, on page 709
- Searching for Access Points, on page 717
- Configuring Global Credentials for Access Points, on page 725
- Configuring Authentication for Access Points, on page 729
- Configuring Embedded Access Points, on page 735
- Converting Autonomous Access Points to Lightweight Mode, on page 737
- Configuring Packet Capture, on page 761
- OfficeExtend Access Points, on page 765
- Using Cisco Workgroup Bridges, on page 785
- Using Non-Cisco Workgroup Bridges, on page 791
- Configuring Backup Controllers, on page 793
- High Availability, on page 799
- Configuring Failover Priority for Access Points, on page 811
- Configuring AP Retransmission Interval and Retry Count, on page 815
- Country Codes, on page 819
- Optimizing RFID Tracking on Access Points, on page 825
- Configuring Probe Request Forwarding, on page 827
- Retrieving the Unique Device Identifier on Controllers and Access Points, on page 829
- Performing a Link Test, on page 831
- Configuring Link Latency, on page 835
- Configuring the TCP MSS, on page 839
- Configuring Power Over Ethernet, on page 841
- Viewing Clients, on page 847
- Configuring LED States for Access Points, on page 849

• Configuring Access Points with Dual-Band Radios, on page 853

CHAPTER 100

Using Access Point Communication Protocols

- CAPWAP, on page 709
- Restrictions for Access Point Communication Protocols, on page 710
- Data Encryption, on page 710
- Viewing CAPWAP Maximum Transmission Unit Information, on page 713
- Debugging CAPWAP, on page 714
- Controller Discovery Process, on page 714
- Verifying that Access Points Join the Controller, on page 716

CAPWAP

Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate with the controller and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is implemented in controller 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 controllers to interoperate with third-party access points in the future

LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

You can deploy CAPWAP controllers and LWAPP controllers on the same network. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP. The only exceptions are that the Cisco Aironet 1040, 1140, 1260, 3500, and 3600 Series Access Points, which support only CAPWAP and join only controllers that run CAPWAP. For example, an 1130 series access point can join a controller running either CAPWAP or LWAPP where an1140 series access point can join only a controller that runs CAPWAP.

The following are some guidelines that you must follow for access point communication protocols:

- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.

- Ensure that the CAPWAP UDP ports 5246 and 5247 (similar to the 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 controller.
- If access control lists (ACLs) are in the control path between the controller and its access points, you need to open new protocol ports to prevent access points from being stranded.

This section contains the following subsections:

Restrictions for Access Point Communication Protocols

- On virtual controller platforms, per-client downstream rate limiting is not supported in FlexConnect central switching.
- Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). We recommend that you always run the controller with the default **config advanced rate enable** command in effect to rate limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, we recommend that you reapply the **config advanced rate enable** command after testing is complete.
- Ensure that the controllers are configured with the correct date and time. If the date and time configured on the controller precedes the creation and installation date of certificates on the access points, the access point fails to join the controller.

Data Encryption

Controllers enable you to encrypt CAPWAP control packets (and optionally, CAPWAP data packets) that are sent between the AP and the controller using Datagram Transport Layer Security (DTLS). DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a controller 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.

Table 24: DTLSv1.2 for CAPWAP Support Information

Release	Support Information
8.2	Not supported
8.3.11x.0 or a later release	Supported in controller and Cisco Wave 2 AP
Any release	Not supported in Cisco Wave 1 AP

The following are supported for web authentication and WebAdmin based on the configuration:

- TLSv1.2.
- TLSv1.0

- SSLv3
- SSLv2

Note Controllers support only static configuration of gateway. Therefore, the ICMP redirect to change IP address of the gateway is not considered.

Restrictions on Data Encryption

- Cisco 1130 and 1240 series access points support DTLS data encryption with software-based encryption.
- The following access points support DTLS data encryption with hardware-based encryption: 1040, 1140, 1250, 1260, 1550, 1600, 1700, 2600, 2700, 3500, 3600, 3700, .
- Cisco Aironet 1552 and 1522 outdoor access points support data DTLS.
- DTLS data encryption is not supported on Cisco Aironet 700, 800, 1530 Series Access Points.
- In Cisco Aironet 18xx Series APs, only software DTLS data encryption is supported with limited throughput performance. Hardware encryption is not supported.
- DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points. Most access points are deployed in a secure network within a company building, so data encryption is not necessary. In contrast, the traffic between an OfficeExtend access point and the controller travels through an unsecure public network, so data encryption is more important for these access points. When data encryption is enabled, traffic is encrypted at the access point before it is sent to the controller and at the controller before it is sent to the client.
- Encryption limits throughput at both the controller and the access point, and maximum throughput is desired for most enterprise networks.
- In a Cisco unified local wireless network environment, do not enable DTLS on the Cisco 1130 and 1240 access points, as it may result in severe throughput degradation and may render the APs unusable.

  See the OfficeExtend Access Points section for more information on OfficeExtend access points.
- You can use the controller to enable or disable DTLS data encryption for a specific access point or for all access points.
- The availability of data DTLS is as follows:
  - The Cisco 5508 WLC will be available with two licenses options: One that allows data DTLS without any license requirements and another image that requires a license to use data DTLS. See the Upgrading or Downgrading DTLS Images for Cisco 5508 WLC section. The images for the DTLS and licensed DTLS images are as follows:

    Licensed DTLS—AS_5500_LDPE_x_x_x_x.aes

    Non licensed DTLS—AS_5500_x_x_x_x.aes
  - Cisco 2504 WLC, Cisco WiSM2, Cisco Virtual Wireless Controllers—By default do not contain DTLS. To turn on data DTLS, you must install a license. These platforms have a single image with data DTLS turned off. To use data DTLS you must have a license.

For Cisco Virtual Wireless Controllers without Data DTLS, the average controller throughput is about 200 Mbps. With all APs using Data DTLS, the average controller throughput is about 100 Mbps.

- If your controller does not have a data DTLS license and if the access point associated with the controller has DTLS enabled, the data path will be unencrypted.
- Non-Russian customers using Cisco 5508 Series Controller do not need data DTLS license. However all customers using Cisco 2504 WLCs, Cisco 8510 WLCS, Cisco WiSM2, and Cisco Virtual Wireless Controllers need a data DTLS license to turn on the Data DTLS feature.

Upgrading or Downgrading DTLS Images for Cisco 5508 WLC

Step 1 The upgrade operation fails on the first attempt with a warning indicating that the upgrade to a licensed DTLS image is irreversible.

Note Do not reboot the controller after Step 1.

Step 2 On a subsequent attempt, the license is applied and the image is successfully updated.

Guidelines When Upgrading to or from a DTLS Image

- You cannot install a regular image (nonlicensed data DTLS) once a licensed data DTLS image is installed.
- You can upgrade from one licensed DTLS image to another licensed DTLS image.
- You can upgrade from a regular image (DTLS) to a licensed DTLS image in a two step process.
- You can use the **show sysinfo** command to verify the LDPE image, before and after the image upgrade.

Configuring Data Encryption (GUI)

Ensure that the base license is installed on the Cisco WLC. Once the license is installed, you can enable data encryption for the access points.

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the **All APs** page.

Step 2 Click the name of the AP for which you want to enable data encryption.

Step 3 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 4 Check the **Data Encryption** check box to enable data encryption for this access point or unselect it to disable this feature. The default value is unselected.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 5 Save the configuration.

Configuring Data Encryption (CLI)

Note In images without a DTLS license, the **config** or **show** commands are not available.

To enable DTLS data encryption for access points on the controller using the controller CLI, follow these steps:

Step 1 Enable or disable data encryption for all access points or a specific access point by entering this command:

config ap link-encryption {**enable** | **disable**} {**all** | *Cisco_AP*}

The default value is disabled.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 2 When prompted to confirm that you want to disconnect the access point(s) and attached client(s), enter **Y**.

Step 3 Enter the **save config** command to save your configuration.

Step 4 See the encryption state of all access points or a specific access point by entering this command:

show ap link-encryption {**all** | *Cisco_AP*}

This command also shows authentication errors, which tracks the number of integrity check failures, and replay errors, which tracks the number of times that the access point receives the same packet.

Step 5 See a summary of all active DTLS connections by entering this command:

show dtls connections

Note If you experience any problems with DTLS data encryption, enter the **debug dtls** {**all** | **event** | **trace** | **packet**} {**enable** | **disable**} command to debug all DTLS messages, events, traces, or packets.

Step 6 Configure the DTLS version by entering this command:

config ap dtls-version {**dtls1.0** | **dtls1.2** | **dtls_all**}

Viewing CAPWAP Maximum Transmission Unit Information

See the maximum transmission unit (MTU) for the CAPWAP path on the controller by entering this command:

show ap config general *Cisco_AP*

The MTU specifies the maximum size of any packet (in bytes) in a transmission.

Information similar to the following appears:

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... Maria-1250
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.......................... 802.11bg:-A    802.11a:-A
Switch Port Number ........................... 1
MAC Address................................... 00:1f:ca:bd:bc:7c
IP Address Configuration...................... DHCP
IP Address.................................... 1.100.163.193
IP NetMask.................................... 255.255.255.0
CAPWAP Path MTU............................... 1485
```

Debugging CAPWAP

Use these commands to obtain CAPWAP debug information:

- **debug capwap events** {**enable** | **disable**}—Enables or disables debugging of CAPWAP events.
- **debug capwap errors** {**enable** | **disable**}—Enables or disables debugging of CAPWAP errors.
- **debug capwap detail** {**enable** | **disable**}—Enables or disables debugging of CAPWAP details.
- **debug capwap info** {**enable** | **disable**}—Enables or disables debugging of CAPWAP information.
- **debug capwap packet** {**enable** | **disable**}—Enables or disables debugging of CAPWAP packets.
- **debug capwap payload** {**enable** | **disable**}—Enables or disables debugging of CAPWAP payloads.
- **debug capwap hexdump** {**enable** | **disable**}—Enables or disables debugging of the CAPWAP hexadecimal dump.
- **debug capwap dtls-keepalive** {**enable** | **disable**}—Enables or disables debugging of CAPWAP DTLS data keepalive packets.

Controller Discovery Process

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

The following are some guidelines for the controller discovery process:

- Upgrade and downgrade paths from LWAPP to CAPWAP or from CAPWAP to LWAPP are supported. An access point with an LWAPP image starts the discovery process in LWAPP. If it finds an LWAPP controller, it starts the LWAPP discovery process to join the controller. If it does not find a LWAPP controller, it starts the discovery in CAPWAP. If the number of times that the discovery process starts with one discovery type (CAPWAP or LWAPP) exceeds the maximum discovery count and the access point does not receive a discovery response, the discovery type changes to the other type. For example, if the access point does not discover the controller in LWAPP, it starts the discovery process in CAPWAP.
- 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 controller.
- To configure the IP addresses that the controller sends in its CAPWAP discovery responses, use the **config network ap-discovery nat-ip-only** {**enable** | **disable**} command.

Note If you disable **nat-ip-only**, the controller sends all active AP-Manager interfaces with their non-NAT IP in discovery response to APs.

If you enable **nat-ip-only**, the controller sends all active AP-Manager interfaces with NAT IP if configured for the interface, else non-NAT IP.

We recommend that you configure the interface as AP-Manager interface with NAT IP or non-NAT IP keeping these scenarios in mind because the AP chooses the least loaded AP-Manager interface received in the discovery response.

- Access points must be discovered by a controller before they can become an active part of the network. The lightweight access points support the following controller discovery processes:
  - Layer 3 CAPWAP or LWAPP discovery—This feature can be enabled on different subnets from the access point and uses either IPv4 or IPv6 addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
  - CAPWAP Multicast Discovery—Broadcast does not exist in IPv6 address. Access point sends CAPWAP discovery message to all the controllers multicast address (FF01::18C). The controller receives the IPv6 discovery request from the AP only if it is in the same L2 segment and sends back the IPv6 discovery response.
  - Locally stored controller IPv4 or IPv6 address discovery—If the access point was previously associated to a controller, the IPv4 or IPv6 addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IPv4 or IPv6 addresses on an access point for later deployment is called *priming the access point*.
  - DHCP server discovery using option 43—This feature uses DHCP option 43 to provide controller IPv4 addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.
  - DHCP server discovery using option 52 —This feature uses DHCP option 52 to allow the AP to discover the IPv6 address of the controller to which it connects. As part of the DHCPv6 messages, the DHCP server provides the controllers management with an IPv6 address.
  - DNS discovery—The access point can discover controllers through your domain name server (DNS). You must configure your DNS to return controller IPv4 and IPv6 addresses in response to CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name.

    When an access point receives an IPv4/IPv6 address and DNSv4/DNSv6 information from a DHCPv4/DHCPv6 server, it contacts the DNS to resolve CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, which may include either IPv4 addresses or IPv6 addresses or both the addresses, the access point sends discovery requests to the controllers.

Guidelines and Restrictions on Controller Discovery Process

- During the discovery process, the 1040, 1140, 1260, 3500, and 3600 series access points will only query for Cisco CAPWAP Controllers. It will not query for LWAPP controllers. If you want these access points to query for both LWAPP and CAPWAP controllers then you need to update the DNS.

- Ensure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.
- To avoid downtime restart CAPWAP on AP while configuring Global HA, so that AP goes back and joins the backup primary controller. This starts a discovery with the primary controller in the back ground. If the discovery with primary is successful, it goes back and joins the primary again.

Verifying that Access Points Join the Controller

When replacing a controller, ensure that access points join the new controller.

Verifying that Access Points Join the Controller (GUI)

Step 1 Configure the new controller as a primary controller as follows:
a) Choose **Controller** > **Advanced** > **Master Controller Mode** to open the Master Controller Configuration page.
b) Select the **Master Controller Mode** check box.
c) Click **Apply** to commit your changes.
d) Click **Save Configuration** to save your changes.

Step 2 (Optional) Flush the ARP and MAC address tables within the network infrastructure.

Step 3 Restart the access points.

Step 4 Once all the access points have joined the new controller, configure the controller not to be a primary controller by unselecting the **Master Controller Mode** check box on the Master Controller Configuration page.

Verifying that Access Points Join the Controller (CLI)

Step 1 Configure the new controller as a primary controller by entering this command:
config network master-base enable

Step 2 (Optional) Flush the ARP and MAC address tables within the network infrastructure.

Step 3 Restart the access points.

Step 4 Configure the controller not to be a primary controller after all the access points have joined the new controller by entering this command:
config network master-base disable

CHAPTER 101

Searching for Access Points

- Information About Searching for Access Points, on page 717
- Searching the AP Filter (GUI), on page 717
- Monitoring the Interface Details, on page 719
- Searching for Access Point Radios, on page 722

Information About Searching for Access Points

You can search for specific access points in the list of access points on the All APs page. To do so, you create a filter to display only access points that meet certain criteria (such as MAC address, status, access point mode, and certificate type). This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

Searching the AP Filter (GUI)

Step 1 Choose **Monitor** > **Access Point Summary**> **All APs** > **Details** to open the All APs page.

This page lists all of the access points joined to the controller. For each access point, you can see its name, MAC address, uptime, status, operating mode, certificates, OfficeExtend access point status, and access point submode.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can access these pages by clicking the page number links. Each page shows up to 20 access points.

Step 2 Click **Change Filter** to open the Search AP dialog box.

Step 3 Select one or more of the following check boxes to specify the criteria used when displaying access points:

- **MAC Address**—The MAC address of an access point.

  Note When you enable the MAC Address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC Address filter is disabled automatically.

- **AP Name**—Enter the name of an access point.
- **AP Model**—Enter the model name of an access point.
- **Operating Status**—Select one or more of the following check boxes to specify the operating status of the access points:

- **UP**—The access point is up and running.

  Note When the APs are in downloading state, during which time the APs are nonfunctional due to no configuration on the APs, the WLC GUI shows these AP radios in UP state on the Monitor page.

- **DOWN**—The access point is not operational.
- **REG**—The access point is registered to the controller.
- **DEREG**—The access point is not registered to the controller.
- **DOWNLOAD**—The controller is downloading its software image to the access point.

- **Port Number**—Enter the controller port number to which the access point is connected.
- **Admin Status**—Choose **Enabled** or **Disabled** to specify whether the access points are enabled or disabled on the controller.
- **AP Mode**—Select one or more of the following options to specify the operating mode of the access points:
  - **Local—The default option.**

    Note The 600 OEAP series access point uses only local mode.

    When an access point in local mode connects to a Cisco Flex 7500 Series Controller, it does not serve clients. The access point details are available in the controller. To enable an access point to serve clients or perform monitoring-related tasks when connected to the Cisco Flex 7500 Series Controller, the access point mode must be in FlexConnect or monitor mode. Use the following command to automatically convert access points to a FlexConnect mode or monitor mode on joining the controller:

    config ap autoconvert {**flexconnect** | **monitor** | **disable**}

    All access points that connect to the controller will either be converted to FlexConnect mode or monitor mode depending on the configuration provided.

  - **FlexConnect**—This mode is used for 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3600, and 800 access points.
  - **REAP**—This mode is the remote edge lightweight access point.
  - **Monitor**—This mode is the monitor-only mode.
  - **Rogue Detector**—This mode monitors the rogue APs on wire. It does not transmit or receive frames over the air or contain rogue APs.

    Note Information about rogues that are detected is not shared between controllers. Therefore, we recommend that every controller has its own connected rogue detector AP when rogue detector APs are used.

  - **Sniffer**—The access point starts sniffing the air on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). It includes information on the time stamp, signal strength, packet size, and so on.

    Note The Bridge option is displayed only if the AP is bridge capable.

    Note If the AP mode is set to “Bridge” and the AP is not REAP capable, an error appears.

Note In the access point sniffer, the server to which the data is to be sent should be on the same VLAN as the wireless controller management VLAN otherwise an error will be displayed.

- **Bridge**—This mode sets the AP mode to "Bridge" if you are connecting a Root AP.
- **SE-Connect**—This mode allows you to connect to spectrum expert and it allows the access point to perform spectrum intelligence.

  Note Spectrum intelligence is supported on , 2600 and 3600 series access points. 1260 series access points does not support the spectrum intelligence.

  Note When an access point is configured in SE-Connect mode, the access point reboots and rejoins the controller. Access points that are configured in this mode do not serve the client.

- **Flex+Bridge**— The standalone mode support is applicable when the AP is in this mode.

- **Certificate Type**—Select one or more of the following check boxes to specify the types of certificates installed on the access points:
  - **MIC**—Manufactured-installed certificate
  - **SSC**—Self-signed certificate
  - **LSC**—Local significant certificate

  Note See the Authorizing Access Points section for more information about these certificate types.

- **Primary S/W Version**—Select this check box to enter the primary software version number
- **Backup S/W Version**—Select this check box to enter the secondary software version number.

Step 4 Click **Apply**.

Only the access points that match your search criteria appear on the All APs page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1d:e5:54:0e:e6, AP Name:pmsk-ap, Operational Status: UP, Status: Enabled, and so on).

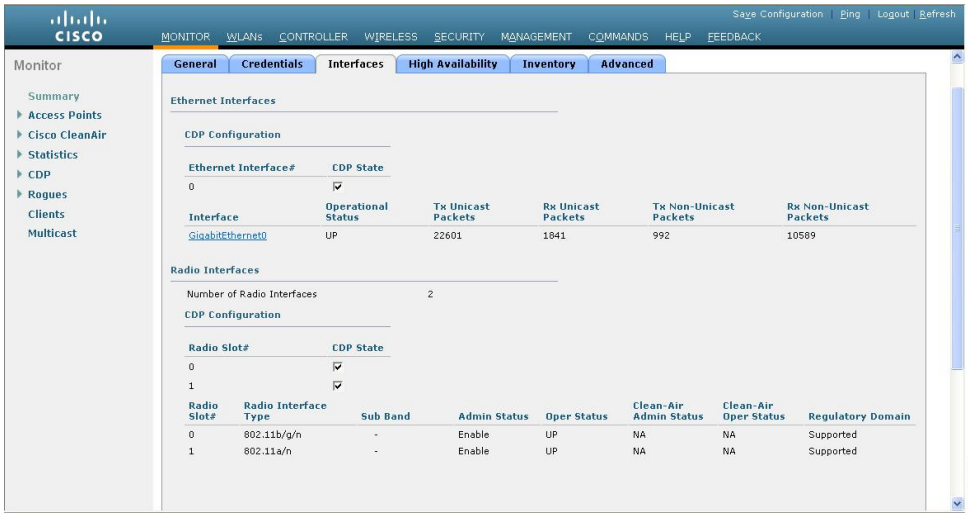
Note If you want to remove the filters and display the entire access point list, click **Clear Filter**.

Monitoring the Interface Details

Step 1 Choose **Monitor** > **Summary** > **All APs**. The All APs > Details page appears.

Step 2 Click the **Interfaces** tab.

Figure 44: Interfaces Tab



Step 3 Click on the available Interface name. The Interface Details page appears.

Step 4 The Interface Details page displays the following parameter details.

Table 25: Interfaces Parameters Details

Button	Description
AP Name	Name of the access point.
Link Speed	Speed of the interference in Mbps.
RX Bytes	Total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Total number of unicast packets received on the interface.
RX Non-Unicast Packets	Total number of nonunicast or multicast packets received on the interface.
Input CRC	Total number of CRC error in packets while receiving on the interface.
Input Errors	Sum of all errors in the packets while receiving on the interface.
Input Overrun	Number of times the receiver hardware was incapable of handling received data to a hardware buffer because the input rate exceeded the receiver's capability to handle that data.
Input Resource	Total number of resource errors in packets received on the interface.
Runts	Number of packets that are discarded because they are similar to the medium's minimum packet size.

Button	Description
Throttle	Total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Total number of packet retransmitted due to an Ethernet collision.
Output Resource	Resource errors in packets transmitted on the interface.
Output Errors	Errors that prevented the final transmission of packets out of the interface.
Operational Status	Operational state of the physical ethernet interface on the AP.
Duplex	Interface's duplex mode.
TX Bytes	Number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Total number of nonunicast or multicast packets transmitted on the interface.
Input Aborts	Total number of packets terminated while receiving on the interface.
Input Frames	Total number of packets received incorrectly that has a CRC error and a noninteger number of octets on the interface.
Input Drops	Total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Total number of packets discarded on the interface due to an unknown protocol.
Giants	Number of packets that are discarded because they exceeded the medium's maximum packet size.
Interface Resets	Number of times that an interface has been completely reset.
Output No Buffer	Total number of packets discarded because there was no buffer space.
Output Underrun	Number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Total number of packets dropped while transmitting from the interface because the queue was full.

Searching for Access Point Radios

Information About Searching for Access Point Radios

You can search for specific access point radios in the list of radios on the 802.11a/n/ac Radios page or the 802.11b/g/n Radios page. You can access these pages from the Monitor tab on the menu bar when viewing access point radios or from the Wireless tab on the menu bar when configuring access point radios. To search for specific access point radios, you create a filter to display only radios that meet certain criteria (such as radio MAC address, access point name, or CleanAir status). This feature is especially useful if your list of access point radios spans multiple pages, which prevents you from viewing them all at once.

Searching for Access Point Radios (GUI)

Step 1 Perform either of the following:

- Choose **Monitor** > **Access Points Summary** > **802.11a/n (or 802.11b/g/n)** > **Radios** > **Details** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.
- Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n** (or **802.11b/g/n**) to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

  These pages show all of the 802.11a/n/ac or 802.11b/g/n access point radios that are joined to the controller and their current settings.

  The total number of access point radios appears in the upper right-hand corner of the page. If the list of radios spans multiple pages, you can access these pages by clicking the page number links. Each page shows up to 25 access point radios.

  Note In a Cisco Unified Wireless Network environment, the 802.11a/n/ac and 802.11b/g/n radios should not be differentiated based on their Base Radio MAC addresses, as they may have the same addresses. Instead, the radios should be differentiated based on their physical addresses.

Step 2 Click **Change Filter** to open the **Search AP** dialog box.

Step 3 Select one of the following check boxes to specify the criteria used when displaying access point radios:

- **MAC Address**—Base radio MAC address of an access point radio.
- **AP Name**—Access point name.

  Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- **CleanAir Status**—Select one or more of the following check boxes to specify the operating status of the access points:
  - **UP**—The spectrum sensor for the access point radio is currently operational.
  - **DOWN**—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled.

- **ERROR**—The spectrum sensor for the access point radio has crashed, making CleanAir monitoring nonoperational for this radio. We recommend rebooting the access point or disabling CleanAir functionality on the radio.
- **N/A**—The access point radio is not capable of supporting CleanAir functionality. Currently, only Cisco Aironet 3500 series access point radios can be configured for Cisco CleanAir.

Step 4 Click **Find** to commit your changes. Only the access point radios that match your search criteria appear on the 802.11a/n/ac Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point radio list, click **Clear Filter**.

CHAPTER 102

Configuring Global Credentials for Access Points

- Global Credentials for Access Points, on page 725
- Restrictions for Global Credentials for Access Points, on page 726
- Configuring Global Credenitals for Access Points, on page 726

Global Credentials 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 on to the nonprivileged mode and enter **show** and **debug** commands, which poses a security threat. The default enable password must be changed to prevent unauthorized users from accessing to the access point's console port and entering configurable commands.

The following are some guidelines to configure global credentials for access points:

- You can set a global username, password, and enable password that all access points that are currently joined to the controller and any that join in the future inherit as they join the controller. 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 controller, the access point enables console port security, and you are prompted for your username and password whenever you log in to the access point’s console port. When you log on, 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 controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.
- You must keep track of the credentials used by the access points. Otherwise, you might not be able to log onto the console port of the access point. If you need to return the access points to the default *Cisco*/*Cisco* username and password, you must clear the controller’s configuration and the access point’s configuration to return them to factory-default settings. To clear the controller’s configuration, choose **Commands** > **Reset to Factory Default** > **Reset** on the controller GUI, or enter the **clear config** command on the controller CLI. To clear the access point’s configuration, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Clear All Config** on the controller GUI, or enter the **clear ap config** *Cisco_AP* command on the controller CLI. To clear the access point's configuration except its static IP address, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Clear Config Except**

Static IP, or enter the **clear ap config** *ap-name* **keep-ip-config** command on the controller CLI. After the access point rejoins a controller, it adopts the default *Cisco*/*Cisco* username and password.

Note If the AP is in Bridge mode, then the same Bridge mode is retained after the factory reset of the AP; if the AP is in FlexConnect, Local, Sniffer, or any other mode, then the AP mode is set to Local mode after the factory reset of the AP. If you press the Reset button on the AP and perform a true factory reset, then the AP moves to a cookie configured mode.

Note Suppose you configure an indoor Cisco AP to go into the mesh mode. If you want to reset the Cisco AP to the local mode, use the **test mesh mode local** command.

- To reset the AP hardware, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Reset AP Now**.

This section contains the following subsections:

Restrictions for Global Credentials for Access Points

- The controller software features are supported on all access points that have been converted to lightweight mode except the 1100 series. VxWorks access points are not supported.
- Telnet is not supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs.
- A global Access Point login credentials once configured in WLC cannot be removed.

Configuring Global Credenitals for Access Points

Configuring Global Credentials for Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 In the **Username** field, enter the username that is to be inherited by all access points that join the controller.

Step 3 In the **Password** field, enter the password that is to be inherited by all access points that join the controller.

You can set a global username, password, and enable password that all access points inherit as they join the controller including access points that are currently joined to the controller and any that join in the future. You can override the global credentials and assign a unique username, password, and enable password for a specific access point. The following are requirements enforced on the 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.
- The AP passwords or secret passwords should not contain the following characters:

  &, <, >, ", and '

Step 4 In the Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller.

Step 5 Click **Apply** to send the global username, password, and enable password to all access points that are currently joined to the controller or that join the controller in the future.

Step 6 Click **Save Configuration** to save your changes.

Step 7 (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to override the global credentials.
c) Choose the **Credentials** tab. The All APs > Details for (Credentials) page appears.
d) Select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.
e) In the Username, Password, and Enable Password text boxes, enter the unique username, password, and enable password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

f) Click **Apply** to commit your changes.
g) Click **Save Configuration** to save your changes.

Note If you want to force this access point to use the controller's global credentials, unselect the **Over-ride Global Credentials** check box.

Configuring Global Credentials for Access Points (CLI)

Step 1 Configure the global username, password, and enable password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password* **all**

Step 2 (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point by entering this command:

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note If you want to force this access point to use the controller's global credentials, enter the **config ap mgmtuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

Step 3 Enter the **save config** command to save your changes.

Step 4 Verify that global credentials are configured for all access points that join the controller by entering this command:

show ap summary

Note If global credentials are not configured, the Global AP User Name text box shows "Not Configured."

To view summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

Step 5 See the global credentials configuration for a specific access point by entering this command:

show ap config general *Cisco_AP*

Note The name of the access point is case sensitive.

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."

CHAPTER 103

Configuring Authentication for Access Points

- AP 802.1X Supplicant, on page 729
- Prerequisites for Configuring Authentication for Access Points, on page 730
- Restrictions for Authenticating Access Points, on page 731
- Configuring Authentication for Access Points (GUI), on page 731
- Configuring Authentication for Access Points (CLI), on page 732
- Configuring the Switch for Authentication, on page 733

AP 802.1X Supplicant

IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network. The device can combine the function of an access point, depending on the fixed configuration or installed modules.

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The switch uses a RADIUS server (Cisco ISE) which uses EAP-FAST with anonymous PAC provisioning to authenticate the supplicant AP device.

You can configure global authentication settings that all access points that are currently associated with the controller and any that associate in the future. You can also override the global authentication settings and assign unique authentication settings for a specific access point.

After the 802.1x authentication is configured on the switch, it allows 802.1x authenticated device traffic only.

There are two modes of authentication models:

- Global authentication—authentication setup for all APs
- AP Level authentication—authentication setup for a particular AP

The switch by default authenticates one device per port. This limitation is not present in the Cisco Catalyst Switches. The host mode type configured on the switch determines the number and type of endpoints allowed on a port. The host mode options are:

- Single host mode-a single IP or MAC address is authenticated on a port. This is set as the default.
- Multi-host mode-authenticates the first MAC address and then allows an unlimited number of other MAC addresses. Enable the host mode on the switch ports if connected AP has been configured with local switching mode. It allows the client's traffic pass the switch port. If you want a secured traffic path, then enable dot1x on the WLAN to protect the client data.

The feature supports AP in local mode, FlexConnect mode, sniffer mode, and monitor mode. It also supports WLAN in central switching and local switching modes.

Note In FlexConnect mode, ensure that the VLAN support is enabled on the AP the correct native VLAN is configured on it.

Table 26: Deployment Options

802.1x on AP	Switch	Result
DISABLED	ENABLED	AP does not join the controller
ENABLED	DISABLED	AP joins the controller. After failing to receive EAP responses, fallbacks to non-dot1x CAPWAP discovery automatically
ENABLED	ENABLED	AP joins the controller, post port-Authentication

In a situation where the credentials on the AP need correction, disable the Switch port Dot1x Authentication, and re-enable the port authentication after updating the credentials.

This section contains the following subsections:

Prerequisites for Configuring Authentication for Access Points

Step 1 If the access point is new, do the following:

a) Boot the access point with the installed recovery image.

b) If you choose not to follow this suggested flow and instead enable 802.1X authentication on the switch port connected to the access point prior to the access point joining the controller, enter this command:

lwapp ap dot1x username *username* **password** *password*

Note If you choose to follow this suggested flow and enable 802.1X authentication on the switch port after the access point has joined the controller and received the configured 802.1X credentials, you do not need to enter this command.

Note This command is available only for access points that are running the applicable recovery image.

Connect the access point to the switch port.

Step 2 Install the required software image on the controller and reboot the controller.

Step 3 Allow all access points to join the controller.

Step 4 Configure authentication on the controller.

Step 5 Configure the switch to allow authentication.

Restrictions for Authenticating Access Points

- The OEAP 600 Series access points do not support LEAP.
- Always disable the Bridge Protocol Data Unit (BPDU) guard on the switch port connected to the AP. Enabling the BPDU guard is allowed only when the switch puts the port in port fast mode.

Configuring Authentication for Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 Under 802.1x Supplicant Credentials, select the **802.1x Authentication** check box.

Step 3 In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 4 In the Password and Confirm Password text boxes, enter the password that is to be inherited by all access points that join the controller.

Note You must enter a strong password in these text boxes. Strong passwords have the following characteristics:

- They are at least eight characters long
- They contain a combination of uppercase and lowercase letters, numbers, and symbols
- They are not a word in any language

Step 5 Click **Apply** to send the global authentication username and password to all access points that are currently joined to the controller and to any that join the controller in the future.

Step 6 Click **Save Configuration** to save your changes.

Step 7 If desired, you can choose to override the global authentication settings and assign a unique username and password to a specific access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to override the authentication settings.
c) Click the **Credentials** tab to open the All APs > Details for (Credentials) page.
d) Under 802.1x Supplicant Credentials, select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global authentication username and password from the controller. The default value is unselected.
e) In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

f) Click **Apply** to commit your changes.
g) Click **Save Configuration** to save your changes.

Note If you want to force this access point to use the controller's global authentication settings, unselect the **Over-ride Global Credentials** check box.

Configuring Authentication for Access Points (CLI)

Step 1 Configure the global authentication username and password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:

config ap 802.1Xuser add username *ap-username* **password** *ap-password* **all**

Note You must enter a strong password for the *ap-password* parameter. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Step 2 (Optional) Override the global authentication settings and assign a unique username and password to a specific access point. To do so, enter this command:

config ap 802.1Xuser add username *ap-username* **password** *ap-password Cisco_AP*

Note You must enter a strong password for the *ap-password* parameter. See the note in Step 1 for the characteristics of strong passwords.

The authentication settings that you enter in this command are retained across controller and access point reboots and whenever the access point joins a new controller.

Note If you want to force this access point to use the controller's global authentication settings, enter the **config ap 802.1Xuser delete** *Cisco_AP* command. The following message appears after you execute this command: "`AP reverted to global username configuration.`"

Step 3 Enter the **save config** command to save your changes.

Step 4 (Optional) Disable 802.1X authentication for all access points or for a specific access point by entering this command:

config ap 802.1Xuser disable {**all** | *Cisco_AP*}

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 5 See the authentication settings for all access points that join the controller by entering this command:

show ap summary

Information similar to the following appears:

```
Number of APs.................................. 1
Global AP User Name............................ globalap
```

```
Global AP Dot1x User Name..................... globalDot1x
```

Step 6 See the authentication settings for a specific access point by entering this command:

show ap config general *Cisco_AP*

Note The name of the access point is case sensitive.

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."

Step 7 See the authentication status on the AP by entering this command:

show authentication interface wired-port status

Configuring the Switch for Authentication

To enable 802.1X authentication on a switch port, on the switch CLI, enter these commands:

- Switch# **configure terminal**
- Switch(config)# **dot1x system-auth-control**
- Switch(config)# **aaa new-model**
- Switch(config)# **aaa authentication dot1x default group radius**
- Switch(config)# **radius-server host** *ip_addr* **auth-port** *port* **acct-port** *port* **key** *key*
- Switch(config)# **interface fastethernet2/1**
- Switch(config-if)# **switchport mode access**
- Switch(config-if)# **dot1x pae authenticator**
- Switch(config-if)# **dot1x port-control auto**
- Switch(config-if)# **end**

CHAPTER 104

Configuring Embedded Access Points

- Embedded Access Points, on page 735

Embedded Access Points

Controller software release 7.0.116.0 or later releases support the embedded access points: AP801 and AP802, which are the integrated access points on the Cisco 880 Series Integrated Services Routers (ISRs). This access points use a Cisco IOS software image that is separate from the router Cisco IOS software image. The access points can operate as autonomous access points configured and managed locally, or they can operate as centrally managed access points that utilize the CAPWAP or LWAPP protocol. The AP801 and AP802 access points are preloaded with both an autonomous Cisco IOS release and a recovery image for the unified mode.

The following are some guidelines for embedded access points:

- Before you use an AP801 or AP802 Series Lightweight Access Point with controller software release 7.0.116.0 or later releases, you must upgrade the software in the Next Generation Cisco 880 Series Integrated Services Routers (ISRs) to Cisco IOS 151-4.M or later.

  Note In Release 7.4, all AP modes except bridging (required for mesh) are supported for both AP801 and AP802. In Release 7.5 and later, all AP modes are supported on AP802; however, bridging is not supported on AP801.

- When you want to use the AP801 or AP802 with a controller, you must enable the recovery image for the unified mode on the access point by entering the **service-module wlan-ap 0 bootimage unified** command on the router in privileged EXEC mode.
- If the **service-module wlan-ap 0 bootimage unified** command does not work, make sure that the software license is still eligible.
- After enabling the recovery image, enter the **service-module wlan-ap 0 reload** command on the router to shut down and reboot the access point. After the access point reboots, it discovers the controller, downloads the full CAPWAP or LWAPP software release from the controller, and acts as a lightweight access point.

Note To use the CLI commands mentioned above, the router must be running Cisco IOS Release 12.4(20)T or later releases.

- To support CAPWAP or LWAPP, the router must be activated with at least the Cisco Advanced IP Services IOS license-grade image. A license is required to upgrade to this Cisco IOS image on the router. For licensing information, see http://www.cisco.com/c/en/us/td/docs/routers/access/sw_activation/SA_on_ISR.html.
- After the AP801 or AP802 boots up with the recovery image for the unified mode, it requires an IP address to communicate with the controller and to download its unified image and configuration from the controller. The router can provide DHCP server functionality, the DHCP pool to reach the controller, and setup option 43 for the controller IP address in the DHCP pool configuration. Use the following configuration to perform this task:

  ip dhcp pool *pool_name*

  network *ip_address subnet_mask*

  dns-server *ip_address*

  default-router *ip_address*

  option 43 hex *controller_ip_address_in_hex*

  Example:

```
ip dhcp pool embedded-ap-pool
 network 60.0.0.0 255.255.255.0
   dns-server 171.70.168.183
   default-router 60.0.0.1
   option 43 hex  f104.0a0a.0a0f   /* single WLC IP address(10.10.10.15) in hex format
  */
```

- The AP801 and AP802 802.11n radio supports lower power levels than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 and AP802 access points store the radio power levels and passes them to the controller when the access point joins the controller. The controller uses the supplied values to limit the user's configuration.
- The AP801 and AP802 access points can be used in FlexConnect mode.

For more information about the AP801, see the documentation for the Cisco 800 Series ISRs at http://www.cisco.com/c/en/us/support/routers/800-series-routers/tsd-products-support-series-home.html.

For more information about the AP802, see the documentation for the Next generation Cisco 880 Series ISRs at http://www.cisco.com/c/dam/en/us/td/docs/routers/access/800/860-880-890/software/configuration/guide/SCG_880_series.pdf.

CHAPTER 105

Converting Autonomous Access Points to Lightweight Mode

- Converting Autonomous Access Points to Lightweight Mode, on page 737
- Restrictions for Converting Autonomous Access Points to Lightweight Mode, on page 738
- Converting Autonomous Access Points to Lightweight Mode, on page 738
- Reverting from Lightweight Mode to Autonomous Mode, on page 739
- Authorizing Access Points, on page 740
- Configuring VLAN Tagging for CAPWAP Frames from Access Points, on page 746
- Using DHCP Option 43 and DHCP Option 60, on page 748
- Troubleshooting the Access Point Join Process, on page 748
- Sending Debug Commands to Access Points Converted to Lightweight Mode, on page 753
- Understanding How Converted Access Points Send Crash Information to the Controller, on page 753
- Understanding How Converted Access Points Send Radio Core Dumps to the Controller, on page 753
- Uploading Memory Core Dumps from Converted Access Points, on page 755
- Viewing the AP Crash Log Information, on page 756
- Displaying MAC Addresses for Converted Access Points, on page 757
- Disabling the Reset Button on Access Points Converted to Lightweight Mode, on page 757
- Configuring a Static IP Address on a Lightweight Access Point, on page 757
- Supporting Oversized Access Point Images, on page 760

Converting Autonomous Access Points to Lightweight Mode

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

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/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_01101010.html

The following are some guidelines for converting autonomous APs to lightweight mode APs:

- All Cisco lightweight access points support 16 BSSIDs per radio and a total of 16 wireless LANs per access point. When a converted access point associates with a controller, wireless LANs with IDs 1

through 16 are pushed to the access point if the AP is part of the default AP group on the controller. You can use other AP group configurations to push other wireless LANs to the new AP.

When a 802.11ac module (the RM3000AC) is added to a 3600 AP, you can have only 8 wireless LANs on the 802.11a/n/ac radio.

- Access points converted to lightweight mode must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- It is not possible to perform archive download while CAPWAP image download is in progress or CAPWAP DTLS is flipping. (CSCvn74377)

This section contains the following subsections:

Restrictions for Converting Autonomous Access Points to Lightweight Mode

- Access points converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN controllers and cannot communicate with WDS devices. However, the controller provides functionality that is equivalent to WDS when the access point associates to it.
- After you convert an access point to lightweight mode, the console port provides read-only access to the unit.

Converting Autonomous Access Points to Lightweight Mode

1. Download the CAPWAP file matching your access point model from Cisco.com. Two types of CAPWAP files are available:
   - Fully functional CAPWAP files, identified by the *k9w8* string in their name. When booting this image, the AP is fully functional and can join a controller to obtain its configuration.
   - Recovery mode CAPWAP files, identified by the *rcvk9w8* string in their name. These files are smaller than the fully functional *k9w8* CAPWAP files. When booting *rcvk9w8* files, the AP can join a controller to download a fully functional image. The AP will then reboot, use the fully functional image and rejoin a controller to obtain its configuration.
2. position the image on an FTP server
3. Configure the AP to connect to the FTP server as a FTP client. This is done under global configuration mode, with the command **ip ftp** *username*, and **ip ftp** *password*. For example:

```
Ap#configure terminal
ap(config)#ip ftp username cisco
ap(config)#ip ftp password Cisco123
ap(config)#exit
```

4. Once the parameters are configured, you can start the download process on the AP. Use the **archive download-sw** command, with the **/force-reload** argument to have the AP reboot at the end of the cycle, and **/overwrite** to replace the autonomous code with the CAPWAP code. See the following example:

```
ap#archive download-sw /force-reload /overwrite
ftp://10.100.1.31/ap3g2-rcvk9w8-tar.152-4.JB6.tar
examining image...
Loading ap3g2-rcvk9w8-tar.152-4.JB6.tar
extracting info (273 bytes)!
Image info:
    Version Suffix: rcvk9w8-
    Image Name: ap3g2-rcvk9w8-mx
    Version Directory: ap3g2-rcvk9w8-mx
    Ios Image Size: 2335232
    Total Image Size: 2335232
    Image Feature: WIRELESS LAN|CAPWAP|RECOVERY
    Image Family: ap3g2
    Wireless Switch Management Version: 3.0.51.0
Extracting files...
ap3g2-rcvk9w8-mx/ (directory) 0 (bytes)
extracting ap3g2-rcvk9w8-mx/ap3g2-rcvk9w8-mx (2327653 bytes)!!!!!!!!!
extracting ap3g2-rcvk9w8-mx/info (273 bytes)
```

The AP reboots into lightweight mode and looks for a controller.

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. If the access point is associated to a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, 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.

Reverting to a Previous Release (CLI)

Step 1 Log on to the CLI on the controller to which the access point is associated.

Step 2 Revert from lightweight mode, by entering this command:

config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*

Step 3 Wait until the access point reboots and reconfigure the access point using the CLI or GUI.

Reverting to a Previous Release 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 *ap3g2-k9w7-tar.152-4.JB4.tar* for a 2700 or 3700 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 **ap3g2-k9w7-tar.default** for a 2700 or a 3700 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 the 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

In controller software releases prior to 5.2, the controller may either use self-signed certificates (SSCs) to authenticate access points or send the authorization information to a RADIUS server (if access points have manufactured-installed certificates [MICs]). In controller software release 5.2 or later releases, you can configure the controller to use a local significant certificate (LSC).

Access points manufactured after July 18, 2005 contain a manufactured-installed certificate (MIC). The controller can use this certificate to authenticate the access points. Alternatively, you can use an authentication list on the controller or an external RADIUS server.

Authorizing Access Points Using SSCs

The Control and Provisioning of Wireless Access Points protocol (CAPWAP) secures the control communication between the access point and controller by a secure key distribution requiring X.509 certificates on both the access point and controller. CAPWAP relies on provisioning of the X.509 certificates. Cisco Aironet access points shipped before July 18, 2005 do not have a MIC, so these access points create an SSC when upgraded to operate in lightweight mode. Controllers are programmed to accept local SSCs for authentication of specific access points and do not forward those authentication requests to a RADIUS server. This behavior is acceptable and secure.

This section contains the following subsections:

Authorizing Access Points for Virtual Controllers Using SSC

Virtual controllers use SSC certificates instead of Manufacturing Installed Certificates (MIC) used by physical controllers. You can configure the controller to allow an AP to validate the SSC of the virtual controller. When an AP validates the SSC, the AP checks if the hash key of the virtual controller matches the hash key stored in its flash. If a match is found, the AP associates with the controller. If a match is not found, the validation fails and the AP disconnects from the controller and restarts the discovery process. By default, hash validation is enabled. An AP must have the virtual controller hash key in its flash before associating with the virtual controller. If you disable hash validation of the SSC, the AP bypasses the hash validation and directly moves to the Run state. APs can associate with a physical controller, download the hash keys and then associate with a virtual controller. If the AP is associated with a physical controller and hash validation is disabled, the AP associates with any virtual controller without hash validation. The hash key of the virtual controller can be configured for a mobility group member. This hash key gets pushed to the APs, so that the APs can validate the hash key of the controller.

Configuring SSC (GUI)

Step 1 Choose **Security** > **Certificate** > **SSC** to open the Self Significant Certificates (SSC) page.

The SSC device certification details are displayed.

Step 2 Select the **Enable SSC Hash Validation** check box to enable the validation of the hash key.

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

Configuring SSC (CLI)

Step 1 To configure hash validation of SSC, enter this command:

config certificate ssc hash validation {**enable** | **disable**}

Step 2 To see the hash key details, enter this command:

show certificate ssc

Authorizing Access Points Using MICs

You can configure controllers to use RADIUS servers to authorize access points using MICs. The controller uses an access point's MAC address as both the username and password when sending the information to a RADIUS server. For example, if the MAC address of the access point is 000b85229a70, both the username and password used by the controller to authorize the access point are 000b85229a70.

Note The lack of a strong password by the use of the access point's MAC address should not be an issue because the controller uses MIC to authenticate the access point prior to authorizing the access point through the RADIUS server. Using MIC provides strong authentication.

Note If you use the MAC address as the username and password for access point authentication on a RADIUS AAA server, do not use the same AAA server for client authentication.

Authorizing Access Points Using LSCs

You can use an LSC if you want your own public key infrastructure (PKI) to provide better security, to have control of your certificate authority (CA), and to define policies, restrictions, and usages on the generated certificates.

The LSC CA certificate is installed on access points and controllers. You need to provision the device certificate on the access point. The access point gets a signed X.509 certificate by sending a certRequest to the controller. The controller acts as a CA proxy and receives the certRequest signed by the CA for the access point.

Guidelines and Restrictions

- Starting in Release 8.3.112.0, device certification is required to enable LSC. Due to this requirement, we recommend that you follow these guidelines:
  - Ensure that APs are provisioned with LSC for them to associate with LSC-enabled controllers.
  - Ensure that there is no mixed environment where some APs use MIC and some use LSC.
  - You do not have to specify the **Number of attempts to LSC** and **AP Ethernet MAC addresses**.

    For more information about this, see CSCve63755.
- When the CA server is in manual mode and if there is an AP entry in the LSC SCEP table that is pending enrollment, the controller waits for the CA server to send a pending response. If there is no response from the CA server, the controller retries a total of three times to get a response, after which the fallback mode comes into effect where the AP provisioning times out and the AP reboots and comes up with MIC.
- LSC on controller does not take password challenge. Therefore, for LSC to work, you must disable password challenge on the CA server.

Configuring Locally Significant Certificates (GUI)

Step 1 Choose **Security** > **Certificate** > **LSC** to open the Local Significant Certificates (LSC) - General page.

Step 2 In the CA Server URL text box, enter the URL to the CA server. You can enter either a domain name or an IP address.

Step 3 In the Params text boxes, enter the parameters for the device certificate. [Optional] The key size is a value from 2048 to 4096 (in bits), and the default value is 2048.

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

Step 5 To add the CA certificate into the controller's certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose **Add**.

Step 6 To add the device certificate into the controller's certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose **Add**.

Step 7 Select the **Enable LSC on Controller** check box to enable the LSC on the system.

Step 8 Click **Apply** to commit your changes.

Step 9 Choose the **AP Provisioning** tab to open the Local Significant Certificates (LSC) - AP Provisioning page.

Step 10 Select the **Enable** check box and click **Update** to provision the LSC on the access point.

Step 11 Click **Apply** to commit your changes.

Step 12 When a message appears indicating that the access points will be rebooted, click **OK**.

Step 13 In the **Number of Attempts to LSC** field, enter the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC). The range is 0 to 255 (inclusive), and the default value is 3.

Note If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

Note If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Step 14 Enter the access point MAC address in the **AP Ethernet MAC Addresses** field and click **Add** to add access points to the provision list.

Note If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

Note To remove an access point from the provision list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning. If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 15 Click **Apply** to commit your changes.

Step 16 Click **Save Configuration** to save your changes.

Configuring Locally Significant Certificates (CLI)

Step 1 Configure the URL to the CA server by entering this command:

config certificate lsc ca-server *http://url:port/path*

where *url* can be either a domain name or IP address.

Note You can configure only one CA server. To configure a different CA server, delete the configured CA server using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

Step 2 Configure the parameters for the device certificate by entering this command:

config certificate lsc subject-params *country state city orgn dept e-mail*

Note The common name (CN) is generated automatically on the access point using the current MIC/SSC format C*xxxx*-*MacAddr*, where *xxxx* is the product number.

Step 3 [Optional] Configure a key size by entering this command:

config certificate lsc other-params *keysize*

The *keysize* is a value from 2048 to 4096 (in bits), and the default value is 2048.

Step 4 Add the LSC CA certificate into the controller's certificate database by entering this command:

config certificate lsc ca-cert {**add** | **delete**}

Step 5 Add the LSC device certificate into the controller's certificate database by entering this command:

config certificate lsc device-cert {**add** | **delete**}

Step 6 Enable LSC on the system by entering this command:

config certificate lsc {**enable** | **disable**}

Step 7 Provision the LSC on the access point by entering this command:

config certificate lsc ap-provision {**enable | disable** }

Step 8 Configure the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC) by entering this command:

config certificate lsc ap-provision revert-cert *retries*

where *retries* is a value from 0 to 255, and the default value is 3.

Note If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

Note If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note If you are configuring LSC for the first time, Cisco recommends that you configure a nonzero value.

Step 9 Add access points to the provision list by entering this command:

config certificate lsc ap-provision auth-list add *AP_mac_addr*

Note If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

Note To remove access points from the provision list, enter the **config certificate lsc ap-provision auth-list delete** *AP_mac_addr command.*

Note If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in *Step 8*). If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 10 See the LSC summary by entering this command:

show certificate lsc summary

Information similar to the following appears:

```
LSC Enabled..................................... Yes
LSC CA-Server................................... http://10.0.0.1:8080/caserver

LSC AP-Provisioning............................. Yes
 Provision-List................................. Not Configured
 LSC Revert Count in AP reboots................. 3
```

```
LSC Params:
 Country..................................... US
 State....................................... ca
 City........................................ ss
 Orgn........................................ org
 Dept........................................ dep
 Email....................................... dep@co.com
 KeySize..................................... 2048

LSC Certs:
 CA Cert..................................... Not Configured
 RA Cert..................................... Not Configured
```

Step 11 See details about the access points that are provisioned using LSC by entering this command:

show certificate lsc ap-provision

Information similar to the following appears:

```
LSC AP-Provisioning......................... Yes
Provision-List.............................. Present

Idx  Mac Address
---  ------------
1  00:18:74:c7:c0:90
```

Authorizing Access Points (GUI)

Step 1 Choose **Security** > **AAA** > **AP Policies** to open the **AP Policies** page.

Step 2 If you want the access point to accept self-signed certificates (SSCs), manufactured-installed certificates (MICs), or local significant certificates (LSCs), select the appropriate check box.

Step 3 If you want the access points to be authorized using a AAA RADIUS server, check the **Authorize MIC APs against auth-list or AAA** check box.

Step 4 If you want the access points to be authorized using an LSC, check the **Authorize LSC APs against auth-list** check box.

Enter the Ethernet MAC address for all APs except when in bridge mode (where you need to enter the radio MAC address).

Step 5 Click **Apply** to commit your changes.

Step 6 Follow these steps to add an access point to the controller's authorization list:

a) Click **Add** to access the **Add AP to Authorization List** area.
b) In the **MAC Address** field, enter the MAC address of the access point.
c) From the **Certificate Type** drop-down list, choose **MIC**, **SSC**, or **LSC**.
d) Click **Add**. The access point appears in the access point authorization list.

Note To remove an access point from the authorization list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note To search for a specific access point in the authorization list, enter the MAC address of the access point in the Search by MAC text box and click **Search**.

Authorizing Access Points (CLI)

Procedure

- Configure an access point authorization policy by entering this command:

  config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **authorize-lsc-ap** {**enable** | **disable**}}

- Configure an access point to accept manufactured-installed certificates (MICs), self-signed certificates (SSCs), or local significant certificates (LSCs) by entering this command:

  config auth-list ap-policy {**mic | ssc** | **lsc** {**enable** | **disable**}}

- Configure the user name to be used in access point authorization requests.

  config auth-list ap-policy {**authorize-ap username** {**ap_name** | **ap_mac** | **both**}}

- Add an access point to the authorization list by entering this command:

  config auth-list add {**mic** | **ssc** | **lsc**} *ap_mac* [*ap_key*]

  where *ap_key* is an optional key hash value equal to 20 bytes or 40 digits.

Note To delete an access point from the authorization list, enter this command: **config auth-list delete ap_mac**.

- See the access point authorization list by entering this command:

  show auth-list

Configuring VLAN Tagging for CAPWAP Frames from Access Points

VLAN Tagging for CAPWAP Frames from Access Points

You can configure VLAN tagging on the Ethernet interface either directly on the AP console or through the controller. The configuration is saved in the flash memory and all CAPWAP frames use the VLAN tag as configured, along with all the locally switched traffic, which is not mapped to a VLAN.

Restrictions for VLAN Tagging for CAPWAP Frames from APs

- This feature is not supported on mesh access points that are in bridge mode.
- CAPWAP VLAN tagging is supported in Release 8.5 and later releases on these 802.11ac Wave 2 APs: 18xx, 2800, 3800, and 1560.

This section contains the following subsections:

Configuring VLAN Tagging for CAPWAP Frames from Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the AP name from the list of AP names to open the Details page for the AP.

Step 3 Click the **Advanced** tab.

Step 4 In the VLAN Tagging area, select the **VLAN Tagging** check box.

Step 5 In the **Trunk VLAN ID** text box, enter an ID.

If the access point is unable to route traffic through the specified trunk VLAN after about 10 minutes, the access point performs a recovery procedure by rebooting and sending CAPWAP frames in untagged mode to try and reassociate with the controller. The controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN.

If the access point is unable to route traffic through the specified trunk VLAN, it untags the packets and reassociates with the controller. The controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN.

If the trunk VLAN ID is 0, the access point untags the CAPWAP frames.

The VLAN Tag status is displayed showing whether the AP tags or untags the CAPWAP frames.

Step 6 Click **Apply**.

Step 7 You are prompted with a warning message saying that the configuration will result in a reboot of the access point. Click **OK** to continue.

Step 8 Click **Save Configuration**.

What to do next

After the configuration, the switch or other equipment connected to the Ethernet interface of the AP must also be configured to support tagged Ethernet frames.

Configuring VLAN Tagging for CAPWAP Frames from Access Points (CLI)

Step 1 Configure VLAN tagging for CAPWAP frames from access points by entering this command:

config ap ethernet tag {**disable** | **id** *vlan-id*} {*ap-name* | **all**}

Step 2 You can see VLAN tagging information for an AP or all APs by entering this command:

show ap ethernet tag {**summary** | *ap-name*}

Using DHCP Option 43 and DHCP Option 60

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

The format of the TLV block is as follows:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of the IP addresses of controller management interfaces

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 listed above. The VCI string will have the "ServiceProvider". For example, a 3600 with this option will return this VCI string: "Cisco AP c3600-ServiceProvider".

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

Troubleshooting the Access Point Join Process

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

Controller software release 5.2 or later releases enable you to 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 controller 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 controller 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 controller, the controller collects information for all access points that send a discovery message to this controller and maintains information for any access points that have successfully joined this controller.

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

You can view join-related information for the following numbers of access points:

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

If any of these conditions are met and the access point has not yet joined a controller, 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.

Note The access point joins the controller with a DHCP address from an internal DHCP pool configured on WLC. When the DHCP lease address is deleted in WLC, the access point reloads with the following message:

AP Rebooting: Reset Reason - Admin Reload. This is a common behavior in Cisco IOS and Wave 2 APs.

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

When the access point joins a controller for the first time, the controller 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 controller, and the global syslog server IP address configuration on the controller has been changed using the **config ap syslog host global** *syslog_server_IP_address* command. In this case, the controller pushes the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific** *Cisco_AP syslog_server_IP_address* command. In this case, the controller pushes the new specific syslog server IP address to the access point.
- The access point gets disconnected from the controller, and the syslog server IP address has been configured from the access point CLI using the **lwapp ap log-server** *syslog_server_IP_address* command. This command works only if the access point is not connected to any controller.
- The access point gets disconnected from the controller and joins another controller. In this case, the new controller 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, provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points using the controller GUI and view the access point join information using the controller GUI or CLI.

Note When an AP in a Release 8.0 image tries to join Cisco WLC, Release 8.3 (having Release 8.2 as the primary image and Release 8.2.1 as the secondary image on Flash), the AP goes into a perpetual loop. (Note that the release numbers are used only as an example to illustrate the scenario of three different images and does not apply to the releases mentioned.) This loop occurs due to version mismatch. After the download, when the AP compares its image with the Cisco WLC image, there will be a version mismatch. The AP will start the entire process again, resulting in a loop.

Configuring the Syslog Server for Access Points (CLI)

Step 1 Perform one of the following:

- To configure a global syslog server for all access points that join this controller, enter this command:

  config ap syslog host global *syslog_server_IP_address*

  Note By default, the global syslog server IPv4/IPv6 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 controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

  Note Only one Syslog Server is used for both IPv4 and IPv6.

- To configure a syslog server for a specific access point, enter this command:

  config ap syslog host specific *Cisco_AP syslog_server_IP_address*

  Note By default, the syslog server IPv4/IPv6 address for each access point is 0.0.0.0, which indicates that the access point is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

Step 2 Enter the **save config** command to save your changes.

Step 3 See the global syslog server settings for all access points that join the controller by entering this command:

show ap config global

Information similar to the following appears:

```
AP global system logging host..................... 255.255.255.255
```

Step 4 See the syslog server settings for a specific access point by entering this command:

show ap config general *Cisco_AP*

Viewing Access Point Join Information

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

Viewing Access Point Join Information (GUI)

Step 1 Choose **Monitor** > **Statistics** > **AP Join** to open the AP Join Stats page.

This page lists all of the access points that are joined to the controller or that have tried to join. It shows the radio MAC address, access point name, current join status, Ethernet MAC address, IP address, and last join time for each access point.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can view these pages by clicking the page number links. Each page shows the join statistics for up to 25 access points.

Note If you want to remove an access point from the list, hover your cursor over the blue drop-down arrow for that access point and click **Remove**.

Note If you want to clear the statistics for all access points and start over, click **Clear Stats on All APs**.

Step 2 If you want to search for specific access points in the list of access points on the AP Join Stats page, follow these steps to create a filter to display only access points that meet certain criteria (such as MAC address or access point name).

Note This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

a) Click **Change Filter** to open the Search AP dialog box.
b) Select one of the following check boxes to specify the criteria used when displaying access points:
   - **MAC Address**—Enter the base radio MAC address of an access point.
   - **AP Name**—Enter the name of an access point.

   Note When you enable one of these filters, the other filter is disabled automatically.

c) Click **Find** to commit your changes. Only the access points that match your search criteria appear on the AP Join Stats page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

   Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Step 3 To see detailed join statistics for a specific access point, click the radio MAC address of the access point. The AP Join Stats Detail page appears.

This page provides information from the controller's perspective on each phase of the join process and shows any errors that have occurred.

Viewing Access Point Join Information (CLI)

Use these CLI commands to see access point join information:

- See the MAC addresses of all the access points that are joined to the controller or that have tried to join by entering this command:

  show ap join stats summary all

- See the last join error detail for a specific access point by entering this command:

  show ap join stats summary *ap_mac*

  where *ap_mac* is the MAC address of the 802.11 radio interface.

Note To obtain the MAC address of the 802.11 radio interface, enter the **show interfaces Dot11Radio 0** command on the access point.

Information similar to the following appears:

```
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
```

- See all join-related statistics collected for a specific access point by entering this command:

  show ap join stats detailed *ap_mac*

  Information similar to the following appears:

```
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
```

- Clear the join statistics for all access points or for a specific access point by entering this command:

  clear ap join stats {**all** | *ap_mac*}

Sending Debug Commands to Access Points Converted to Lightweight Mode

You can enable the controller to send debug commands to an access point converted to lightweight mode by entering this command:

debug ap {**enable** | **disable** | **command** *cmd*} *Cisco_AP*

When this feature is enabled, the controller sends debug commands to the converted access point as character strings. You can send any debug command supported by Cisco Aironet access points that run Cisco IOS software in lightweight mode.

Understanding How Converted Access Points Send Crash Information to the Controller

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 controller. If the unit rebooted because of a crash, the controller pulls up the crash file using existing CAPWAP messages and stores it in the controller flash memory. The crash info copy is removed from the access point flash memory when the controller pulls it from the access point.

Understanding How Converted Access Points Send Radio Core Dumps to the Controller

When a radio module in a converted access point generates a core dump, the access point stores the core dump file of the radio on its local flash memory at the time of the radio crash. It sends a notification message to the controller indicating which radio generated a core dump file. The controller sends a trap that alerts you so that you can retrieve the radio core file from the access point.

The retrieved core file is stored in the controller flash and can be uploaded through TFTP or FTP to an external server for analysis. The core file is removed from the access point flash memory when the controller pulls it from the access point.

Retrieving Radio Core Dumps (CLI)

Step 1 Transfer the radio core dump file from the access point to the controller by entering this command:

config ap crash-file get-radio-core-dump *slot Cisco_AP*

For the *slot* parameter, enter the slot ID of the radio that crashed.

Step 2 Verify that the file was downloaded to the controller by entering this command:

show ap crash-file

Uploading Radio Core Dumps (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **Radio Core Dump**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in the 7.4 and later releases)

Step 4 In the IP Address text box, enter the IP address of the server.

Step 5 In the File Path text box, enter the directory path of the file.

Step 6 In the File Name text box, enter the name of the radio core dump file.

Note The *filename* that you enter should match the filename generated on the controller. You can determine the *filename* on the controller by entering the **show ap crash-file** command.

Step 7 If you chose FTP as the Transfer Mode, follow these steps:

a) In the Server Login Username text box, enter the FTP server login name.
b) In the Server Login Password text box, enter the FTP server login password.
c) In the Server Port Number text box, enter the port number of the FTP server. The default value for the server port is 21.

Step 8 Click **Upload** to upload the radio core dump file from the controller. A message appears indicating the status of the upload.

Uploading Radio Core Dumps (CLI)

Step 1 Transfer the file from the controller to a server by entering these commands:

- **transfer upload mode** {**tftp** | **ftp** | **sftp**}
- **transfer upload datatype radio-core-dump**
- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

Note The *filename* that you enter should match the filename generated on the controller. You can determine the *filename* on the controller by entering the **show ap crash-file** command.

Note Ensure that the *filename* and *server_path_to_file* do not contain these special characters: \, :, *, ?, ", <, >, and |. You can use only / (forward slash) as the path separator. If you use the disallowed special characters in the filename, then the special characters are replaced with _ (underscores); and if you use the disallowed special characters in the *server_path_to_file*, then the path is set to the root path.

Step 2 If you are using an FTP server, also enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the *port* parameter is 21.

Step 3 View the updated settings by entering this command:

transfer upload start

Step 4 When prompted to confirm the current settings and start the software upload, answer **y**.

Uploading Memory Core Dumps from Converted Access Points

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

Uploading Access Point Core Dumps (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** > *access point name* > and choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 2 Select the **AP Core Dump** check box to upload a core dump of the access point.

Step 3 In the TFTP Server IP text box, enter the IP address of the TFTP server.

Step 4 In the File Name text box, enter a name of the access point core dump file (such as *dump.log*).

Step 5 Select the **File Compression** check box to compress the access point core dump file. When you enable this option, the file is saved with a .gz extension (such as *dump.log.gz*). This file can be opened with WinZip.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Uploading Access Point Core Dumps (CLI)

Step 1 Upload a core dump of the access point by entering this command on the controller:

config ap core-dump enable *tftp_server_ip_address filename* {**compress** | **uncompress**} {*ap_name* | **all**}

where

- *tftp_server_ip_address* is the IP address of the TFTP server to which the access point sends core dump files.

  Note The access point must be able to reach the TFTP server.

- *filename* is the name that the access points uses to label the core file.
- **compress** configures the access point to send compressed core files whereas **uncompress** configures the access point to send uncompressed core files.

  Note When you choose **compress**, the file is saved with a .gz extension (for example, dump.log.gz). This file can be opened with WinZip.

- *ap_name* is the name of a specific access point for which core dumps are uploaded and **all** is all access points converted to lightweight mode.

Step 2 Enter the **save config** command to save your changes.

Viewing the AP Crash Log Information

Whenever the controller reboots or upgrades, the AP crash log information gets deleted from the controller. We recommend that you make a backup of AP crash log information before rebooting or upgrading the controller.

Viewing the AP Crash Log information (GUI)

Procedure

- Choose **Management** > **Tech Support** > **AP Crash Log** to open the AP Crash Logs page.

Viewing the AP Crash Log information (CLI)

Step 1 Verify that the crash file was downloaded to the controller by entering this command:

show ap crash-file

Information similar to the following appears:

```
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.
```

Step 2 See the contents of the AP crash log file by entering this command:

show ap crash-file *Cisoc_AP*

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

Disabling the Reset Button on Access Points Converted to Lightweight Mode

You can disable the reset button on access points converted to lightweight mode. The reset button is labeled MODE on the outside of the access point.

Use this command to disable or enable the reset button on one or all converted access points associated to a controller:

config ap rst-button {**enable** | **disable**} {*ap-name*}

The reset button on converted access points is enabled by default.

Configuring a Static IP Address on 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 APs.

An access point cannot discover the controller 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.

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.

Configuring a Static IP Address (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure a static IP address. The All APs > Details for (General) page appears.

Step 3 Under IP Config, select the **Static IP (IPv4/IPv6)** check box if you want to assign a static IP address to this access point. The default value is unselected.

Note The static IP configured on the AP will take precedence over the preferred mode configured on the AP. For example: If AP has static IPV6 address and prefer-mode is set to IPV4, then the AP will join over IPv6.

Step 4 Enter the static IPv4/IPv6 address of the access point, subnet mask/ prefix length assigned to the access point IPv4/IPv6 address, and the IPv4/IPv6 gateway of the access point in the corresponding text boxes.

Step 5 Click **Apply** to commit your changes. The access point reboots and rejoins the controller, and the static IPv4/IPv6 address that you specified in Step 4 is sent to the access point.

Step 6 After the static IPv4/IPv6 address has been sent to the access point, you can configure the DNS server IP address and domain name as follows:

a) In the DNS IP Address text box, enter the IPv4/IPv6 address of the DNS server.
b) In the Domain Name text box, enter the name of the domain to which the access point belongs.
c) Click **Apply** to commit your changes.
d) Click **Save Configuration** to save your changes.

Configuring a Static IP Address (CLI)

Step 1 Configure a static IP address on the access point by entering this command:

For IPv4—**config ap static-ip enable** *Cisco_AP ip_address mask gateway*

For IPv6—**config ap static-ip enable** *Cisco_AP ip_address prefix_length gateway*

Note To disable static IP for the access point, enter the **config ap static-ip disable** *Cisco_AP* command.

Note The static IP configured on the AP takes precedence over the preferred mode that is configured on the AP. For example: If AP has static IPv6 address and prefer-mode is set to IPv4, then the AP will join over IPv6.

Step 2 Enter the **save config** command to save your changes.

The access point reboots and rejoins the controller, and the static IP address that you specified in Step 1 is pushed to the access point.

Step 3 After the static IPv4/IPv6 address has been sent to the access point, you can configure the DNSv4/DNSv6 server IP address and domain name as follows:

a) To specify a DNSv4/DNSv6 server so that a specific access point or all access points can discover the controller using DNS resolution, enter this command:

config ap static-ip add nameserver {*Cisco_AP* | **all**} *ip_address*

Note To delete a DNSv4/DNSv6 server for a specific access point or all access points, enter the **config ap static-ip delete nameserver** {*Cisco_AP* | **all**} command.

b) To specify the domain to which a specific access point or all access points belong, enter this command:

config ap static-ip add domain {*Cisco_AP* | **all**} *domain_name*

Note To delete a domain for a specific access point or all access points, enter this command: **config ap static-ip delete domain** {*Cisco_AP* | **all**}.

c) Enter the **save config** command to save your changes.

Step 4 See the IPv4/IPv6 address configuration for the access point by entering this command:

- For IPv4:

  show ap config general *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>

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
...
```

- For IPv6:

  show ap config general *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>

Cisco AP Identifier.............................. 16
Cisco AP Name.................................... AP2602I-A-K9-1
...
IPv6 Address Configuration....................... DHCPv6
IPv6 Address..................................... 2001:9:2:16:1ae:a1da:c2c7:44b
IPv6 Prefix Length............................... 128
Gateway IPv6 Addr................................ fe80::c60a:cbff:fe79:53c4
NAT External IP Address.......................... None

...
```

```
IPv6 Capwap UDP Lite.............................. Enabled
Capwap Prefer Mode................................ Ipv6 (ApGroup Config)
Hotspot Venue Group............................... Unspecified
Hotspot Venue Type................................ Unspecified
DNS server IP ..................................... Not Available
```

Supporting Oversized Access Point Images

Controller software release 5.0 or later releases allow you to upgrade to an oversized access point image by automatically deleting the recovery image to create sufficient space.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

Recovering the Access Point—Using the TFTP Recovery Procedure

Step 1 Download the required recovery image from Cisco.com (for example, ap3g2-rcvk9w8-tar.152-4.JB6.tar for 2700 or 3700 APs) 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 controller to download the oversized access point image and complete the upgrade procedure.

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

CHAPTER 106

Configuring Packet Capture

- Information About Packet Capture, on page 761
- Restrictions for Packet Capture, on page 762
- Configuring Packet Capture (CLI), on page 762

Information About Packet Capture

To resolve issues such as voice and security on wireless networks, you might need to dump packets from the AP for analysis while the AP continues to operate normally. The packets can be dumped on to an FTP server. This process of dumping packets for analysis is called Packet Capture. Use the controller to start or stop packet capture for clients. You can choose the type of packets that need to be captured using the controller CLI from the following types:

- Management Packets
- Control Packets
- Data Packets
  - Dot1X
  - ARP
  - IAPP
  - All IP
  - UDP with matching port number
  - DHCP
  - TCP with matching port number
  - Multicast frames
  - Broadcast frames

The packets are captured and dumped in the order of arrival or transmit of packets except for beacons and probe responses. The packet capture contains information such as channel, RSSI, data rate, SNR, and timestamp. Each packet is appended with additional information from the AP. You can choose to dump either just packet headers or full packets.

The following are some guidelines for packet capture:

- If FTP transfer time is slower than the packet rate, some of the packets do not appear in the capture file.
- If the buffer does not contain any packets, a known dummy packet is dumped to keep the connection alive.
- A file is created on the FTP server for each AP based on unique AP and controller name and timestamp. Ensure that the FTP server is reachable by the AP.
- If the FTP transfer fails or FTP connection is lost during packet capture, the AP stops capturing packets, notifies with an error message and SNMP trap, and a new FTP connection is established.

Restrictions for Packet Capture

- Packet capture can be enabled for only one client.
- This feature is not supported in intercontroller roaming scenarios. If you know the AP or the controller to which the client is going to roam, you can configure the packet capture for the client in the new controller or AP using the CLI.
- Not all packets in the air are captured, but only those that reach the radio driver.
- By default, a packet capture process is stopped after 10 minutes. You can, however, configure the packet capture to stop at any time between 1 to 60 minutes.

Configuring Packet Capture (CLI)

Step 1 Configure FTP parameters for packet capture by entering this command:

config ap packet-dump ftp serverip *ip-address* **path** *path* **username** *user_ID* **password** *password*

Step 2 Start or stop packet capture by entering this command:

config ap packet-dump {**start** *client-mac-address ap-name* | **stop**}

Step 3 Configure the buffer size for packet capture by entering this command:

config ap packet-dump buffer-size *size-in-kb*

Step 4 Configure the time for packet capture by entering this command:

config ap packet-dump capture-time *time-in-minutes*

The valid range is between 1 to 60 minutes.

Step 5 Configure the types of packets to be captured by entering this command:

config ap packet-dump classifier {**arp** | **broadcast** | **control** | **data** | **dot1x** | **iapp** | **ip** | **management** | **multicast** | {**tcp port** *port-number*} | {**udp port** *port-number*}} {**enable** | **disable**}

Step 6 Configure the packet length after truncation by entering this command:

config ap packet-dump truncate *length-in-bytes*

Step 7 Know the status of packet capture by entering this command:

show ap packet-dump status

Step 8 Configure debugging of packet capture by entering this command:

debug ap packet-dump {**enable** | **disable**}

CHAPTER 107

OfficeExtend Access Points

- Information About OfficeExtend Access Points, on page 765
- OEAP 600 Series Access Points, on page 766
- OEAP in Local Mode, on page 767
- Supported WLAN Settings for 600 Series OfficeExtend Access Point, on page 767
- WLAN Security Settings for the 600 Series OfficeExtend Access Point, on page 768
- Authentication Settings, on page 771
- Supported User Count on 600 Series OfficeExtend Access Point, on page 772
- Remote LAN Settings, on page 772
- Channel Management and Settings, on page 773
- Firewall Settings, on page 774
- Additional Caveats, on page 774
- Implementing Security, on page 775
- Licensing for an OfficeExtend Access Point, on page 775
- Configuring OfficeExtend Access Points, on page 776
- Configuring a Personal SSID on an OfficeExtend Access Point Other than 600 Series OEAP, on page 781
- Viewing OfficeExtend Access Point Statistics, on page 782
- Remote LANs, on page 782

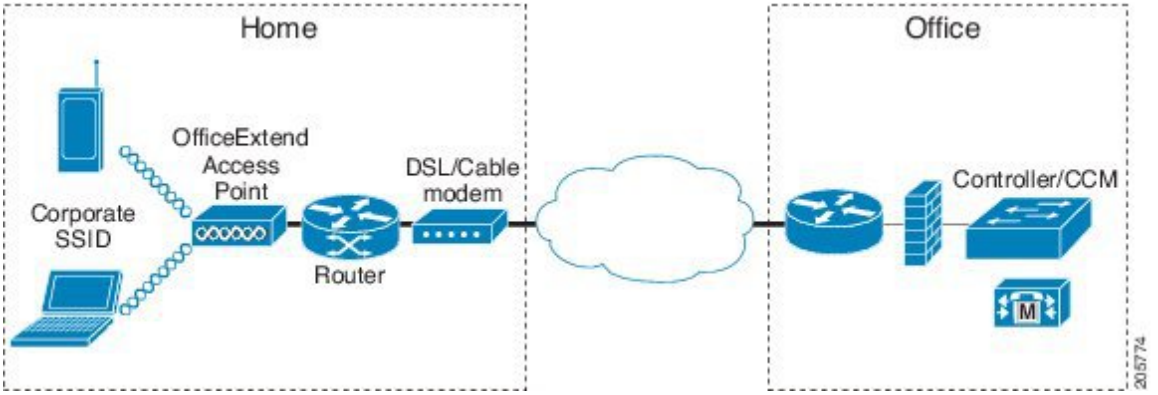
Information About OfficeExtend Access Points

A Cisco OfficeExtend access point (Cisco OEAP) provides secure communications from a Cisco WLC to a Cisco AP at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Note DTLS is permanently enabled on the Cisco OEAP. You cannot disable DTLS on this access point.

Figure 45: Typical OfficeExtend Access Point Setup

The following figure shows a typical OfficeExtend access point setup.



Note Cisco OEAPs are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. There is no limit to the number of Cisco OEAPs that you can deploy behind a NAT device.

All the supported indoor AP models with integrated antenna can be configured as OEAP except the AP-700I, AP-700W, and AP802 series access points.

Note All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

Note See the Release Notes for information about supported Cisco OEAPs.

OEAP 600 Series Access Points

This section details the requirements for configuring a Cisco wireless LAN controller for use with the Cisco 600 Series OfficeExtend Access Point. The 600 Series OfficeExtend Access Point supports split mode operation, and it requires configuration through the WLAN controller in local mode. This section describes the configurations necessary for proper connection and supported feature sets.

Note IPv6 is not supported on Cisco 600 Series OfficeExtend Access Points.

Note The CAPWAP UDP 5246 and 5247 ports must be open on the firewall between the WLAN controller and the 600 Series OfficeExtend Access Point.

Note Multicast is not supported on Cisco 600 Series OfficeExtend Access Points.

OEAP in Local Mode

The Cisco OEAP connects to the Cisco WLC in local mode. You cannot alter these settings.

Note Monitor mode, FlexConnect mode, Sniffer mode, Rogue Detector, Bridge, and SE-Connect are not supported on the Cisco OEAP and are not configurable.

Figure 46: OEAP Mode

Supported WLAN Settings for 600 Series OfficeExtend Access Point

The 600 Series OfficeExtend Access Point supports a maximum of three WLANs and one remote LAN. If your network deployment has more than three WLANs, you must place the 600 Series OfficeExtend Access Point in an AP group. If the 600 Series OfficeExtend Access Points are added to an AP group, the same limit of three WLANs and one remote LAN still applies for the configuration of the AP group.

If the 600 Series OfficeExtend Access Point is in the default group, which means that it is not in a defined AP group, the WLAN/remote LAN IDs must be set lower than ID 8.

If additional WLANs or remote LANs are created with the intent of changing the WLANs or remote LAN being used by the 600 Series OfficeExtend Access Point, you must disable the current WLANs or remote LAN that you are removing before enabling the new WLANs or remote LAN on the 600 Series OfficeExtend Access Point. If there are more than one remote LANs enabled for an AP group, disable all remote LANs and then enable only one of them.

If more than three WLANs are enabled for an AP group, disable all WLANs and then enable only three of them.

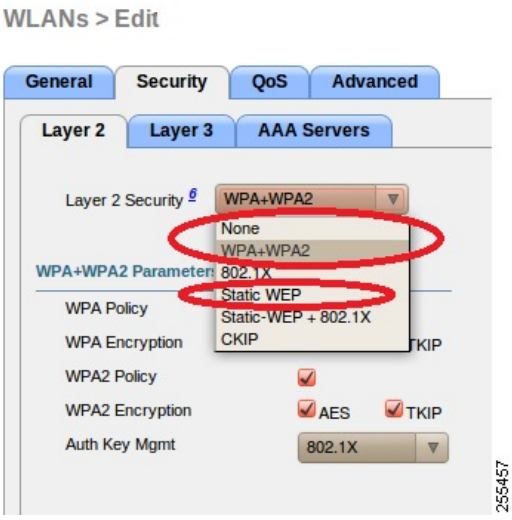
WLAN Security Settings for the 600 Series OfficeExtend Access Point

When configuring the security settings in the WLAN (see the following figure), note that there are specific elements that are not supported on the 600 Series OfficeExtend Access Point. CCX is not supported on the 600 Series OfficeExtend Access Point, and elements related to CCX are not supported.

For Layer 2 Security, the following options are supported for the 600 Series OfficeExtend Access Point:

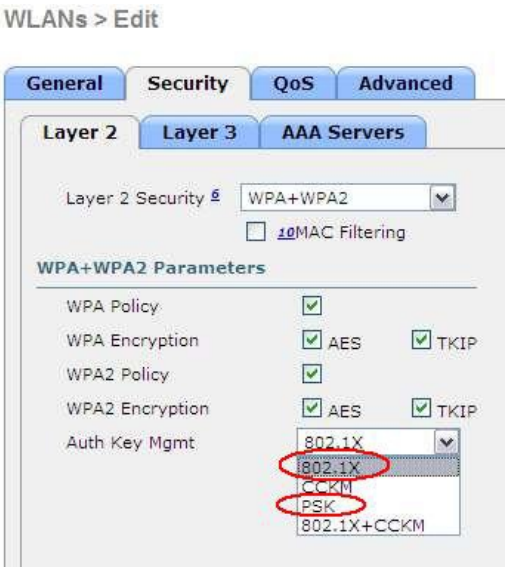
- None
- WPA+WPA2
- Static WEP
- 802.1X (only for remote LANs)

Figure 47: WLAN Layer 2 Security Settings



In the Security tab (see the following figure), do not select CCKM in WPA+WPA2 settings. Select only 802.1X or PSK.

Figure 48: WLAN Security Settings - Auth Key Management



Security encryption settings must be identical for WPA and WPA2 for TKIP and AES. The following are examples of incompatible settings for TKIP and AES.

Figure 49: Incompatible WPA and WPA2 Security Encryption Settings for OEAP 600 Series

Figure 50: Incompatible WPA and WPA2 Security Encryption Settings for OEAP 600 Series

The following are examples of compatible settings:

Figure 51: Compatible Security Settings for OEAP Series

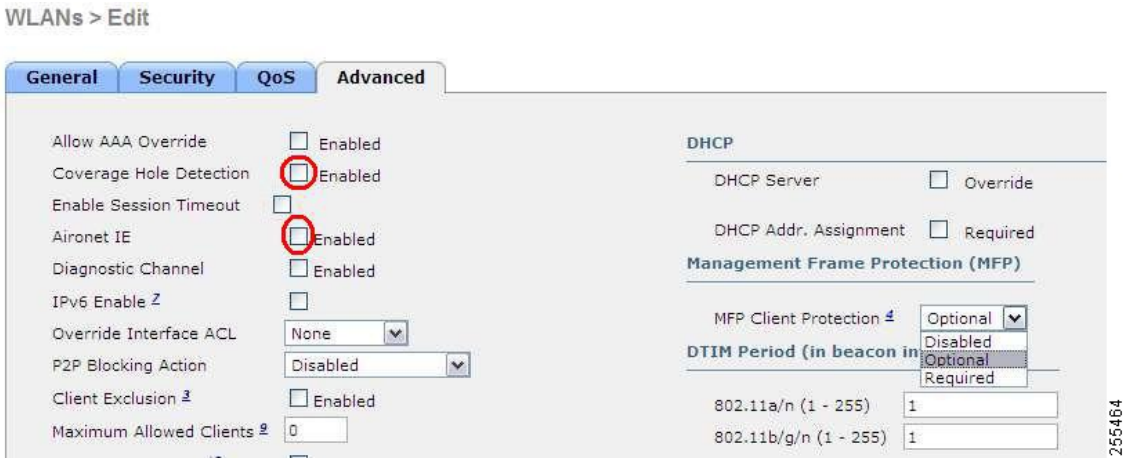
Figure 52: Compatible Security Settings for OEAP Series

QoS settings are supported (see the following figure), but CAC is not supported and should not be enabled.

Note Do not enable Coverage Hole Detection.

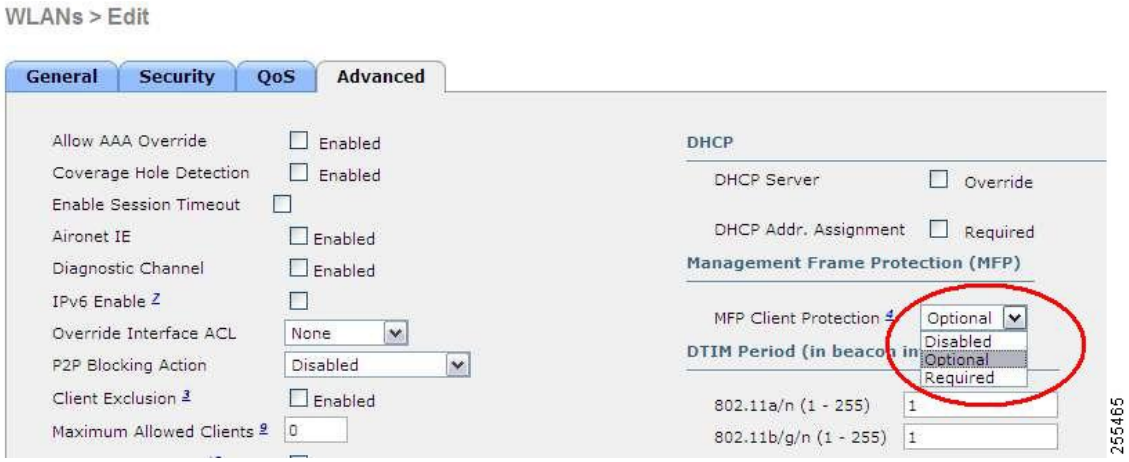
Note Aironet IE should not be enabled. This option is not supported.

Figure 53: QoS Settings for OEAP 600



MFP is also not supported and should be disabled or set to optional.

Figure 54: MFP Settings for OEAP Series Access Points



Client Load Balancing and Client Band Select are not supported.

Authentication Settings

For authentication on the 600 Series OfficeExtend Access Point, LEAP is not supported. This configuration must be addressed on the clients and RADIUS servers to migrate them to EAP-Fast, EAP-TTLS, EAP-TLS, or PEAP.

If Local EAP is being utilized on the controller, the settings would also have to be modified not to use LEAP.

Supported User Count on 600 Series OfficeExtend Access Point

Only 15 users are allowed to connect on the WLANs provided on the Cisco 600 Series OEAP at any one time, a sixteenth user cannot authenticate until one of the first clients is deauthenticated or timeout on the controller occurs. This number is cumulative across the controller WLANs on the 600 Series OfficeExtend Access Point.

For example, if two controller WLANs are configured and there are 15 users on one of the WLANs, no other users can join the other WLAN on the 600 Series OfficeExtend Access Point at that time.

This limit does not apply to the local private WLANs that the end user configures on the 600 Series OfficeExtend Access Point for personal use. Clients connected on these private WLANs or on the wired ports do not affect these limits.

Note This limit does not apply to other AP models that operate in the OfficeExtend mode.

Remote LAN Settings

Only four clients can connect through a remote LAN port on the 600 Series OfficeExtend Access Point. This number does not affect the fifteen user limit imposed for the Controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.

Remote LAN is configured in the same way that a WLAN or Guest LAN is configured on the controller:

Figure 55: Remote LAN Settings for OEAP 600 Series AP

Security settings can be left open, set for MAC filtering, or set for Web Authentication. The default is to use MAC filtering. Additionally, you can specify 802.1X Layer 2 security settings.

Figure 56: Layer 2 Security Settings for OEAP 600 Series APs in Remote LANs

Figure 57: Layer 3 Security Settings for OEAP 600 Series APs in Remote LANs

Channel Management and Settings

The radios for the 600 Series OfficeExtend Access Point are controlled through the Local GUI on the access point and not through the Wireless LAN Controller. The Tx power and channel settings can be set manually through the controller interface. RRM is not supported on the 600 Series OfficeExtend Access Point.

The 600 series scans and chooses channels for 2.4-GHz and 5-GHz during startup as long as the default settings on the local GUI are left as default in both spectrums.

Figure 58: Channel Selection for OEAP 600 Series APs

The channel bandwidth for 5.0 GHz is also configured on the 600 Series OfficeExtend Access Point Local GUI, for 20-MHz or 40-MHz wide channels. Setting the channel width to 40 MHz for 2.4 GHz is not supported and fixed at 20 MHz.

Figure 59: Channel Width for OEAP 600 APs

Firewall Settings

Firewall can be enabled on Cisco 600 Series OfficeExtend Access Point and filtering and forwarding rules can be applied. These ten pre-configured applications can be enabled or disabled:

- FTP
- Telnet
- SMTP
- DNS
- TFTP
- HTTP
- POP3
- NNTP
- SNMP
- HTTPS

These applications can be unblocked by providing the protocol (TCP/UDP), LAN client IP range and destination port range.

Note The firewall is applicable only to the personal traffic on the OEAP 600 APs The data traffic between the controller and OEAP 600 APs is addressed by a firewall in the corporate network.

600 Series OfficeExtend Access Point supports a maximum of ten port forwarding rules. Every rule takes protocol (TCP/UDP), WAN port range, Local LAN client IP (where traffic will be forwarded), LAN port range, and enable or disable as a parameter.

The DMZ feature allows one network computer connected to local LAN or WLAN to be exposed to the Internet for use of a special-purpose service like Internet gaming. DMZ forwards all the ports terminating on WAN IP at the same time to one PC. The Port Range Forwarding feature opens only the required ports to be opened, while DMZ opens all the ports of one computer, exposing the computer to the Internet or WAN. This will forward all the incoming WAN packets to any port which has the port forwarding rule configured on it. CAPWAP control and data connection ports will not be forwarded to DMZ IP.

Additional Caveats

- The Cisco 600 Series OfficeExtend Access Points (OEAPs) are designed for single AP deployments, therefore client roaming between Cisco 600 Series OEAPs is not supported.

  Disabling the 802.11a/n/ac or 802.11b/g/n on the controller may not disable these spectrums on the Cisco 600 Series OEAP because local SSID may be still working.

- Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

- Cisco Aironet APs other than 600 Series OEAPs that are converted to OEAP mode and mapped to locally switched WLAN forward the DHCP request to the local subnet on the AP connected switch. To avoid this condition, you must disable local switching and local authentication.

- For Cisco 600 Series OEAP to associate with Cisco Virtual Wireless LAN Controller, follow these steps:
  1. Configure the OEAP to associate with a physical controller that is using 7.5 or a later release and download the corresponding AP image.
  2. Configure the OEAP so that the OEAP does not associate with the physical controller again; for example, you can implement an ACL in the network to block CAPWAP between the OEAP and the physical controller.
  3. Configure the OEAP to associate with the Cisco Virtual Wireless LAN Controller.
- OEAP ACL is only supported for Cisco 600 Series OEAPs. For other AP models working as OEAP, you must use FlexConnect Split ACLs.

Implementing Security

Note The LSC configuration is optional. The Cisco OEAPs points do not support LSC.

1. Use local significant certificates (LSCs) to authorize your OfficeExtend access points, by following the instructions in the "Authorizing Access Points Using LSCs" sectionn.
2. Implement AAA server validation using the access point's MAC address, name, or both as the username in authorization requests, by entering this command:

   config auth-list ap-policy authorize-ap username {*ap_mac* | *Cisco_AP* | **both**}

   Using the access point name for validation can ensure that only the OfficeExtend access points of valid employees can associate with the controller. To implement this security policy, ensure that you name each OfficeExtend access point with an employee ID or employee number. When an employee is terminated, run a script to remove this user from the AAA server database, which prevents that employee's OfficeExtend access point from joining the network.
3. Save your changes by entering this command:

   save config

Note CCX is not supported on the 600 OEAP. Elements related to CCX are not supported. Also, only 802.1X or PSK is supported. TKIP and AES security encryption settings must be identical for WPA and WPA2.

Licensing for an OfficeExtend Access Point

To use Cisco OEAPs, a base license must be installed and in use on the Cisco WLC. After the license is installed, you can enable the OfficeExtend mode on the supported Cisco Aironet AP models that support OfficeExtend mode.

Configuring OfficeExtend Access Points

After Cisco Aironet access point has associated with the controller, you can configure it as an OfficeExtend access point.

Configuring OfficeExtend Access Points (GUI)

Step 1 Choose **Wireless** to open the **All APs** page.

Step 2 Click the name of the desired access point to open the **All APs > Details** page.

Step 3 Enable FlexConnect on the access point as follows:

a) In the **General** tab, choose **FlexConnect** from the **AP Mode** drop-down list to enable FlexConnect for this access point.

Step 4 Configure one or more controllers for the access point as follows:

a) Click the **High Availability** tab.

b) Enter the name and IP address of the primary controller for this access point in the **Primary Controller Name** and **Management IP Address** text boxes.

Note You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

c) If desired, enter the name and IP address of a secondary or tertiary controller (or both) in the corresponding **Controller Name** and **Management IP Address** text boxes.

d) Click **Apply**. The access point reboots and then rejoins the controller.

Note The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

Step 5 Enable OfficeExtend access point settings as follows:

a) Click the **FlexConnect** tab.

b) Select the **Enable OfficeExtend AP** check box to enable the OfficeExtend mode for this access point. The default value is selected.

Unselecting this check box disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to the factory-default settings, enter **clear ap config** *Cisco_AP* on the controller CLI. If you want to clear only the access point's personal SSID, click **Reset Personal SSID**.

Note The OfficeExtend AP support is enabled for all the supported Cisco Aironet integrated antenna access points.

Note Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point by selecting the **Rogue Detection** check box on the **All APs > Details for (Advanced)** page. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

Note DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point by selecting the **Data Encryption** check box on the **All APs > Details for (Advanced)** page.

Note Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by selecting the **Telnet** or **SSH** check box on the **All APs > Details for (Advanced)** page.

Note Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point by selecting the **Enable Link Latency** check box on the All APs > Details for (Advanced) page.

c) Check the **Enable Least Latency Controller Join** check box if you want the access point to choose the controller with the least latency when joining. Otherwise, leave this check box unchecked, which is the default value. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the controller that responds first.

d) Click **Apply**.

The **OfficeExtend AP** text box on the All APs page shows which access points are configured as OfficeExtend access points.

Step 6 Configure a specific username and password for the OfficeExtend access point so that the user at home can log into the GUI of the OfficeExtend access point:

a) Click the **Credentials** tab.

b) Select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.

c) In the **Username**, **Password**, and **Enable Password** text boxes, enter the unique username, password, and enable password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

d) Click **Apply**.

Note If you want to force this access point to use the controller's global credentials, uncheck the **Over-ride Global Credentials** check box.

These credentials are valid for Telnet/SSH and not for GUI of Wave 2 Cisco OEAP. For the GUI of Wave 2 Cisco OEAP, the default username of admin and the default password of admin can be used upon the first login and you are prompted to change the credentials locally on the Cisco OEAP.

Step 7 Configure access to local GUI, LAN ports, and local SSID of the OfficeExtend access points:

a) Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

b) Under OEAP Config Parameters, select or unselect the **Disable Local Access** check box to enable or disable local access of the OfficeExtend access points.

Note By default, the **Disable Local Access** check box is unselected and therefore the Ethernet ports and personal SSIDs are enabled. This configuration does not affect remote LAN. The port is enabled only when you configure a remote LAN.

Step 8 Configure split tunneling for the OfficeExtend access points as follows:

a) Choose **Wireless** > **Access Points** > **Global Configuration**.

b) In the OEAP Config Parameters area, select or unselect the **Disable Split Tunnel** check box.

Disabling split tunneling here disables split tunneling for all the WLANs and remote LANs. You can also disable split tunneling on a specific WLAN or remote LAN.

c) Click **Apply**.

Step 9 Click **Save Configuration**.

Step 10 If your controller supports only OfficeExtend access points, see the Configuring RRM section for instructions on setting the recommended values for the DCA interval, channel scan duration, and neighbor packet frequency.

Configuring OfficeExtend Access Points (CLI)

Procedure

- Enable FlexConnect on the access point by entering this command:

  config ap mode flexconnect *Cisco_AP*

- Configure one or more controllers for the access point by entering one or all of these commands:

  config ap primary-base *controller_name Cisco_AP controller_ip_address*

  config ap secondary-base *controller_name Cisco_AP controller_ip_address*

  config ap tertiary-base *controller_name Cisco_AP controller_ip_address*

Note You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Note The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

- Enable the OfficeExtend mode for this access point by entering this command:

  config flexconnect office-extend {**enable** | **disable**} *Cisco_AP*

  The default value is enabled. The **disable** parameter disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to the factory-default settings, enter this command:

  clear ap config *cisco-ap*

  If you want to clear only the access point's personal SSID, enter this command:

  config flexconnect office-extend clear-personalssid-config *Cisco_AP*

Note Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point or for all access points using the **config rogue detection** {**enable** | **disable**} {*Cisco_AP* | **all**} command. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

Note DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points using the **config ap link-encryption** {**enable** | **disable**} {*Cisco_AP* | **all**} command.

Note Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point using the **config ap** {**telnet** | **ssh**} {**enable** | **disable**} *Cisco_AP* command.

Note Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller using the **config ap link-latency** {**enable** | **disable**} {*Cisco_AP* | **all**} command.

- Enable the access point to choose the controller with the least latency when joining by entering this command:

  config flexconnect join min-latency {**enable** | **disable**} *Cisco_AP*

  The default value is disabled. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco WLC that responds first.

- Configure a specific username and password that users at home can enter to log into the GUI of the OfficeExtend access point by entering this command:

  config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

  The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note If you want to force this access point to use the controller's global credentials, enter the **config ap mgmtuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

- To configure access to the local network for the Cisco OfficeExtend access points, enter the following command:

  config network oeap local-network {**enable** | **disable**}

  When disabled, the local SSIDs, local ports are inoperative; and the console is not accessible. When reset, the default restores local access. This configuration does not affect the remote LAN configuration if configured on the access points.

- Configure the Dual R-LAN Ports feature, which allows the Ethernet port 3 of Cisco OfficeExtend access points to operate as a remote LAN by entering this command:

  config network oeap dual-rlan-ports {**enable** | **disable**}

This configuration is global to the controller and is stored by the AP and the NVRAM variable. When this variable is set, the behavior of the remote LAN is changed. This feature supports different remote LANs per remote LAN port.

The remote LAN mapping is different depending on whether the default group or AP Groups is used:

- Default Group—If you are using the default group, a single remote LAN with an even numbered remote LAN ID is mapped to port 4. For example, a remote LAN with remote LAN ID 2 is mapped to port 4. The remote LAN with an odd numbered remote LAN ID is mapped to port 3. For example, a remote LAN with remote LAN ID 1 is mapped to port 3.
- AP Groups—If you are using an AP group, the mapping to the OEAP ports is determined by the order of the AP groups. To use an AP group, you must first delete all remote LANs and WLANs from the AP group leaving it empty. Then, add the two remote LANs to the AP group adding the port 3 AP remote LAN first, and the port 4 remote group second, followed by any WLANs.

- Enable or disable split tunneling by entering this command:

  config network oeap split-tunnel {**enable** | **disable**}

  Disabling split tunneling here disables split tunneling for all the WLANs and remote LANs. You can also disable split tunneling on a specific WLAN or remote LAN.

- Save your changes by entering this command:

  save config

Note If your controller supports only OfficeExtend access points, see the Configuring Radio Resource Management section for instructions on setting the recommended value for the DCA interval.

Configuring Split Tunneling for a WLAN or a Remote LAN

Configuring Split Tunneling for a WLAN or a Remote LAN (GUI)

Step 1 Choose **WLANs** and click the WLAN ID to open the WLANs > Edit page.

The WLAN that you choose can be a WLAN or a remote LAN depending on its configuration.

Step 2 Click the **Advanced** tab.

Step 3 In the OEAP area, select or unselect the **Split Tunnel** check box.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Split Tunneling for a WLAN or a Remote LAN (CLI)

Procedure

- Enable or disable split tunneling for a WLAN by entering this command:

config wlan split-tunnel *wlan-id* {**enable** | **disable**}

- See the split tunneling status for a WLAN by entering this command:
  show wlan *wlan-id*
- Enable or disable split tunneling for a remote LAN by entering this command:
  config remote-lan split-tunnel *rlan-id* {**enable** | **disable**}
- See the split tunneling status for a remote LAN by entering this command:
  show remote-lan *rlan-id*

Note When a remote LAN or wireless client on a corporate SSID communicate among themselves, all the traffic on the corporate SSID and remote LAN is tunneled back to the controller.

Configuring a Personal SSID on an OfficeExtend Access Point Other than 600 Series OEAP

The Cisco 600 Series OEAPs are not supported from Cisco Wireless Release 8.4.

Step 1 Find the IP address of your OfficeExtend access point by doing one of the following:

- Log on to your home router and look for the IP address of your OfficeExtend access point.
- Ask your company's IT professional for the IP address of your OfficeExtend access point.
- Use an application such as Network Magic to detect devices on your network and their IP addresses.

Step 2 With the OfficeExtend access point connected to your home router, enter the IP address of the OfficeExtend access point in the Address text box of your Internet browser and click **Go**.

Note Make sure that you are not connected to your company's network using a virtual private network (VPN) connection.

Step 3 When prompted, enter the username and password to log into the access point.

Step 4 On the OfficeExtend Access Point Welcome page, click **Enter**. The OfficeExtend Access Point Home page appears.

Step 5 Choose **Configuration** to open the Configuration page.

Step 6 In the SSID text box, enter the personal SSID that you want to assign to this access point. This SSID is locally switched.

Note A controller with an OfficeExtend access point publishes only up to 15 WLANs to each connected access point because it reserves one WLAN for the personal SSID.

Step 7 From the Security drop-down list, choose **Open**, **WPA2/PSK (AES)**, or **104 bit WEP** to set the security type to be used by this access point.

Note If you choose WPA2/PSK (AES), make sure that the client is configured for WPA2/PSK and AES encryption.

Step 8 If you chose WPA2/PSK (AES) in *Step 8*, enter an 8- to 38-character WPA2 passphrase in the Secret text box. If you chose 104 bit WEP, enter a 13-character ASCII key in the Key text box.

Step 9 Click **Apply**.

Note If you want to use the OfficeExtend access point for another application, you can clear this configuration and return the access point to the factory-default settings by clicking **Clear Config**. You can also clear the access point's configuration from the controller CLI by entering the **clear ap config** *Cisco_AP* command.

These steps can be used for configuring a personal SSID on OfficeExtend access points only. See the *Aironet 600 Series OfficeExtend Access Point Configuration Guide* for information on configuring a personal SSID on OEAP 600 APs.

Viewing OfficeExtend Access Point Statistics

Use these commands to view information about the OfficeExtend access points on your network:

- See a list of all OfficeExtend access points by entering this command:

  show flexconnect office-extend summary

- See the link delay for OfficeExtend access points by entering this command:

  show flexconnect office-extend latency

- See the encryption state of all access points or a specific access point by entering this command:

  show ap link-encryption {**all** | *Cisco_AP*}

  This command also shows authentication errors, which track the number of integrity check failures, and replay errors, which track the number of times that the access point receives the same packet. See the data plane status for all access points or a specific access point by entering this command:

  show ap data-plane {**all** | *Cisco_AP*}

Remote LANs

This section describes how to configure remote LANs.

Prerequisites

- You must remove all remote LANs from a controller's configuration before moving to a release that does not support the remote LAN functionality. The remote LAN changes to a WLAN in earlier releases, which could cause an undesirable or unsecured WLAN being broadcast on the wireless network. Remote LAN is only supported in release 7.0.116.0 and later.
- Remote LAN can be applied on a dedicated LAN port on a Cisco Aironet 600 Series OEAP.

Restrictions

- Only four clients can connect to a Cisco Aironet 600 Series OEAP through a remote LAN port. This number does not affect the fifteen WLAN limit imposed for the controller WLANs. The remote LAN

client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.

- It is not possible to configure 802.1X on remote LANs through the controller GUI; configuration only through CLI is supported.

This section contains the following subsections:

Configuring a Remote LAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

This page lists all of the WLANs and remote LANs currently configured on the controller. For each WLAN, you can see its WLAN/remote LAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs/Remote LANs appears in the upper right-hand corner of the page. If the list of WLANs/Remote LANs spans multiple pages, you can access these pages by clicking the page number links.

Note If you want to delete a Remote LAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove**, or select the check box to the left of the row, choose **Remove Selected** from the drop-down list, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the remote LAN is removed from any access point group to which it is assigned and from the access point's radio.

Step 2 Create a new Remote-LAN by choosing **Create New** from the drop-down list and clicking **Go**. The WLANs > New page appears.

Step 3 From the Type drop-down list, choose **Remote LAN** to create a remote LAN.

Step 4 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this Remote WLAN. The profile name must be unique.

Step 5 From the WLAN ID drop-down list, choose the ID number for this WLAN.

Step 6 Click **Apply** to commit your changes. The **WLANs > Edit** page appears.

Note You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

Step 7 Use the parameters on the General, Security, and Advanced tabs to configure this remote LAN. See the sections in the rest of this chapter for instructions on configuring specific features.

Step 8 On the General tab, select the **Status** check box to enable this remote LAN. Be sure to leave it unselected until you have finished making configuration changes to the remote LAN.

Note You can also enable or disable remote LANs from the WLANs page by selecting the check boxes to the left of the IDs that you want to enable or disable, choosing **Enable Selected** or **Disable Selected** from the drop-down list, and clicking **Go**.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring a Remote LAN (CLI)

Procedure

- See the current configuration of the remote LAN by entering this command:

  show remote-lan *remote-lan-id*

- Enable or disable remote LAN by entering this command:

  config remote-lan {**enable** | **disable**} *remote-lan-id*

- Enable or disable 802.1X authentication for remote LAN by entering this command:

  config remote-lan security 802.1X {**enable** | **disable**} *remote-lan-id*

Note The encryption on a remote LAN is always “none.”

- Enable or disable local EAP with the controller as an authentication server by entering this command:

  config remote-lan local-auth enable *profile-name remote-lan-id*

- If you are using an external AAA authentication server, use the following command:

  config remote-lan radius_server auth {**add** | **delete**} *remote-lan-id server id*

  config remote-lan radius_server auth {**add** | **delete**} *remote-lan-id*

CHAPTER 108

Using Cisco Workgroup Bridges

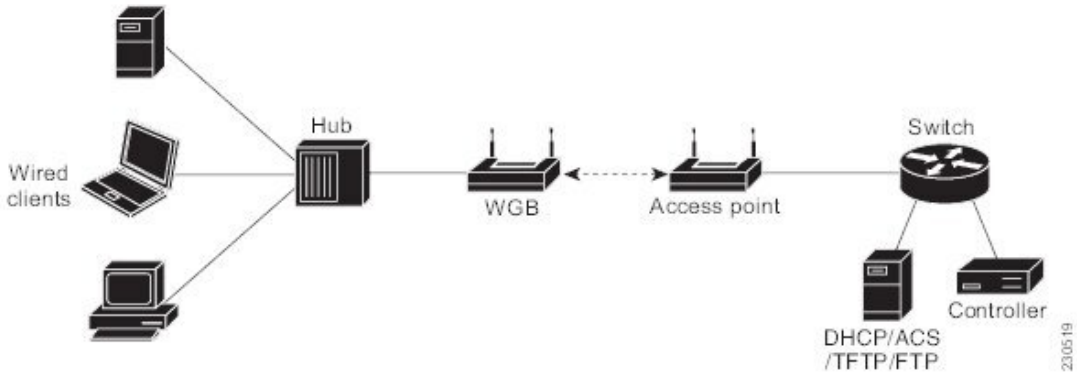
- Information About Cisco Workgroup Bridges, on page 785
- Restrictions for Cisco Workgroup Bridges, on page 787
- WGB Configuration Example, on page 788
- Viewing the Status of Workgroup Bridges (GUI), on page 789
- Viewing the Status of Workgroup Bridges (CLI), on page 789
- Debugging WGB Issues (CLI), on page 789

Information About Cisco Workgroup Bridges

A workgroup bridge (WGB) is a mode that can be configured on an autonomous 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. The lightweight access point treats the WGB as a wireless client.

A Cisco IOS AP as a WGB using the Cisco IOS 15.2 or later releases support Protected Extensible Authentication Protocol (PEAP) with the controller.

Figure 60: WGB Example



Note If the lightweight access point fails, the WGB attempts to associate to another access point.

The following are some guidelines for Cisco Workgroup Bridges:

- The WGB can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release 12.4(3g)JA or later releases (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or later releases (on 16-MB access points). These access points include the AP1120, AP1121, AP1130, AP1231, AP1240, and AP1310. Cisco IOS releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

  Note If your access point has two radios, you can configure only one for workgroup bridge mode. This radio is used to connect to the lightweight access point. We recommend that you disable the second radio.

  Enable the workgroup bridge mode on the WGB as follows:

  - On the WGB access point GUI, choose **Workgroup Bridge** for the role in radio network on the Settings > Network Interfaces page.
  - On the WGB access point CLI, enter the **station-role workgroup-bridge** command.

  Note See the sample WGB access point configuration in the WGB Configuration Example section.

- The following features are supported for use with a WGB:
  - Guest N+1 redundancy
  - Local EAP
  - Open, WEP 40, WEP 128, CKIP, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, and EAP-TLS authentication modes
- Wired clients connected to the WGB are not authenticated for security. Instead, the WGB is authenticated against the access point to which it associates. Therefore, we recommend that you physically secure the wired side of the WGB.
- Wired clients connected to a WGB inherit the WGB's QoS and AAA override attributes.
- To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.
- If you have to apply ACL to WGB during run time, do not modify the ACL configuration for interface in the controller during run time. If you need to modify any ACLs, then you must disable all WLANs that are in the controller or disable both the 802.11a and 80.11b networks. Also, ensure that there are no clients associated and mapped to that interface and then you can modify the ACL settings.

Restrictions for Cisco Workgroup Bridges

- The WGB can associate only with lightweight access points.
- Only WGBs in client mode (which is the default value) are supported. Those WGBs in infrastructure mode are not supported. Perform one of the following to enable client mode on the WGB:
  - On the WGB access point GUI, choose **Disabled** for the Reliable Multicast to WGB parameter.
  - On the WGB access point CLI, enter the **no infrastructure client** command.

  Note VLANs are not supported for use with WGBs.

- The following features are not supported for use with a WGB:
  - Idle timeout
  - Web authentication

  Note If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB wired clients are deleted.

- The WGB supports a maximum of 20 wired clients. If you have more than 20 wired clients, use a bridge or another device.
- The DirectStream feature from the controller does not work for clients behind workgroup bridges and the stream is denied.
- With Layer 3 roaming, if you plug a wired client into the WGB network after the WGB has roamed to another controller (for example, to a foreign controller), the wired client's IP address displays only on the anchor controller, not on the foreign controller.
- If a wired client does not send traffic for an extended period of time, the WGB removes the client from its bridge table, even if traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. To avoid the traffic loss, prevent the wired client from being removed from the bridge table by configuring the aging-out timer on the WGB to a large value using the following Cisco IOS commands on the WGB:

  ```
  configure terminal
  bridge bridge-group-number aging-time seconds
  exit
  end
  ```

  where *bridge-group-number* is a value between 1 and 255, and *seconds* is a value between 10 and 1,000,000 seconds. We recommend configuring the *seconds* parameter to a value greater than the wired client's idle period.
- When you delete a WGB record from the controller, all of the WGB wired clients' records are also deleted.

- These features are not supported for wired clients connected to a WGB:
  - MAC filtering
  - Link tests
  - Idle timeout
- The broadcast forwarding toward wired WGB clients works only on the native VLAN. If additional VLANs are configured, only the native VLAN forwards broadcast traffic.
- Wired clients behind a WGB cannot connect to a DMZ/Anchor controller. To enable wired clients behind a WGB to connect to an anchor controller in a DMZ, you must enable VLANs in the WGB using the **config wgb vlan enable** command.
- The **dot11 arp-cache** global configuration command that you can enter on the access point that is in WGB mode is not supported.
- WGB clients do not show enc-cipher and AKM because they are wired clients. WGB APs, however, show correct values of enc-cipher and AKM.

WGB Configuration Example

The following is an example of the configuration of a WGB access point using static WEP with a 40-bit WEP key:

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

```
ap# 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#
```

Viewing the Status of Workgroup Bridges (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

The WGB text box on the right side of the page indicates whether any of the clients on your network are workgroup bridges.

Step 2 Click the MAC address of the desired client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows "WGB" if this client is a workgroup bridge, and the Number of Wired Client(s) text box shows the number of wired clients that are connected to this WGB.

Step 3 See the details of any wired clients that are connected to a particular WGB as follows:

a) Click **Back** on the Clients > Detail page to return to the Clients page.

b) Hover your cursor over the blue drop-down arrow for the desired WGB and choose **Show Wired Clients**. The WGB Wired Clients page appears.

Note If you want to disable or remove a particular client, hover your cursor over the blue drop-down arrow for the desired client and choose **Remove** or **Disable**, respectively.

c) Click the MAC address of the desired client to see more details for this particular client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows "WGB Client," and the rest of the text boxes on this page provide additional information for this client.

Viewing the Status of Workgroup Bridges (CLI)

Step 1 See any WGBs on your network by entering this command:

show wgb summary

Step 2 See the details of any wired clients that are connected to a particular WGB by entering this command:

show wgb detail *wgb_mac_address*

Debugging WGB Issues (CLI)

Before you begin

- Enable debugging for IAPP messages, errors, and packets by entering these commands:
  - **debug iapp all enable**—Enables debugging for IAPP messages.

- **debug iapp error enable**—Enables debugging for IAPP error events.
- **debug iapp packet enable**—Enables debugging for IAPP packets.

- Debug an roaming issue by entering this command:

  debug mobility handoff enable
- Debug an IP assignment issue when DHCP is used by entering these commands:
  - **debug dhcp message enable**
  - **debug dhcp packet enable**
- Debug an IP assignment issue when static IP is used by entering these commands:
  - **debug dot11 mobile enable**
  - **debug dot11 state enable**

CHAPTER 109

Using Non-Cisco Workgroup Bridges

- Non-Cisco Workgroup Bridges, on page 791
- Restrictions for Non-Cisco Workgroup Bridges, on page 792

Non-Cisco Workgroup Bridges

When a Cisco workgroup bridge (WGB) is used, the WGB informs the access points of all the clients that it is associated with. The controller is aware of the clients associated with the access point. When non-Cisco WGBs are used, the controller has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the controller 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

The following are some guidelines for non-Cisco workgroup bridges:

- The controller can accommodate non-Cisco WGBs so that the controller can forward ARP, DHCP, and data traffic to and from the wired clients behind workgroup bridges by enabling the passive client feature. To configure your controller to work with non-Cisco WGBs, you must enable the passive client feature so that all traffic from the wired clients is routed through the WGB to the access point. All traffic from the wired clients is routed through the work group bridge to the access point.

  Note For FlexConnect APs in local switching, non-Cisco workgroup-bridge clients in bridged mode are supported using the **config flexconnect group** *group-name* **dhcp overridden-interface enable** command.

- When a WGB wired client leaves a multicast group, the downstream multicast traffic to other WGB wired clients is interrupted briefly.
- If you have clients that use PC virtualization software such as VMware, you must enable this feature.

Note We have tested multiple third-party devices for compatibility but cannot ensure that all non-Cisco devices work. Support for any interaction or configuration details on the third-party device should be discussed with the device manufacturer.

- You must enable the passive client functionality for all non-Cisco workgroup bridges.
- You might need to use the following commands to configure DHCP on clients:
  - Disable DHCP proxy by using the **config dhcp proxy disable** command.
  - Enable DHCP boot broadcast by using the **config dhcp proxy disable bootp-broadcast enable** command.

This section contains the following subsection:

Restrictions for Non-Cisco Workgroup Bridges

- Only Layer 2 roaming is supported for WGB devices.
- Layer 3 security (web authentication) is not support for WGB clients.
- Visibility of wired hosts behind a WGB on a controller is not supported because the non-Cisco WGB device performs MAC hiding. Cisco WGB supports IAPP.
- ARP poisoning detection does not work on a WLAN when the flag is enabled.
- VLAN select is not supported for WGB clients.
- Some third-party WGBs need to operate in non-DHCP relay mode. If problems occur with the DHCP assignment on devices behind the non-Cisco WGB, use the **config dhcp proxy disable** and **config dhcp proxy disable bootp-broadcast disable** commands.

  The default state is DHCP proxy enabled. The best combination depends on the third-party characteristics and configuration.

CHAPTER 110

Configuring Backup Controllers

- Backup Controllers, on page 793
- Restrictions for Configuring Backup Controllers, on page 794
- Configuring Backup Controllers (GUI), on page 794
- Configuring Backup Controllers (CLI), on page 795

Backup Controllers

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

The following are some guidelines for configuring backup controllers:

- You can configure primary and secondary backup controllers (which are used if primary, secondary, or tertiary controllers are not specified or are not responsive) for all access points connected to the controller as well as various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller 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 controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.
- The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list. When the access point receives a new discovery response from a controller, the backup controller list is updated. Any controller that fails to respond to two consecutive primary discovery requests is removed from the list. If the access point's local controller fails, it chooses an available controller from the backup controller list in this order: primary, secondary, tertiary, primary backup, and secondary backup. The access point waits for a discovery response from the first available controller in the backup list and joins the controller 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 controller cannot be joined and waits for a discovery response from the next available controller in the list.
- When an access point's primary controller comes back online, the access point disassociates from the backup controller and reconnects to its primary controller. The access point falls back only to its primary controller and not to any available secondary controller for which it is configured. For example, if an access point is configured with primary, secondary, and tertiary controllers, it fails over to the tertiary controller when the primary and secondary controllers become unresponsive. If the secondary controller

comes back online while the primary controller is down, the access point does not fall back to the secondary controller and stays connected to the tertiary controller. The access point waits until the primary controller comes back online to fall back from the tertiary controller to the primary controller. If the tertiary controller fails and the primary controller is still down, the access point then falls back to the available secondary controller.

This section contains the following subsections:

Restrictions for Configuring Backup Controllers

- You can configure the fast heartbeat timer only for access points in local and FlexConnect modes.

Configuring Backup Controllers (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 From the Local Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for access points in local mode or choose **Disable** to disable this timer. The default value is Disable.

Step 3 If you chose Enable in Step 2, enter the Local Mode AP Fast Heartbeat Timeout text box to configure the fast heartbeat timer for access points in local mode. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the AP Fast Heartbeat Timeout value for Cisco Flex 7510 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco Flex 7510 Controllers is 10. The default value for other controllers is 1 second.

Step 4 From the FlexConnect Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for FlexConnect access points or choose **Disable** to disable this timer. The default value is Disable.

Step 5 If you enable FlexConnect fast heartbeat, enter the FlexConnect Mode AP Fast Heartbeat Timeout value in the FlexConnect Mode AP Fast Heartbeat Timeout text box. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the FlexConnect Mode AP Fast Heartbeat Timeout value for Cisco Flex 7510 Controllers is 10–15 (inclusive) and is 1–10 for other controllers. The default value for the heartbeat timeout for Cisco Flex 7510 Controllers is 10. The default value for other controllers is 1 second.

Step 6 In the AP Primary Discovery Timeout text box, a value between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.

Step 7 If you want to specify a primary backup controller for all access points, enter the IPv4/IPv6 address of the primary backup controller in the Back-up Primary Controller IP Address (IPv4/IPv6) text box and the name of the controller in the Back-up Primary Controller Name text box.

Note The default value for the IP address is 0.0.0.0, which disables the primary backup controller.

Step 8 If you want to specify a secondary backup controller for all access points, enter the IPv4/IPv6 address of the secondary backup controller in the Back-up Secondary Controller IP Address (IPv4/IPv6) text box and the name of the controller in the Back-up Secondary Controller Name text box.

Note The default value for the IP address is 0.0.0.0, which disables the secondary backup controller.

Step 9 Click **Apply** to commit your changes.

Step 10 Configure primary, secondary, and tertiary backup controllers for a specific access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to configure primary, secondary, and tertiary backup controllers.
c) Choose the **High Availability** tab to open the All APs > Details for (High Availability) page.
d) If desired, enter the name and IP address of the primary controller for this access point in the Primary Controller text boxes.

Note Entering an IP address for the backup controller is optional in this step and the next two steps. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. The controller name and IP address must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

e) If desired, enter the name and IP address of the secondary controller for this access point in the Secondary Controller text boxes.
f) If desired, enter the name and IP address of the tertiary controller for this access point in the Tertiary Controller text boxes.
g) Click **Apply** to commit your changes.

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

Configuring Backup Controllers (CLI)

Step 1 Configure a primary controller for a specific access point by entering this command:

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

Note The *controller_ip_address* parameter in this command and the next two commands is optional. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. In each command, the *controller_name* and *controller_ip_address* must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

Step 2 Configure a secondary controller for a specific access point by entering this command:

config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 3 Configure a tertiary controller for a specific access point by entering this command:

config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 4 Configure a primary backup controller for all access points by entering this command:

config advanced backup-controller primary *system name ip_addr*

Note This command is valid for both IPv4 and IPv6

Step 5 Configure a secondary backup controller for all access points by entering this command:

config advanced backup-controller secondary *system name ip_addr*

Note To delete a primary or secondary backup controller entry, enter *0.0.0.0* for the controller IPv4/IPv6 address.

Note This command is valid for both IPv4 and IPv6

Step 6 Enable or disable the fast heartbeat timer for local or FlexConnect access points by entering this command:

config advanced timers ap-fast-heartbeat {**local** | **flexconnect** | **all**} {**enable | disable**} *interval*

where **all** is both local and FlexConnect access points, and *interval* is a value between 1 and 10 seconds (inclusive). Specifying a small heartbeat interval reduces the amount of time that it takes to detect a controller failure. The default value is disabled.Configure the access point heartbeat timer by entering this command:

config advanced timers ap-heartbeat-timeout *interval*

where *interval* is a value between 1 and 30 seconds (inclusive). This value should be at least three times larger than the fast heartbeat timer. The default value is 30 seconds.

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.

Step 7 Configure the access point primary discovery request timer by entering this command:

config advanced timers ap-primary-discovery-timeout *interval*

where *interval* is a value between 30 and 3600 seconds. The default value is 120 seconds.

Step 8 Configure the access point discovery timer by entering this command:

config advanced timers ap-discovery-timeout *interval*

where *interval* is a value between 1 and 10 seconds (inclusive). The default value is 10 seconds.

Step 9 Configure the 802.11 authentication response timer by entering this command:

config advanced timers auth-timeout *interval*

where *interval* is a value between 5 and 600 seconds (inclusive). The default value is 10 seconds.

Step 10 Save your changes by entering this command:

save config

Step 11 See an access point's configuration by entering these commands:

- **show ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**

Information similar to the following appears for the **show ap config general** *Cisco_AP* command for Primary Cisco Switch IP Address using IPv4:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
```

```
MAC Address..................................... 00:13:80:60:48:3e
IP Address Configuration........................ DHCP
IP Address...................................... 1.100.163.133
...
Primary Cisco Switch Name....................... 1-5520
Primary Cisco Switch IP Address................. 2.2.2.2
Secondary Cisco Switch Name..................... 1-8540
Secondary Cisco Switch IP Address............... 2.2.2.2
Tertiary Cisco Switch Name...................... 2-8540
Tertiary Cisco Switch IP Address................ 1.1.1.4
...
```

Information similar to the following appears for the **show ap config general** *Cisco_AP* command for Primary Cisco Switch IP Address using IPv6:

```
Cisco AP Identifier............................. 1
Cisco AP Name................................... AP6
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............................ 802.11bg:-A 802.11a:-A
Switch Port Number ............................. 13
MAC Address..................................... 44:2b:03:9a:9d:30
IPv6 Address Configuration...................... DHCPv6
IPv6 Address.................................... 2001:9:5:96:295d:3b2:2db2:9b47
IPv6 Prefix Length.............................. 128
Gateway IPv6 Addr............................... fe80::6abd:abff:fe8c:764a
NAT External IP Address......................... None
CAPWAP Path MTU................................. 1473
Telnet State.................................... Globally Disabled
Ssh State....................................... Globally Disabled
Cisco AP Location............................... _5500
Cisco AP Floor Label............................ 0
Cisco AP Group Name............................. IPv6-Same_VLAN
Primary Cisco Switch Name....................... Maulik_WLC_5500-HA
Primary Cisco Switch IP Address................. 2001:9:5:95::11
```

Information similar to the following appears for the **show advanced backup-controller** command when configured using IPv4:

```
AP primary Backup Controller ................... controller1 10.10.10.10
AP secondary Backup Controller ............... 0.0.0.0
```

Information similar to the following appears for the **show advanced backup-controller** command when configured using IPv6:

```
AP primary Backup Controller ................... WLC_5500-2 fd09:9:5:94::11
AP secondary Backup Controller ................. vWLC 9.5.92.11
```

Information similar to the following appears for the **show advanced timers** command:

```
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
```

CHAPTER 111

High Availability

- Information About High Availability, on page 799
- Restrictions for High Availability, on page 803
- Configuring High Availability (GUI), on page 806
- Enabling High Availability (CLI), on page 807
- Replacing the Primary Controller in an HA Setup, on page 810

Information About High Availability

High availability (HA) in controllers allows you to reduce the downtime of the wireless networks that occurs due to the failover of controllers.

A 1:1 (Active:Standby-Hot) stateful switchover of access points and clients is supported (HA SSO). In an HA architecture, one controller is configured as the primary controller and another controller as the secondary controller.

After you enable HA, the primary and secondary controllers are rebooted. During the boot process, the role of the primary controller is negotiated as active and the role of the secondary controller as standby-hot. After a switchover, the secondary controller becomes the active controller and the primary controller becomes the standby-hot controller. After subsequent switchovers, the roles are interchanged between the primary and the secondary controllers. The reason or cause for most switchover events is due to a manual trigger, a controller and/or a network failure.

During an HA SSO failover event, all of the AP CAPWAP sessions and client sessions in RUN state on the controller are statefully switched over to the standby controller without interruption, except PMIPv6 clients, which will need to reconnect and authenticate to the controller following an HA SSO switchover. For additional client SSO behaviors and limitations, see the "Client SSO" section in the *High Availability (SSO) Deployment Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html#pgfId-53637

The standby-hot controller continuously monitors the health of the active controller through its dedicated redundancy port. Both the controllers share the same configurations, including the IP address of the management interface.

Before you enable HA, ensure that both the controllers can successfully communicate with one another through their dedicated redundancy port, either through a direct cable connection or through Layer 2. For more details, see the "Redundancy Port Connectivity" section in the *High Availability (SSO) Deployment Guide*:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html#pgfId-83028

ACL and NAT IP configurations are synchronized to the HA standby controller when these parameters are configured before HA pair-up. If the NAT IP is set on the management interface, the access point sets the AP manager IP address as the NAT IP address.

The following are some guidelines for high availability:

- We recommend that you do not pair two controllers of different hardware models. If they are paired, the higher controller model becomes the active controller and the other controller goes into maintenance mode.
- We recommend that you do not pair two controllers on different controller software releases. If they are paired, the controller with the lower redundancy management address becomes the active controller and the other controller goes into maintenance mode.
- All download file types, such as image, configuration, web-authentication bundle, and signature files– are downloaded on the active controller first and then pushed to the standby-hot controller.
- Certificates should be downloaded separately on each controller before they are paired.
- You can upload file types such as configuration files, event logs, crash files, and so on, from the standby-hot controller using the GUI or CLI of the active controller. You can also specify a suffix to the filename to identify the uploaded file.
- To perform a peer upload, use the service port. In a management network, you can also use the redundancy management interface (RMI) that is mapped to the redundancy port or RMI VLAN, or both, where the RMI is the same as the management VLAN. Note that the RMI and the redundancy port should be in two separate Layer2 VLANs, which is a mandatory configuration.
- If the controllers cannot reach each other through the redundant port and the RMI, the primary controller becomes active and the standby-hot controller goes into the maintenance mode.

Note To achieve HA between two Cisco Wireless Services Module 2 (WiSM2) platforms, the controllers should be deployed on a single chassis, or on multiple chassis using a virtual switching system (VSS) and extending a redundancy VLAN between the multiple chassis.

Note A redundancy VLAN should be a nonroutable VLAN in which a Layer 3 interface should not be created for the VLAN, and the interface should be allowed on the trunk port to extend an HA setup between multiple chassis. Redundancy VLAN should be created like any other data VLAN on Cisco IOS-based switching software. A redundancy VLAN is connected to the redundant port on Cisco WiSM2 through the backplane. It is not necessary to configure the IP address for the redundancy VLAN because the IP address is automatically generated. Also, ensure that the redundancy VLAN is not the same as the management VLAN.

For more information, see the "*High Availability Connectivity Using Redundant VLAN on WiSM-2 WLC*" section in the in the *High Availability (SSO) Deployment Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html#pgfId-43232

Note When the RMIs for two controllers that are a pair, and that are mapped to same VLAN and connected to same Layer3 switch stop working, the standby controller is restarted.

The "mobilityHaMac is out of range" XML message is seen during the active/standby second switchover in an HA setup. This occurs if mobility HA MAC field is more than 128.

- When HA is enabled, the standby controller always uses the Remote Method Invocation (RMI), and all the other interfaces—dynamic and management, are invalid.

Note The RMI is meant to be used only for active and standby communications and not for any other purpose.

- When HA is enabled, ensure that you do not use the backup image. If this image is used, the HA feature might not work as expected:
  - The service port and route information that is configured is lost after you enable SSO. You must configure the service port and route information again after you enable SSO. You can configure the service port and route information for the standby-hot controller using the **peer-service-port** and **peer-route** commands.
  - For Cisco WiSM2, service port reconfigurations are required after you enable redundancy. Otherwise, Cisco WiSM2 might not be able to communicate with the supervisor. We recommend that you enable DHCP on the service port before you enable redundancy.
  - We recommend that you do not use the **reset** command on the standby-hot controller directly. If you use this, unsaved configurations will be lost.
- We recommend that you enable link aggregation configuration on the controllers before you enable the port channel in the infrastructure switches.

- All the configurations that require reboot of the active controller results in the reboot of the standby-hot controller.
- The Rogue AP Ignore list is not synchronized from the active controller to the standby-hot controller. The list is relearned through SNMP messages from Cisco Prime Infrastructure after the standby-hot controller becomes active.
- Client SSO related guidelines:
  - The standby controller maintains two client lists: one is a list of clients in the Run state and the other is a list of transient clients in all the other states.
  - Only the clients that are in the Run state are maintained during failover. Clients that are in transition, such as roaming, 802.1X key regeneration, web authentication logout, and so on, are dissociated.
  - As with AP SSO, Client SSO is supported only on WLANs. The controllers must be in the same subnet. Layer3 connection is not supported.
- In Release 7.3.x, AP SSO is supported, but client SSO is not supported, which means that after an HA setup that uses Release 7.3.x encounters a switchover, all the clients associated with the controller are deauthenticated and forced to reassociate.
- You must manually configure the mobility MAC address on the then active controller post switchover, when a peer controller has a controller software release that is prior to Release 7.2.

Redundancy Management Interface

The active and standby-hot controllers use the RMI to check the health of the peer controller and the default gateway of the management interface through network infrastructure.

The RMI is also used to send notifications from the active controller to the standby-hot controller if a failure or manual reset occurs. The standby-hot controller uses the RMI to communicate to the syslog, NTP/SNTP server, FTP, and TFTP server.

It is mandatory to configure the IP addresses of the Redundancy Management Interface and the Management Interface in the same subnet on both the primary and secondary controllers.

Redundancy Port

The redundancy port is used for configuration, operational data synchronization, and role negotiation between the primary and secondary controllers.

The redundancy port checks for peer reachability by sending UDP keepalive messages every 100 milliseconds (default frequency) from the standby-hot controller to the active controller. If a failure of the active controller occurs, the redundancy port is used to notify the standby-hot controller.

If an NTP/SNTP server is not configured, the redundancy port performs a time synchronization from the active controller to the standby-hot controller.

In Cisco WiSM2, the redundancy VLAN must be configured on the Cisco Catalyst 6000 Supervisor Engine because there is no physical redundancy port available on Cisco WiSM2.

The redundancy port and the redundancy VLAN in Cisco WiSM2 are assigned an automatically generated IP address in which the last two octets are obtained from the last two octets of the RMI. The first two octets are always 169.254. For example, if the IP address of the RMI is 209.165.200.225, the IP address of the redundancy port is 169.254.200.225.

The redundancy ports can connect over an L2 switch. Ensure that the redundancy port round-trip time is less than 80 milliseconds if the keepalive timer is set to default, that is, 100 milliseconds, or 80 percent of the keepalive timer if you have configured the keepalive timer in the range of 100 milliseconds to 400 milliseconds. The failure detection time is calculated, for example, if the keepalive timer is set to 100 milliseconds, as follows: 3 * 100 = 300 + 60 = 360 + jitter (12 milliseconds) = ~400 milliseconds. Also, ensure that the bandwidth between redundancy ports is 60 Mbps or higher. Ensure that the maximum transmission unit (MTU) is 1500 bytes or higher.

Related Documentation

- *High Availability (SSO) Deployment Guide*—https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html
- *N+1 High Availability Deployment Guide*—https://www.cisco.com/c/en/us/td/docs/wireless/technology/hi_avail/N1_High_Availability_Deployment_Guide.html

Restrictions for High Availability

- We recommend that you do not disable LAG physical ports when HA SSO is enabled.
- HA sync for Fabric-related statistics is not supported.
- In an HA environment using FlexConnect locally switched clients, the client information might not show the username. To get details about the client, you must use the MAC address of the client. This restriction does not apply to FlexConnect centrally switched clients or central (local) mode clients.
- It is not possible to access the Cisco WiSM2 GUI through the service interface when you have enabled HA. The workaround is to create a service port interface again after HA is established.
- In an HA environment, an upgrade from an LDPE image to a non-LDPE image is not supported.
- It is not possible to pair two primary controllers or two secondary controllers.
- Standby controllers are unavailable on the APs connected switch port.
- An HA-SKU controller with an evaluation license cannot become a standby controller. However, an HA-SKU controller with zero license can become a standby controller.
- In an HA setup, CPU-ACL cannot be applied on the service port. However, if you want to block the service port using CPU-ACL, you can use the command **config acl high-priority** to configure as required.
- Service VLAN configuration is lost when moving from HA mode to non-HA mode and conversely. You should then configure the service IP address manually again.
- The following scenario is not supported: The primary controller has the management address and the redundancy management address in the same VLAN, and the secondary controller has the management address in the same VLAN as the primary one, and the redundancy management address in a different VLAN.
- The following is a list of some software upgrade scenarios:
  - A software upgrade on the active controller ensures the upgrade of the standby-hot controller.
  - An in-service upgrade is not supported. Therefore, you should plan your network downtime before you upgrade the controllers in an HA environment.

- Rebooting the active controller after a software upgrade also reboots the standby-hot controller.
- We recommend that both active and standby-hot controllers have the same software image in the backup before running the **config boot backup** command. If both active and standby-hot controllers have different software images in the backup, and if you run the **config boot backup** command in the active controller, both the controllers reboot with their respective backup images breaking the HA pair due to a software mismatch.
- A schedule reset applies to both the controllers in an HA environment. The peer controller reboots a minute before the scheduled time expires on the active controller.
- You can reboot the standby-hot controller from the active controller by entering the **reset peer-system** command if the scheduled reset is not planned. If you reset only the standby-hot controller with this command, any unsaved configurations on the standby-hot controller are lost. Therefore, ensure that you save the configurations on the active controller before you reset the standby-hot controller.
- If an SSO is triggered at the time of the image transfer, a preimage download is reinitiated.
- Only **debug** and **show** commands are allowed on the standby-hot controller.
- After a switchover, if a peer controller has a controller software release that is prior to Release 7.5, all the mobility clients are deauthenticated.

- It is not possible to access the standby-hot controller through the controller GUI, Cisco Prime Infrastructure, or Telnet. You can access the standby-hot controller only on its console.
- In an HA setup, client Tx or Rx packets are not sent to the standby controller, hence, Remote Method Invocation (RMI) is not supported.
- When a failover occurs, the standby controller must be in a standby-hot state and the redundant port in a terminal state in SSO for successful switchover to occur.
- To enable or disable LAG, you must disable HA.

Note If LAG is disabled and both primary and backup ports are connected to the management interface and if the primary port becomes nonoperational, a switchover might occur because the default gateway is not reachable and backup port failover might exceed 12 seconds.

- Pairwise Master Key (PMK) cache synchronization is not supported on FlexConnect local-authenticated clients.
- Client SSO restrictions:
  - New mobility is not supported.
  - Posture and network admission control out-of-band are not supported because the client is not in the Run state.
  - The following are not synchronized between the active and standby controller:
    - Cisco Compatible Extension-based applications
    - Client statistics

- Proxy Mobile IPv6, Application Visibility and Control, session initiation protocol (SIP), and static call admission control (CAC) tree
- Workgroup bridges and the clients that are associated with them
- Passive clients

- Encryption is supported.

- Encryption is supported only if the active and standby controllers communicate through the Redundancy Management Interface on the management ports. Encryption is not supported if the redundancy port is used for communication between the active and standby controllers.
- You cannot change the NAT address configuration of the management interface when the controllers are in redundancy mode. To enable NAT address configuration on the management interface, you must remove the redundancy configuration first, make the required changes on the primary controller, and then reenable the redundancy configuration on the same controller.
- On Cisco WiSM2 and Cisco Catalyst 6500 Series Supervisor Engine 2T, if HA is enabled, post switchover, the APs might disconnect and reassociate with the WiSM2 controller. To prevent this from occurring, before you configure HA, we recommend that you verify, in the port channel, the details of both the active and standby Cisco WiSM2 controllers that the ports are balanced in the same order and the port channel hash distribution uses fixed algorithm. If they are not in order, you must change the port channel distribution to be fixed and reset Cisco WiSM2 from the Cisco Catalyst 6500 Series Supervisor Engine 2T.
- After you enable SSO, you must access both the standby and active controller using:
  - The console connection
  - SSH facility on the service port
  - SSH facility on the redundant management interface

Note While SSO is enabled, you cannot access both the standby and active controller either using the web UI/the telnet facility or using Cisco Prime Infrastructure/Prime NCS on the service port. This issue is addressed via CSCuf71713 in Release 8.2 and later releases.

- Synchronization of bulk configurations is supported only for the configurations that are stored in XMLs. Scheduled reboot is a configuration that is not stored in XMLs or Flash. Therefore, the scheduled reboot configuration is not included in the synchronization of bulk configurations.
- When a switchover occurs, the controller does not synchronize the information on DHCP dirty bit from the active to standby controller even when DHCP dirty bit is set on the active controller. After a switchover, the controller populates the DHCP dirty bit based on the client DHCP retries.
- If you are using Cisco WiSM2, we recommend that you use the following release versions of Cisco IOS on Cisco Catalyst 6500 Series Supervisor Engine 2T:
  - 15.1(02)SY
  - 15.1(01)ICB40.1

- 15.1(01)ICB29.36
- 15.1(01)ICB29.1
- 15.1(01)IC66.25
- 15.1(01)IB273.72

Configuring High Availability (GUI)

Before you begin

Ensure that the management interfaces of both controllers are in the same subnet. You can verify this on the GUI of both the controllers by choosing **Controllers > Interfaces** and viewing the IP addresses of the management interface.

Step 1 On the GUI of both the controllers, choose **Controller > Redundancy > Global Configuration**.

The **Global Configuration** window is displayed.

Step 2 Enter the addresses of the controllers in the **Redundant Management IP** field and the **Peer Redundant Management IP** field.

Note Ensure that the Redundant Management Interface IP address of one controller is the same as the Redundant Management Interface IP address of the peer controller.

Step 3 From the **Redundant Unit** drop-down list, choose one of the controllers as primary and the other as secondary.

Step 4 On the GUI of both the controllers, set the **SSO** to **Enabled** state.

Note After you enable an SSO, the service port peer IP address and the service port netmask appear on the configuration window. Note that the service port peer IP address and the netmask can be pushed to the peer only if the HA peer is available and operational. When you enable HA, you do not have to configure the service port peer IP address and the service port netmask parameters. You must configure the parameters only when the HA peer is available and operational. After you enable SSO, both the controllers are rebooted. During the reboot process, the controllers negotiate the redundancy role through the redundant port, based on the configuration. The primary controller becomes the active controller and the secondary controller becomes the standby controller.

Step 5 [Optional] After the HA pair becomes available and operational, you can configure the peer service port IP address and the netmask after the service port is configured as static. If you enable DHCP on the service port, you do not have to configure these parameters on the **Global Configuration** window:

- **Service Port Peer IP**—IP address of the service port of the peer controller.
- **Service Port Peer Netmask**—Netmask of the service port of the peer controller.
- **Mobility MAC Address**—A common MAC address for both the active and standby controllers that is used in the mobility protocol. If an HA pair has to be added as a mobility member for a mobility group, the mobility MAC address (instead of the system MAC address of the active or standby controller) should be used. Normally, the mobility MAC address is chosen as the MAC address of the active controller and you do not have to manually configure this.

- **Keep Alive Timer**—The timer that controls how often the standby controller sends keepalive messages to the active controller. The valid range is between 100 to 1000 milliseconds.
- **Peer Search Timer**—The timer that controls how often the active controller sends peer search messages to the standby controller. The valid range is between 60 to 300 seconds.

Note After you enable the HA and pair the controllers, there is only one unified GUI to manage the HA pair through the management port. GUI access through the service port is not feasible for both the active and standby controllers. The standby controller can be managed only through the console port or the service port.

Only Telnet and SSH sessions are allowed through the service port of the active and standby controllers.

Step 6 Click **Save Configuration**.

Step 7 View the redundancy status of the HA pair by choosing **Monitor > Redundancy > Summary**.

The **Redundancy Summary** window is displayed.

Step 8 (Optional) Perform these steps to configure the peer network route:

a) Choose **Controller** > **Redundancy** > **Peer Network Route**.

The **Network Routes Peer** window is displayed.

This window provides a summary of the existing service port network routes of the peer controller to network or element management systems on a different subnet. You can view the IP address, IP netmask, and gateway IP address.

b) To create a new peer network route, click **New**.
c) Enter the **IP address**, **IP netmask**, and the **Gateway IP address** of the route.
d) Click **Apply**.

Enabling High Availability (CLI)

Step 1 Before you configure HA, it is mandatory to have the management interface of both the controllers in the same subnet. See the interface summary information by entering these commands on both the controllers:

show interface summary

Step 2 HA is disabled by default. Before you enable HA, it is mandatory to configure the redundancy management IP address and the peer redundancy management IP address. Both the interfaces must be in the same subnet as the management interface. Enter the following commands to configure the redudancy management IP addresses:

- On WLC1: **config interface redundancy-management** *redundancy-mgmt-ip-addr-wlc1***peer-redundancy-management** *peer-redundancy-mgmt-ip-addr-wlc2*
- On WLC2: **config interface redundancy-management** *redundancy-mgmt-ip-addr-wlc2***peer-redundancy-management** *peer-redundancy-mgmt-ip-addr-wlc1*

Step 3 Configure one controller as primary (by default, the WLC HA Unit ID is primary and should have a valid AP-BASE count license installed) and another controller as secondary (AP-BASE count from the primary controller is inherited by this unit) by entering these commands:

- WLC1 as primary—**config redundancy unit primary**
- WLC2 as secondary—**config redundancy unit secondary**

Note You are not required to configure the unit as secondary if it is a factory-ordered HA SKU that can be ordered from Release 7.3 onwards. A factory-ordered HA SKU is a default secondary unit and takes the role of the standby controller the first time it is paired with an active controller that has a valid AP count license.

To convert any existing controller as a standby controller, use the **config redundancy unit secondary** command on the CLI. This command works only if the controller that is intended to work as a standby also has some number of permanent license count. This condition is only valid for the Cisco 5508 controller, where a minimum of 50 AP permanent licenses are needed to be converted to standby. This restriction is not applicable to other controller models.

Step 4 After you have configured the controllers with redundancy management and peer redundancy management IP addresses and have configured the redundant units, you must enable SSO. Ensure that the physical connections are operational between both the controllers (that is, both the controllers are connected back to back via the redundant port using an Ethernet cable) and the uplink is also connnected to the infrastructure switch and the gateway is reachable from both the controllers before SSO is enabled.

After SSO is enabled, controllers are rebooted. During the boot process, the controllers negotiate the HA role as per the configuration via the redundant port. If the controllers cannot reach each other via the redundant port or via the redundant management interface, the controller that is configured as secondary might go into maintenance mode.

Enable SSO on both the controllers by entering these commands:

config redundancy mode sso

Note Enabling SSO initiates a controller reboot.

Step 5 Enabling SSO reboots the controllers to negotiate the HA role as per the configuration performed. Once the role is determined, configuration is synchronized from the active controller to the standby controller via the redundant port. Initially, the controller configured as secondary reports XML mismatch and downloads the configuration from the active controller and reboot again. During the next reboot after determining the HA role, the controller validates the configuration again, reports no XML mismatch,and process further to establish itself as the standby controller.

Note Once SSO is enabled, you can access the standby controller through a console connection or through SSH on the service port and on the redundant management interface.

Step 6 After SSO is enabled, controllers are rebooted, the XML configuration is synchronized, WLC1 transitions its state to active and WLC2 transitions its state to standby hot. From this point, GUI, Telnet, and SSH for WLC2 on the management interface does not work because all the configurations and management must be done from the active controller. If required, the standby controller (WLC2) can be managed only through the console or service port.

Once the peer controller transitions to the standby hot state, the *-Standby* keyword is automatically appended to the standby controller's prompt name.

Step 7 To see the redundancy summary information for both the controllers, enter this command:

show redundancy summary

Configuring High Availability Parameters

Procedure

- Configure encryption of communication between controllers by entering this command:

  config redundancy link-encryption {**enable** | **disable**}

- Configure the IP address and netmask of the peer service port of the standby controller by entering this command:

  config redundancy interface address peer-service-port *ip-address netmask*

  This command can be run only if the HA peer controller is available and operational.

- (Optional) Configure the route configurations of the standby controller by entering this command:

  config redundancy peer-route {**add** *network-ip-addr ip-mask* | **delete** *network-ip-addr*}

Note This command can be run only if the HA peer controller is available and operational.

- (Optional) Configure a mobility MAC address by entering this command:

  config redundancy mobilitymac *mac-addr*

Note

- This command can be run only when SSO is disabled.
- If you upgrade from Release 8.0.110.0 to a later release, this command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade.

- Configure a redundancy timer by entering this command:

  config redundancy timer {**keep-alive-timer** *time-in-milliseconds* | **peer-search-timer** *time-in-seconds*}

- View the status of the redundancy by entering this command:

  show redundancy {**summary** | **detail**}

- View information about the redundancy management interface by entering this command:

  show interface detailed redundancy-management

- View information about the redundancy port by entering this command:

  show interface detailed redundancy-port

- Reboot a peer controller by entering this command:

  reset peer-system

- Start the upload of file types, such as configuration, event logs, crash files, and so on from the standby-hot controller by entering this command on the active controller:

  transfer upload peer-start

Replacing the Primary Controller in an HA Setup

In an HA setup, suppose the primary controller is not operational and you are required to replace it; the standby controller is operational with all the APs associated with it; and the new controller received return material authorization (RMA) that can be added with one of the failed controllers in the HA pair. Follow these steps to replace the primary controller in an active HA setup:

Step 1 Ensure that the new controller and the controller to be replaced are running the same version of the controller software.

Step 2 Configure the new controller with the same subnet management IP addresses as the controller to replaced.

Step 3 Configure the new controller with HA configuration that includes redundancy management, IP address, and peer primary. Enable AP SSO.

Step 4 When AP SSO is enabled, the controller reboots. While the controller reboots, the AP SSO discovers the currently active standby controller, synchronized the configuration, and transitions to a standby-hot state.

Note You do not need to break the HA configuration on the current active controller or reboot the current active controller. The configuration will be synchronized with the current active controller.

CHAPTER 112

Configuring Failover Priority for Access Points

- Failover Priority for Access Points, on page 811
- Configuring Failover Priority for Access Points (GUI), on page 811
- Configuring Failover Priority for Access Points (CLI), on page 812
- Viewing Failover Priority Settings (CLI), on page 812

Failover Priority for Access Points

Each controller embedded controller has a defined number of communication ports for access points. When multiple controllers embedded 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.

The following are some guidelines for configuring failover priority for access points:

- You can configure your wireless network so that the backup controller embedded controller 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.
- 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 controller an embedded controller failure than there are available backup controller ports.
- You can enable failover priority on your network and assign priorities to the individual access points.
- By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

This section contains the following subsections:

Configuring Failover Priority for Access Points (GUI)

Step 1 Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

Step 2 From the Global AP Failover Priority drop-down list, choose **Enable** to enable access point failover priority or choose **Disable** to disable this feature and turn off any access point priority assignments. The default value is Disable.

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

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

Step 5 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 6 Click the name of the access point for which you want to configure failover priority.

Step 7 Choose the **High Availability** tab. The All APs > Details for (High Availability) page appears.

Step 8 From the AP Failover Priority drop-down list, choose one of the following options to specify the priority of the access point:

- **Low**—Assigns the access point to the level 1 priority, which is the lowest priority level. This is the default value.
- **Medium**—Assigns the access point to the level 2 priority.
- **High**—Assigns the access point to the level 3 priority.
- **Critical**—Assigns the access point to the level 4 priority, which is the highest priority level.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring Failover Priority for Access Points (CLI)

Step 1 Enable or disable access point failover priority by entering this command:

config network ap-priority {**enable** | **disable**}

Step 2 Specify the priority of an access point by entering this command:

config ap priority {**1** | **2** | **3** | **4**} *Cisco_AP*

where 1 is the lowest priority level and 4 is the highest priority level. The default value is 1.

Step 3 Enter the **save config** command to save your changes.

Viewing Failover Priority Settings (CLI)

- Confirm whether access point failover priority is enabled on your network by entering this command:

  show network summary

  Information similar to the following appears:

```
RF-Network Name............................. mrf
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable
Ethernet Broadcast Mode..................... Disable
```

```
IGMP snooping.............................. Disabled
IGMP timeout............................... 60 seconds
User Idle Timeout.......................... 300 seconds
ARP Idle Timeout........................... 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority.......................... Enabled

...
```

- See the failover priority for each access point by entering this command:

  show ap summary

  Information similar to the following appears:

```
Number of APs.................................. 2
Global AP User Name............................ user
Global AP Dot1x User Name...................... Not Configured

AP Name  Slots  AP Model           Ethernet MAC       Location   Port Country Priority
-------  -----  ------------------ -----------------  ---------  ---- ------- --------
ap:1252  2      AIR-LAP1252AG-A-K9 00:1b:d5:13:39:74  hallway 6  1    US      1
ap:1121  1      AIR-LAP1121G-A-K9  00:1b:d5:a9:ad:08  reception  1    US      3
```

To see the summary of a specific access point, you can specify the access point name. You can also use wildcard searches when filtering for access points.

CHAPTER 113

Configuring AP Retransmission Interval and Retry Count

- AP Retransmission Interval and Retry Count, on page 815
- Restrictions for Access Point Retransmission Interval and Retry Count, on page 815
- Configuring the AP Retransmission Interval and Retry Count (GUI), on page 816
- Configuring the Access Point Retransmission Interval and Retry Count (CLI), on page 816

AP Retransmission Interval and Retry Count

The controller and the APs exchange packets using the 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 APs reassociate with another controller.

This section contains the following subsections:

Restrictions for Access Point Retransmission Interval and Retry Count

- You can configure the retransmission intervals and retry count both at a global as well as a specific access point level. A global configuration applies these configuration parameters to all the access points. That is, the retransmission interval and the retry count are uniform for all 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.
- Retransmission intervals and the retry count do not apply for mesh access points.

Configuring the AP Retransmission Interval and Retry Count (GUI)

You can configure the retransmission interval and retry count for all APs globally or a specific AP.

Step 1 To configure the controller to set the retransmission interval and retry count globally using the controller GUI, follow these steps:

a) Choose **Wireless > Access Points > Global Configuration**.

b) Choose one of the following options under the AP Transmit Config Parameters section:

- **AP Retransmit Count**—Enter the number of times you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- **AP Retransmit Interval**—Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

c) Click **Apply**.

Step 2 To configure the controller to set the retransmission interval and retry count for a specific access point, follow these steps:

a) Choose **Wireless > Access Points > All APs**.

b) Click on the AP Name link for the access point on which you want to set the values.

The **All APs > Details** page appears.

c) Click the **Advanced Tab** to open the advanced parameters page.

d) Choose one of the following parameters under the AP Transmit Config Parameters section:

- **AP Retransmit Count**—Enter the number of times that you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- **AP Retransmit Interval**—Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

e) Click **Apply**.

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

You can configure the retransmission interval and retry count for all access points globally or a specific access point.

- Configure the retransmission interval and retry count for all access points globally by entering the this command:

  config ap retransmit {**interval** | **count**} *seconds* **all**

The valid range for the **interval** parameter is between 3 and 8. The valid range for the **count** parameter is between 2 and 5.

- Configure the retransmission interval and retry count for a specific access point, by entering this command:

  config ap retransmit {**interval** | **count**} *seconds Cisco_AP*

  The valid range for the **interval** parameter is between 3 and 8. The valid range for the **count** parameter is between 2 and 5.

- See the status of the configured retransmit parameters on all or specific APs by entering this command:

  show ap retransmit all

  Note Because retransmit and retry values cannot be set for access points in mesh mode, these values are displayed as N/A (not applicable).

- See the status of the configured retransmit parameters on a specific access point by entering this command:

  show ap retransmit *Cisco_AP*

CHAPTER 114

Country Codes

- Information About Configuring Country Codes, on page 819
- Restrictions for Configuring Country Codes, on page 820
- Configuring Country Codes (GUI), on page 820
- Configuring Country Codes (CLI), on page 821

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.

The following are some guidelines for configuring country codes:

- Generally, you configure one country code per controller, the one matching the physical location of the controller and its access points. However, you can configure more than one country code per Cisco WLC. Prior to Release 8.2, you could configure up to 20 country codes per Cisco WLC; from Release 8.2 onwards, you can configure up to 110 country codes per Cisco WLC. This multiple-country support enables you to manage access points in various countries from a single Cisco WLC.
- Although the controller supports different access points in different regulatory domains (countries), it requires all radios in a single access point to be configured for the same regulatory domain. For example, you should not configure a Cisco 1231 access point's 802.11b/g radio for the US (-A) regulatory domain and its 802.11a radio for the Great Britain (-E) regulatory domain. Otherwise, the controller allows only one of the access point's radios to turn on, depending on which regulatory domain you selected for the access point on the controller. Therefore, make sure that the same country code is configured for both of the access point's radios.

  For a complete list of country codes supported per product, see http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

  or

  http://www.cisco.com/c/en/us/products/collateral/wireless/access-points/product_data_sheet0900aecd80537b6a.html
- When the multiple-country feature is being used, all controllers that are going to join the same RF group must be configured with the same set of countries, configured in the same order.

- When multiple countries are configured and the RRM auto-RF feature is enabled, the RRM assigns the channels that are derived by performing a union of the allowed channels per the AP country code. The APs are assigned channels by the RRM based on their PID country code. APs are only allowed to use legal frequencies that match their PID country code. Ensure that your AP's country code is legal in the country that it is deployed.
- The country list configured on the RF group leader determines what channels the members would operate on. This list is independent of what countries have been configured on the RF group members.

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 WLC
- 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.

Restrictions for Configuring Country Codes

- APs can only operate on the channels for the countries that they are designed for.

Note If an AP was already set to a higher legal power level or is configured manually, the power level is limited only by the particular country to which that AP is assigned.

Configuring Country Codes (GUI)

Step 1 Disable the 802.11 networks as follows:

a) Choose **Wireless** > **802.11a/n/ac** > **Network**.
b) Unselect the **802.11a Network Status** check box.
c) Click **Apply**.
d) Choose **Wireless** > **802.11b/g/n** > **Network**.

e) Unselect the **802.11b/g Network Status** check box.
f) Click **Apply**.

Step 2 Choose **Wireless** > **Country** to open the Country page.

Step 3 Select the check box for each country where your access points are installed. If you selected more than one check box, a message appears indicating that RRM channels and power levels are limited to common channels and power levels.

Step 4 Click **OK** to continue or **Cancel** to cancel the operation.

Step 5 Click **Apply**.

If you selected multiple country codes in *Step 3*, each access point is assigned to a country.

Step 6 See the default country chosen for each access point and choose a different country if necessary as follows:

Note If you remove a country code from the configuration, any access points currently assigned to the deleted country reboot and when they rejoin the controller, they get re-assigned to one of the remaining countries if possible.

a) Perform one of the following:

- Leave the 802.11 networks disabled.
- Reenable the 802.11 networks and then disable only the access points for which you are configuring a country code. To disable an access point, choose **Wireless** > **Access Points** > **All APs**, click the link of the desired access point, choose **Disable** from the Status drop-down list, and click **Apply**.

b) Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.
c) Click the link for the desired access point.
d) Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

The default country for this access point appears in the Country Code drop-down list.

e) If the access point is installed in a country other than the one shown, choose the correct country from the drop-down list. The box contains only those country codes that are compatible with the regulatory domain of at least one of the access point's radios.
f) Click **Apply**.
g) Repeat these steps to assign all access points joined to the controller to a specific country.
h) Reenable any access points that you disabled in *Step a*.

Step 7 Reenable the 802.11 networks if you did not enable them in *Step 6*.

Step 8 Click **Save Configuration**.

Configuring Country Codes (CLI)

Step 1 See a list of all available country codes by entering this command:

show country supported

Step 2 Disable the 802.11 networks by entering these commands:

config 802.11a disable network

config 802.11b disable network

Step 3 Configure the country codes for the countries where your access points are installed by entering this command:

config country *code1*[*,code2,code3,...*]

If you are entering more than one country code, separate each by a comma (for example, **config country US,CA,MX**).

Step 4 Enter **Y** when prompted to confirm your decision.

Step 5 Verify your country code configuration by entering this command:

show country

Step 6 See the list of available channels for the country codes configured on your controller by entering this command:

show country channels

Step 7 Save your changes by entering this command:

save config

Step 8 See the countries to which your access points have been assigned by entering this command:

To see a summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

show ap summary

Step 9 If you entered multiple country codes in *Step 3*, follow these steps to assign each access point to a specific country:

a) Perform one of the following:

- Leave the 802.11 networks disabled.
- Reenable the 802.11 networks and then disable only the access points for which you are configuring a country code. To Reenable the networks, enter this command:

  config 802.11{**a** | **b**} **enable network**

  To disable an access point, enter this command:

  config ap disable *ap_name*

b) To assign an access point to a specific country, enter this command:

config ap country *code* {*ap_name* | **all**}

Make sure that the country code 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 run the **config ap country** *code* **all** command, the specified country code is configured on only the disabled access points. All other access points are ignored.

c) To reenable any access points that you disabled in *Step a*, enter this command:

config ap enable *ap_name*

Step 10 If you did not reenable the 802.11 networks in *Step 9*, enter these commands to reenable them now:

config 802.11{**a** | **b**} **enable network**

Step 11 Save your changes by entering this command:

save config

CHAPTER 115

Optimizing RFID Tracking on Access Points

- Optimizing RFID Tracking on Access Points, on page 825
- Optimizing RFID Tracking on Access Points (GUI), on page 825
- Optimizing RFID Tracking on Access Points (CLI), on page 826

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).

You can use the controller GUI or CLI to configure the access point for monitor mode and to then enable tracking optimization on the access point radio.

This section contains the following subsections:

Optimizing RFID Tracking on Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure monitor mode. The All APs > Details for page appears.

Step 3 From the AP Mode drop-down list, choose **Monitor**.

Step 4 Click **Apply**.

Step 5 Click **OK** when warned that the access point will be rebooted.

Step 6 Click **Save Configuration** to save your changes.

Step 7 Choose **Wireless** > **Access Points** > **Radios** > **802.11b/g/n** to open the 802.11b/g/n Radios page.

Step 8 Hover your cursor over the blue drop-down arrow for the desired access point and choose **Configure**. The 802.11b/g/n Cisco APs > Configure page appears.

Step 9 Disable the access point radio by choosing **Disable** from the Admin Status drop-down list and click **Apply**.

Step 10 Enable tracking optimization on the radio by choosing **Enable** from the Enable Tracking Optimization drop-down list.

Step 11 From the four Channel drop-down lists, choose the channels on which you want to monitor RFID tags.

Note You must configure at least one channel on which the tags will be monitored.

Step 12 Click **Apply**.

Step 13 Click **Save Configuration**.

Step 14 To reenable the access point radio, choose **Enable** from the Admin Status drop-down list and click **Apply**.

Step 15 Click **Save Configuration**.

Optimizing RFID Tracking on Access Points (CLI)

Step 1 Configure an access point for monitor mode by entering this command:

config ap mode monitor *Cisco_AP*

Step 2 When warned that the access point will be rebooted and asked if you want to continue, enter **Y**.

Step 3 Save your changes by entering this command:

save config

Step 4 Disable the access point radio by entering this command:

config 802.11b disable *Cisco_AP*

Step 5 Configure the access point to scan only the DCA channels supported by its country of operation by entering this command:

config ap monitor-mode tracking-opt *Cisco_AP*

Note To specify the exact channels to be scanned, enter the **config ap monitor-mode tracking-opt** *Cisco_AP* command in *Step 6*.

Note To disable tracking optimization for this access point, enter the **config ap monitor-mode no-optimization** *Cisco_AP* command.

Step 6 After you have entered the command in *Step 5*, you can enter this command to choose up to four specific 802.11b channels to be scanned by the access point:

config ap monitor-mode 802.11b fast-channel *Cisco_AP channel1 channel2 channel3 channel4*

Note In the United States, you can assign any value between 1 and 11 (inclusive) to the *channel* variable. Other countries support additional channels. You must assign at least one channel.

Step 7 Reenable the access point radio by entering this command:

config 802.11b enable *Cisco_AP*

Step 8 Save your changes by entering this command:

save config

Step 9 See a summary of all access points in monitor mode by entering this command:

show ap monitor-mode summary

CHAPTER 116

Configuring Probe Request Forwarding

- Probe Request Forwarding, on page 827
- Configuring Probe Request Forwarding (CLI), on page 827

Probe Request Forwarding

Probe requests are 802.11 management frames sent by clients to request information about the capabilities of SSIDs. By default, access points forward acknowledged probe requests to the controller 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 controller. The controller can use the information from unacknowledged probe requests to improve the location accuracy.

Configuring Probe Request Forwarding (CLI)

Step 1 Enable or disable the filtering of probe requests forwarded from an access point to the controller by entering this command:

config advanced probe filter {**enable** | **disable**}

- **enable** (default)—Choose this parameter to only forward acknowledged probe requests to the controller.
- **disable**—Choose this parameter to forward both acknowledged and unacknowledged probe requests to the controller.

Step 2 Limit the number of probe requests sent to the controller per client per access point radio in a given interval by entering this command:

config advanced probe limit *num_probes interval*

where

- *num_probes* is the number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
- *interval* is the probe limit interval (from 100 to 64000 milliseconds).

The default value for *num_probes* is 2 probe requests, and the default value for *interval* is 500 milliseconds.

Step 3 Enter the **save config** command to save your changes.

Step 4 See the probe request forwarding configuration by entering this command:

show advanced probe

Information similar to the following appears:

```
Probe request filtering.........................  Enabled
Probes fwd to controller per client per radio....  2
Probe request rate-limiting interval..........  500 msec
```

CHAPTER 117

Retrieving the Unique Device Identifier on Controllers and Access Points

- Retrieving the Unique Device Identifier on Controllers and Access Points, on page 829
- Retrieving the Unique Device Identifier on Controllers and Access Points (GUI), on page 829
- Retrieving the Unique Device Identifier on Controllers and Access Points (CLI), on page 830

Retrieving the Unique Device Identifier on Controllers 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.

This section contains the following subsections:

Retrieving the Unique Device Identifier on Controllers and Access Points (GUI)

Step 1 Choose **Controller** > **Inventory** to open the Inventory page.

This page shows the five data elements of the controller UDI.

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

Step 3 Click the name of the desired access point.

Step 4 Choose the **Inventory** tab to open the All APs > Details for (Inventory) page.

This page shows the inventory information for the access point.

Retrieving the Unique Device Identifier on Controllers and Access Points (CLI)

Use these commands to retrieve the UDI on controllers and access points using the controller CLI:

Procedure

- **show inventory**—Shows the UDI string of the controller.
- **show inventory ap** *ap_id*—Shows the UDI string of the access point specified.
- **show license udi**—Shows UDI values for licenses.

CHAPTER 118

Performing a Link Test

- Link Test, on page 831
- Performing a Link Test (GUI), on page 832
- Performing a Link Test (CLI), on page 832

Link Test

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 controller can also test the link quality in the access point-to-client direction. The controller 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 controller. Not only can the access point or controller 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 controller.

The controller shows these link-quality metrics for CCX link tests in both directions (out— access point to client; in— client to 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.

Note Follow the instructions in this section to perform a link test using either the GUI or the CLI.

This section contains the following subsections:

Performing a Link Test (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Step 2 Hover your cursor over the blue drop-down arrow for the desired client and choose **LinkTest**. A link test page appears.

Note You can also access this page by clicking the MAC address of the desired client and then clicking the **Link Test** button on the top of the Clients > Detail page.

This page shows the results of the CCX link test.

Note If the client and/or controller does not support CCX v4 or later releases, the controller performs a ping link test on the client instead, and a much more limited link test page appears.

Note The Link Test results of CCX clients when it fails will default to ping test results if the client is reachable.

Step 3 Click **OK** to exit the link test page.

Performing a Link Test (CLI)

Use these commands to run a link test using the controller CLI:

- Run a link test by entering this command:

  linktest *ap_mac*

  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
```

- Adjust the link-test parameters that are applicable to both the CCX link test and the ping test by entering these commands from configuration mode:

  linktest frame-size *size_of_link-test_frames*

  linktest num-of-frame *number_of_link-test_request_frames_per_test*

CHAPTER 119

Configuring Link Latency

- Link Latency, on page 835
- Restrictions for Link Latency, on page 836
- Configuring Link Latency (GUI), on page 836
- Configuring Link Latency (CLI), on page 836

Link Latency

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect and OfficeExtend access points, for which the link could be a slow or unreliable WAN connection.

The following are some guidelines for link latency:

- Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to the network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo responses received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

  Note Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

- The controller 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 controller is up or can be cleared and allowed to restart.
- You can configure link latency for a specific access point using the controller GUI or CLI or for all access points joined to the controller using the CLI.

This section contains the following subsections:

Restrictions for Link Latency

- Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

Configuring Link Latency (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure link latency.

Step 3 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 4 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Step 7 When the All APs page reappears, click the name of the access point again.

Step 8 When the All APs > Details for page reappears, choose the **Advanced** tab again. The link latency and data latency results appear below the Enable Link Latency check box:

- **Current**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Minimum**—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Maximum**—Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.

Step 9 To clear the current, minimum, and maximum link latency and data latency statistics on the controller for this access point, click **Reset Link Latency**.

Step 10 After the page refreshes and the All APs > Details for page reappears, choose the **Advanced** tab. The updated statistics appear in the Minimum and Maximum text boxes.

Configuring Link Latency (CLI)

Step 1 Enable or disable link latency for a specific access point or for all access points currently associated to the controller by entering this command:

config ap link-latency {**enable** | **disable**} {*Cisco_AP* | **all**}

The default value is disabled.

Note The **config ap link-latency** {**enable** | **disable**} **all** command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

Step 2 See the link latency results for a specific access point by entering this command:

show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
AP Link Latency.................................. Enabled
 Current Delay................................... 1 ms
 Maximum Delay................................... 1 ms
 Minimum Delay................................... 1 ms
 Last updated (based on AP Up Time)............ 0 days, 05 h 03 m 25 s
```

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 controller and back.
- **Maximum Delay**—Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Minimum Delay**—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

Step 3 Clear the current, minimum, and maximum link latency statistics on the controller for a specific access point by entering this command:

config ap link-latency reset *Cisco_AP*

Step 4 See the results of the reset by entering this command:

show ap config general *Cisco_AP*

CHAPTER 120

Configuring the TCP MSS

- TCP Adjust MSS, on page 839
- Configuring TCP Adjust MSS (GUI), on page 839
- Configuring TCP Adjust MSS (CLI), on page 840

TCP Adjust 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 controller 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.

In Release 8.5 and later releases, TCP Adjust MSS is enabled by default with a value of 1250. We recommend that you do not change this default value.

TCP Adjust MSS is supported only on APs that are in local mode or FlexConnect with centrally switched WLANs.

This section contains the following subsections:

Configuring TCP Adjust MSS (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 Under **TCP MSS**, check the **Global TCP Adjust MSS** check box and set the MSS for all APs that are associated with the controller.

The valid ranges are:

- For IPv4, TCP must be between 536 and 1363 bytes.
- For IPv6, TCP must be between 1220 and 1331 bytes.

Note Any TCP Adjust MSS value that is below 1220 and above 1331 will not be effective for CAPWAPv6 AP.

Configuring TCP Adjust MSS (CLI)

Step 1 Enable or disable the TCP Adjust MSS on a particular access point or on all access points by entering this command:

config ap tcp-mss-adjust {**enable**|**disable**} {*Cisco_AP* | *all*} *size*

where the *size* parameter is a value between 536 and 1363 bytes for IPv4 and between 1220 and 1331 for IPv6. The default value varies for different clients.

The valid ranges are:

- For IPv4, TCP must be between 536 and 1363 bytes.
- For IPv6, TCP must be between 1220 and 1331 bytes.

Note Any TCP Adjust MSS value that is below 1220 and above 1331 will not be effective for CAPWAPv6 AP.

Step 2 Save your changes by entering this command:

save config

Step 3 See the current TCP Adjust MSS setting for a particular access point or all access points by entering this command:

show ap tcp-mss-adjust {*Cisco_AP* | **all**}

Information similar to the following appears:

```
AP Name              TCP State  MSS Size
------------------   --------   -------
AP58AC.78DC.A810     disabled   -
APa89d.21b2.2688     enabled    1250
AP00FE.C82D.DE80     disabled   -
```

CHAPTER 121

Configuring Power Over Ethernet

- Information About Configuring Power over Ethernet, on page 841
- Configuring Power over Ethernet (GUI), on page 843
- Configuring Power over Ethernet (CLI), on page 844

Information About Configuring Power over Ethernet

When an access point that has been converted to lightweight mode (such as an AP1131 or AP1242) or a 1250 series access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch, you need to configure Power over Ethernet (PoE), also known as *inline power*.

The dual-radio 1250 series access points can operate in four different modes when powered using PoE:

- 20.0 W (Full Power)—This mode is equivalent to using a power injector or an AC/DC adapter.
- 16.8 W—Both transmitters are used but at reduced power. Legacy data rates are not affected, but the M0 to M15 data rates are reduced in the 2.4-GHz band. Throughput should be minimally impacted because all data rates are still enabled. The range is affected because of the lower transmit power. All receivers remain enabled.
- 15.4 W—Only a single transmitter is enabled. Legacy data rates and M0 to M7 rates are minimally affected. M8 to M15 rates are disabled because they require both transmitters. Throughput is better than that received with legacy access points but less than the 20 and 16.8 W power modes.
- 11.0 W (Low Power)—The access point runs, but both radios are disabled.

The following are some guidelines for Power over Ethernet:

- When a dual-radio 1250 series access point is powered using 15.4-W PoE, it cannot operate at full functionality, which requires 20 W. The access point can operate with dual radios on 15.4-W PoE, but performance is reduced in terms of throughput and range. If full functionality is required on 15.4 W, you can remove one of the radios from the 1250 series access point chassis or disable it in controller software release 6.0 or later releases so that the other radio can operate in full 802.11n mode. After the access point radio is administratively disabled, the access point must be rebooted for the change to take effect. The access point must also be rebooted after you reenable the radio to put it into reduced throughput mode.

  These modes provide the flexibility of running the 1250 series access points with the available wired infrastructure to obtain the desired level of performance. With enhanced PoE switches (such as the Cisco Catalyst 3750-E Series Switches), the 1250 series access points can provide maximum features and

functionality with a minimum total cost of ownership. Alternatively, if you decide to power the access point with the existing PoE (802.3af) switches, the access point chooses the appropriate mode of operation based on whether it has one radio or two.

Note For more information about Cisco PoE switches, see http://www.cisco.com/c/en/us/products/switches/epoe.html

The table below shows the maximum transmit power settings for 1250 series access points using PoE.

Table 27: Maximum Transmit Power Settings for 1250 Series Access Points Using PoE

Radio Band	Data Rates	Number of Transmitters	Cyclic Shift Diversity (CSD)	Maximum Transmit Power (dBm)		
				802.3af Mode (15.4 W)	ePoE Power Optimized Mode (16.8 W)	ePoE Mode (20 W)
2.4 GHz	802.11b	1	—	20	20	20
	802.11g	1	—	17	17	17
	802.11n MCS 0-7	1 2	Disabled Enabled (default)	17 Disabled	17 14 (11 per Tx)	17 20 (17 per Tx)
	802.11n MCS 8-15	2	—	Disabled	14 (11 per Tx)	20 (17 per Tx)
5 GHz	802.11a	1	—	17	17	17
	802.11n MCS 0-7	1 2	Disabled Enabled (default)	17 Disabled	17 20 (17 per Tx)	17 20 (17 per Tx)
	802.11n MCS 8-15	2	—	Disabled	20 (17 per Tx)	20 (17 per Tx)

[5] Maximum transmit power varies by channel and according to individual country regulations. See the product documentation for specific details.

- When powered with a non-Cisco standard PoE switch, the 1250 series access point operates under 15.4 Watts. Even if the non-Cisco switch or midspan device is capable of providing higher power, the access point does not operate in enhanced PoE mode.

Configuring Power over Ethernet (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** and then the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

The **PoE Status** text box shows the power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). This text box is not configurable. The controller auto-detects the access point's power source and displays the power level here.

Note This text box applies only to 1250 series access points that are powered using PoE. There are two other ways to determine if the access point is operating at a lower power level. First, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section on the 802.11a/n/ac (or 802.11b/g/n) **Cisco APs > Configure** page. Second, the "PoE Status: degraded operation" message appears in the controller's trap log on the Trap Logs page.

Step 3 Perform one of the following:

- Check the **Pre-standard 802.3af switches** check box if the access point is being powered by a high-power 802.3af Cisco switch. This switch provides more than the traditional 6 Watts of power but do not support the intelligent power management (IPM) feature.
- Uncheck the **Pre-standard 802.3af switches** check box if power is being provided by a power injector. This is the default value.

Step 4 Check the **Power Injector State** check box if the attached switch does not support IPM and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.

Step 5 If you selected the Power Injector State check box in the previous step, the Power Injector Selection and Injector Switch MAC Address parameters appear. The Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed. Choose one of these options from the drop-down list to specify the desired level of protection:

- **Installed**—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

  If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address text box. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address text box blank.

  Note Each time an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override**—This option allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option 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 advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

Step 6 Click **Apply**.

Step 7 If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, follow these steps:

a) Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n**//ac or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.
b) Hover your cursor over the blue drop-down arrow for the radio that you want to disable and choose **Configure**.
c) On the 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page, choose **Disable** from the **Admin Status** drop-down list.
d) Click **Apply**.
e) Manually reset the access point in order for the change to take effect.

Step 8 Click **Save Configuration**.

Configuring Power over Ethernet (CLI)

Use these commands to configure and See PoE settings using the controller CLI:

- If your network contains any older Cisco 6-W switches that could be accidentally overloaded if connected directly to a 12-W access point, enter this command:

  config ap power injector enable {*Cisco_AP* | **all**} **installed**

  The access point remembers that a power injector is connected to this particular switch port. If you relocate the access point, you must reissue this command after the presence of a new power injector is verified.

  Note Ensure CDP is enabled before entering this command. Otherwise, this command will fail.

- Remove the safety checks and allow the access point to be connected to any switch port by entering this command:

  config ap power injector enable {*Cisco_AP* | **all**} **override**

  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.

- If you know the MAC address of the connected switch port and do not want to automatically detect it using the installed option, enter this command:

  config ap power injector enable {*Cisco_AP* | **all**} *switch_port_mac_address*

- If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, enter this command:

  config {**802.11a** | **802.11b**} **disable** *Cisco_AP*

Note You must manually reset the access point in order for the change to take effect.

- See the PoE settings for a specific access point by entering this command:

  show ap config general *Cisco_AP*

  Information similar to the following appears:

```
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)
...
```

  The Power Type/Mode text box shows “degraded mode” if the access point is not operating at full power.

- See the controller’s trap log by entering this command:

  show traplog

  If the access point is not operating at full power, the trap contains “PoE Status: degraded operation.”

- You can power an access point by a Cisco prestandard 15-W switch with Power over Ethernet (PoE) by entering this command:

  config ap power pre-standard {**enable** | **disable**} {**all** | *Cisco_AP*}

  A Cisco prestandard 15-W switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-W switches are available:

  - WS-C3550, WS-C3560, WS-C3750
  - C1880
  - 2600, 2610, 2611, 2621, 2650, 2651
  - 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
  - 2811, 2821, 2851
  - 3631-telco, 3620, 3640, 3660
  - 3725, 3745
  - 3825, 3845

  The **enable** version of this command is required for full functionality when the access point is powered by a Cisco prestandard 15-W switch. It is safe to use if the access point is powered by either an IPM switch or a power injector or if the access point is not using one of the 15-W switches listed above.

  You might need this command if your radio operational status is "Down" when you expect it to be "Up." Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable
```

```
 to
verify sufficient in-line power. Radio slot 0 disabled.
```

CHAPTER 122

Viewing Clients

- Viewing Clients (GUI), on page 847
- Viewing Clients (CLI), on page 848

Viewing Clients (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

This page lists all of the clients that are associated to the controller's access points. It provides the following information for each client:

- The MAC address of the client
- The name of the access point to which the client is associated
- The name of the WLAN used by the client
- The type of client (802.11a, 802.11ac, 802.11b, 802.11g, or 802.11n)

  Note If the 802.11n client associates to an 802.11a radio that has 802.11n enabled, then the client type shows as 802.11a/n/ac. If the 802.11n client associates to an 802.11b/g radio with 802.11n enabled, then the client type shows as 802.11b/n.

- The status of the client connection
- The authorization status of the client
- The port number of the access point to which the client is associated
- An indication of whether the client is a WGB

  Note If you want to remove or disable a client, hover your cursor over the blue drop-down arrow for that client and choose **Remove** or **Disable**, respectively. If you want to test the connection between the client and the access point, hover your cursor over the blue drop-down arrow for that client and choose **Link Test**.

Step 2 Create a filter to display only clients that meet certain criteria (such as the MAC address, status, or radio type) as follows:

a) Click **Change Filter** to open the **Search Clients** dialog box.

b) Select one or more of the following check boxes to specify the criteria used when displaying clients:

- **MAC Address**—Enter a client MAC address.

  Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- **AP Name**—Enter the name of an access point.
- **WLAN Profile**—Choose one of the available WLAN profiles from the drop-down list.
- **Status**—Select the **Associated**, **Authenticated**, **Excluded**, and/or **Idle** check boxes.
- **Radio Type**—Choose **802.11a**, **802.11b**, **802.11g**, **802.11an**, **802.11bn** or **Mobile**.
- **WGB**—Enter the WGB clients associated to the controller's access points.

c) Click **Apply**. The Current Filter parameter at the top of the Clients page shows the filters that are currently applied.

Note If you want to remove the filters and display the entire client list, click **Clear Filter**.

Step 3 Click the MAC address of the client to view detailed information for a specific client. The Clients > Detail page appears.

This page shows the following information:

- The general properties of the client
- The security settings of the client
- The QoS properties of the client
- Client statistics
- The properties of the access point to which the client is associated

Viewing Clients (CLI)

Use these commands to view client information:

- See the clients associated to a specific access point by entering this command:

  show client ap {**802.11a** | **802.11b**} *Cisco_AP*

- See a summary of the clients associated to the controller's access points by entering this command:

  show client summary

- See detailed information for a specific client by entering this command:

  show client detail *client_mac*

- See detailed information of the first eight clients that are in RUN state, associated to the controller's access points by entering this command:

  show client username*username*

CHAPTER 123

Configuring LED States for Access Points

- Configuring LED States, on page 849
- Configuring Flashing LEDs, on page 850

Configuring LED States

LED States for Access Points

In a wireless LAN network where there are a large number of access points, it is difficult to locate a specific access point associated with the controller. You can configure the controller to set the LED state of an access point so that it blinks and the access point can be located. This configuration can be done in the wireless network on a global as well as per-AP level.

The LED state configuration at the global level takes precedence over the AP level.

This section contains the following subsections:

Configuring the LED State for Access Points in a Network Globally (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 Select the **LED state** check box.

Step 3 Choose **Enable** from the drop-down list adjacent to this check box.

Step 4 Click **Apply**.

Configuring the LED State for Access Point in a Network Globally (CLI)

Procedure

- Set the LED state for all access points associated with a controller by entering this command:

  config ap led-state {**enable** | **disable**} **all**

Configuring LED State on a Specific Access Point (GUI)

Step 1 Choose **Wireless > Access Points > All APs** and then the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 3 Select the **LED state** check box.

Step 4 Choose **Enable** from the drop-down list adjacent to this text box.

Step 5 Click **Apply**.

Configuring LED State on a Specific Access Point (CLI)

Step 1 Determine the ID of the access point for which you want to configure the LED state by entering this command:

show ap summary

Step 2 Configure the LED state by entering the following command:

config ap led-state {**enable** | **disable**} *Cisco_AP*

Configuring Flashing LEDs

Information About Configuring Flashing LEDs

Controller software enables you to flash the LEDs on an access point in order to locate it. All Cisco IOS lightweight access points support this feature.

Configuring Flashing LEDs (CLI)

Use these commands to configure LED flashing from the privileged EXEC mode of the controller:

1. Configure the LED flash for an AP by entering this command:

   config ap led-state flash {*seconds* | **indefinite** | **disable**} {*Cisco_AP*}

   The valid LED flash duration for the AP is 1 to 3600 seconds. You can also configure the LED to flash indefinitely or to stop flashing the LED.

2. Disable LED flash for an AP after enabling it by entering this command:

   config ap led-state flash disable *Cisco_AP*

   The command disables LED flashing immediately. For example, if you run the previous command (with the *seconds* parameter set to 60 seconds) and then disable LED flashing after only 20 seconds, the access point's LEDs stop flashing immediately.

3. Save your changes by entering this command:

   save config

4. Check the status of LED flash for the AP by entering this command:

   show ap led-flash *Cisco_AP*

   Information similar to the following appears:

```
(Cisco Controller)> show ap led-flash AP1040_46:b9
Led Flash..................................... Enabled for 450 secs, 425 secs left
```

Note The output of these commands is sent only to the controller console, regardless of whether the commands were entered on the console or in a TELNET/SSH CLI session.

CHAPTER 124

Configuring Access Points with Dual-Band Radios

- Configuring Access Points with Dual-Band Radios (GUI), on page 853
- Configuring Access Points with Dual-Band Radios (CLI), on page 853

Configuring Access Points with Dual-Band Radios (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Radios** > **Dual-Band Radios** to open the Dual-Band Radios page.

Step 2 Hover your cursor over the blue drop-down arrow of the AP and click **Configure**.

Step 3 Configure the Admin Status.

Step 4 Configure CleanAir Admin Status as one of the following:

- Enable
- Disable
- 5 GHz Only
- 2.4 GHz Only

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

What to do next

You can monitor the access points with dual-band radios by navigating to **Monitor** > **Access Points** > **Radios** > **Dual-Band Radios**.

Configuring Access Points with Dual-Band Radios (CLI)

Procedure

- Configure an access point with dual-band radios by entering this command:

config 802.11-abgn {**enable** | **disable**} *ap-name*

- Configure the CleanAir features for an access point with dual-band radios by entering this command:

  config 802.11-abgn cleanair {**enable** | **disable**} *ap-name* **band** *2.4-or-5-GHz*

PART VII

Radio Resource Management

- Configuring RRM, on page 857
- Configuring RRM Neighbor Discovery Packets, on page 879
- Configuring RF Groups, on page 881
- Overriding RRM, on page 889
- Configuring CCX Radio Management Features, on page 897

CHAPTER 125

Configuring RRM

- Information about Radio Resource Management, on page 857
- Restrictions for Configuring RRM, on page 862
- Configuring the RF Group Mode (GUI), on page 863
- Configuring the RF Group Mode (CLI), on page 863
- Configuring Transmit Power Control (GUI), on page 864
- Configuring Off-Channel Scanning Defer, on page 866
- Configuring RRM (CLI), on page 873
- Viewing RRM Settings (CLI), on page 877
- Debug RRM Issues (CLI), on page 877

Information about Radio Resource Management

The Radio Resource Management (RRM) software embedded in the Cisco Wireless LAN Controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables Cisco WLCs 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.

Using this information, RRM can periodically reconfigure the 802.11 RF network for best efficiency. To do this, RRM performs these functions:

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

Radio Resource Monitoring

RRM automatically detects and configures new Cisco WLCs 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 simultaneously scan all valid 802.11a/b/g channels for the country of operation as well as for channels available in other locations. The access points 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 (in the last 100 ms), the access points defer off-channel measurements.

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.

Note When there are numerous rogue access points in the network, the chance of detecting rogues on channels 157 or 161 by a FlexConnect or local mode access point is small. In such cases, the monitor mode AP can be used for rogue detection.

Transmit Power Control

The Cisco WLC dynamically controls access point transmit power based on real-time wireless LAN conditions. You can choose between two versions of transmit power control: TPCv1 and TPCv2. With TPCv1, typically, power can be kept low to gain extra capacity and reduce interference. With TPCv2, transmit power is dynamically adjusted with the goal of minimum interference. TPCv2 is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

The Transmit Power Control (TPC) algorithm 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 the surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve the required coverage levels while avoiding channel interference between access points.

These documents provide more information on Transmit Power Control values for the following access points:

Cisco Aironet 3500 Series http://www.cisco.com/c/en/us/support/wireless/aironet-3500-series/products-installation-guides-list.html

Cisco Aironet 3700 Series http://www.cisco.com/c/en/us/support/wireless/aironet-3700-series/products-installation-guides-list.html

Cisco Aironet 700 Series http://www.cisco.com/c/en/us/support/wireless/aironet-700-series/products-installation-guides-list.html

Cisco Aironet 1530 Series http://www.cisco.com/c/en/us/support/wireless/aironet-1530-series/products-installation-guides-list.html

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 the access points must be mounted in a central hallway, placing the access points close together, but requiring coverage 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 the 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 fields in the **Tx Power Control** window. 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 controller 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, no access point will 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 an e-mail in a café affects the performance of the access point in a neighboring business. Even though these are separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Controllers can dynamically allocate access point channel assignments to avoid conflict and 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 controller'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 simultaneously use 11 or 54 Mbps. By effectively reassigning channels, the controller keeps adjacent channels that are separated.

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

Note Channel change does not require you to shut down the radio.

The controller 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 controller 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 a part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all the 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 controller. Using the RRM algorithms, the controller 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 controller 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 controller may choose to avoid this channel. In huge deployments in which all nonoverlapping channels are occupied, the controller 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 controller can then assign channels to improve the access point that has performed the worst. The load is taken into account when changing the channel structure to minimize the impact on the clients that are 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 *Load and utilization* parameter is disabled by default.

The controller 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 80MHz channels are not supported by DCA.

The RRM startup mode is invoked in the following conditions:

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

You can trigger the RRM startup mode from the CLI.

The 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.

Note DCA algorithm interval is set to 1 hour, but DCA algorithm always runs in default interval of 10 min, channel allocation occurs at 10-min intervals for the first 10 cycles, and channel changes occur as per the DCA algorithm every 10 min. After that the DCA algorithm goes back to the configured time interval. This is common for both DCA interval and anchor time because it follows the steady state.

Note If Dynamic Channel Assignment (DCA)/Transmit Power Control (TPC) is turned off on the RF group member, and auto is set on RF group leader, the channel or TX power on a member gets changed as per the algorithm that is run on the RF group leader.

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 controller. 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 controller discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the controller mitigates the coverage hole by increasing the transmit power level for that specific access point. The controller 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.

Benefits of RRM

RRM produces a network with optimal capacity, performance, and reliability. It frees you from having to continually monitor the network for noise and interference problems, which can be transient and difficult to troubleshoot. RRM ensures that clients enjoy a seamless, trouble-free connection throughout the Cisco unified wireless network.

RRM uses separate monitoring and control for each deployed network: 802.11a and 802.11b/g. The RRM algorithms run separately for each radio type (802.11a and 802.11b/g). RRM uses both measurements and algorithms. RRM measurements can be adjusted using monitor intervals, but they cannot be disabled. RRM algorithms are enabled automatically but can be disabled by statically configuring channel and power assignment. The RRM algorithms run at a specified updated interval, which is 600 seconds by default.

RRM NDP and RF Grouping

The Cisco Neighbor Discovery Packet (NDP) is the fundamental tool for RRM and other wireless applications that provides information about the neighbor radio information. You can configure the controller to encrypt neighbor discovery packets.

An RF group can only be formed between controllers that have the same encryption mechanism. That is, an access point associated to a controller that is encrypted can not be neighbors with an access point associated to a controller that is not encrypted. The two controllers and their access points will not recognize each other as neighbors and cannot form an RF group. It is possible to assign two controllers in a static RF group configuration that has mismatched encryption settings. In this case, the two controllers do not function as a single RF group because the access points belonging to the mismatched controllers do not recognize one another as neighbors in the group.

Guidelines

- This feature enables you to be compliant with the PCI specifications.
- An RF group can only be formed between controllers that have the same encryption mechanism. That is, an access point associated to a controller that is encrypted can not be neighbors with an access point associated to a controller that is not encrypted. The two controllers and their access points will not recognize each other as neighbors and cannot form an RF group. It is possible to assign two controllers in a static RF group configuration that has mismatched encryption settings. In this case, the two controllers do not function as a single RF group because the access points belonging to the mismatched controllers do not recognize one another as neighbors in the group.
- Ensure that the Cisco Wave 2 APs have an SSID enabled for the APs to send NDP packets. If only the AP radios are enabled but not SSID, then the APs cannot send NDP packets and thus RRM does not work as expected.

Information About Configuring RRM

The controller's preconfigured RRM settings are optimized for most deployments. However, you can modify the controller's RRM configuration parameters at any time through either the GUI or the CLI.

You can configure these parameters on controllers that are part of an RF group or on controllers that are not part of an RF group.

The RRM parameters should be set to the same values on every controller in an RF group. The RF group leader can change as a result of controller reboots or depending on which radios hear each other. If the RRM parameters are not identical for all RF group members, varying results can occur when the group leader changes.

Using the controller GUI, you can configure the following RRM parameters: RF group mode, transmit power control, dynamic channel assignment, coverage hole detection, profile thresholds, monitoring channels, and monitor intervals.

Restrictions for Configuring RRM

- The OEAP 600 series access points do not support RRM. The radios for the 600 series OEAP access points are controlled through the local GUI of the 600 series access points and not through the Cisco WLC. Attempting to control the spectrum channel or power, or disabling the radios through the Cisco WLC will fail to have any effect on the 600 series OEAP.

Configuring the RF Group Mode (GUI)

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

Step 2 From the **Group Mode** drop-down list, select the mode 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 This mode does not support IPv6 based configuration.

- leader—Sets the RF group selection to static mode, and sets this Cisco WLC as the group leader.

  Note Leader supports static IPv6 address.

  Note If a RF group member is configured using IPv4 address, then IPv4 address is used to communicate with the leader. The same is applicable for a RF group member configured using IPv6 too.

- off—Sets the RF group selection off. Every Cisco WLC optimizes its own access point parameters.

  Note A configured static leader cannot become a member of another Cisco WLC until its mode is set to “auto”.

  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 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 RF Group Members section as follows:

a. In the Cisco WLC Name text box, enter the Cisco WLC that you want to add as a member to this group.

b. In the **IP Address (IPv4/IPv6)** text box, enter the IPv4/IPv6 address of the RF Group Member.

c. Click **Add Member** 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 the RF Group Mode (CLI)

Step 1 Configure the RF Grouping mode by entering this command:

config advanced { **802.11a** | **802.11b**} **group-mode** {*auto* | *leader* | *off* | *restart*}

- auto—Sets the RF group selection to automatic update mode.
- leader—Sets the RF group selection to static mode, and sets this Cisco WLC as the group leader.

  Note If a group member is configured with IPv4 address, then IPv4 address is used to communicate with a leader and vice versa with IPv6 also.

- off—Sets the RF group selection off. Every Cisco WLC optimizes its own access point parameters.
- restart—Restarts the RF group selection.

  Note A configured static leader cannot become a member of another Cisco WLC until its mode is set to “auto”.

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

Step 2 Add or remove a Cisco WLC as a static member of the RF group (if the mode is set to “leader”) by entering the these commands:

- **config advanced** {**802.11a** | **802.11b**} **group-member add** *controller-name ipv4-or-ipv6-address*
- **config advanced** {**802.11a** | **802.11b**} *group-member* **remove** *controller-name ipv4-or-ipv6-address*

Note You can add RF Group Members using either IPv4 or IPv6 address.

Step 3 See RF grouping status by entering this command:

show advanced {**802.11a** | **802.11b**} *group*

Configuring Transmit Power Control (GUI)

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

Step 2 Choose the Transmit Power Control version from the following options:

- Interference Optimal Mode (TPCv2)—For scenarios where voice calls are extensively used. Transmit power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

  Note We recommend that you use TCPv2 only in cases where RF issues cannot be resolved by using TCPv1. Please evaluate and test the use of TPCv2 with the assistance of Cisco Services.

- Coverage Optimal Mode (TPCv1)—(Default) 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 drop-down 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 **Invoke Power Update Now**.

  Note The Cisco WLC does not evaluate and update the transmit power immediately after you click **Invoke Power Update Now**. 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.

  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 and –67 dBm for TPCv2, 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 Off-Channel Scanning Defer

Off-Channel Scanning Deferral

A lightweight access point, in normal operational conditions, periodically goes off-channel and scans another channel. This is in order to perform RRM operations such as the following:

- Transmitting and receiving Neighbor Discovery Protocol (NDP) packets with other APs.
- Detecting rogue APs and clients.
- Measuring noise and interference.

During the off-channel period, which normally is about 70 milliseconds, the AP is unable to transmit or receive data on its serving channel. Therefore, there is a slight impact on its performance and some client transmissions might be dropped.

While the AP is sending and receiving important data, it is possible to configure off-channel scanning deferral so that the AP does not go off-channel and its normal operation is not impacted. You can configure off-channel scanning deferral on a per-WLAN basis, per WMM UP class basis, with a specified time threshold in milliseconds. If the AP sends or receives, on a particular WLAN, a data frame marked with the given UP class within the specified threshold, the AP defers its next RRM off-channel scan. For example, by default, off-channel scanning deferral is enabled for UP classes 4, 5, and 6, with a time threshold of 100 millseconds. Therefore, when RRM is about to perform an off-channel scan, a data frame marked with UP 4, 5, or 6 is received within the last 100 milliseconds, RRM defers going off-channel. The AP radio does not go off-channel when a voice call sending and receiving audio samples are marked as UP class 6 for every active 20 milliseconds.

Off-channel scanning deferral does come with a tradeoff. Off-channel scanning can impact throughput by 2 percent or more, depending on the configuration, traffic patterns, and so on. Throughput can be slightly improved if you enable off-channel scanning deferral for all traffic classes and increase the time threshold. However, by not going off-channel, RRM can fail to identify AP neighbors and rogues, resulting in negative impact to security, DCA, TPC, and 802.11k messages.

We recommend that you do not change the default off-channel scanning deferral settings.

Configuring Off-Channel Scanning Defer for WLANs

Configuring Off-Channel Scanning Deferral for a WLAN (GUI)

Step 1 Choose **WLANs** to open the **WLANs** page.

Step 2 Click the WLAN ID.

Step 3 Choose the **Advanced** tab from the **WLANs > Edit** page.

Step 4 In the **Off Channel Scanning Defer** section, set the **Scan Defer Priority** by clicking on the priority argument.

Step 5 Set the time in milliseconds in the **Scan Defer Time** field.

Valid values are between 0 and 60000 milliseconds; the default value is 100 milliseconds. If you sent the time to 0, the scan deferral does not happen.

The scan defer time is common for all priorities on the same WLAN and the scan is deferred if a packet is transmitted or received in any one of the defer priorities.

Step 6 Save the configuration.

Configuring Off Channel Scanning Deferral for a WLAN (CLI)

Step 1 Assign a defer-priority for the channel scan by entering this command:

config wlan channel-scan defer-priority *priority-value* {**enable** | **disable**} *wlan-id*

Valid priority value is betweeen 0 and 7 (this value should be set to 6 on the client and on the WLAN).

Use this command to configure the amount of time that scanning will be deferred following an UP packet in the queue.

Step 2 Assign the channel scan defer time (in milliseconds) by entering this command:

config wlan channel-scan defer-time *time-in-msecswlan-id*

The time value is in miliseconds (ms) and the valid range is between 0 and 60000 ms (60 seconds); the default value is 100 ms. This setting should match the requirements of the equipment on your WLAN. If you sent the time to 0, the scan deferral does not happen.

The scan defer time is common for all priorities on the same WLAN and the scan is deferred if a packet is transmitted or received in any one of the defer priorities.

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 controller 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 **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the **Global Parameters** page.
b) Uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box.
c) Click **Apply**.

Step 2 Choose **Wireless** > **802.11a/n/ac** or **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 controller's DCA mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the channel assignment for all joined access points. This is the default value.

- **Freeze**—Causes the controller to evaluate and update the channel assignment for all joined access points, if necessary, but only when you click **Invoke Channel Update Once**.

  Note The controller does not evaluate and update the channel assignment immediately after you click **Invoke Channel Update Once**. 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, which is the default value. 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.

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.

Note If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

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 Check the **Avoid Foreign AP Interference** check box to cause the controller's RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or uncheck it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is selected.

Step 7 Check the **Avoid Cisco AP Load** check box to cause the controller's RRM algorithms to consider 802.11 traffic from APs in your wireless network when assigning channels, or uncheck it to disable this feature. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. The default value is unselected.

Step 8 Check the **Avoid Non-802.11a (802.11b) Noise** check box to cause the controller's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or uncheck it to disable this feature. For example, RRM may have access points avoid channels with significant interference from nonaccess point sources, such as microwave ovens. The default value is selected.

Step 9 Check the **Avoid Persistent Non-WiFi Interference** check box to configure the controller to stop ignoring persistent non-Wi-Fi interference in new channel calculation. The persistent non-Wi-Fi interference is considered during the metric calculation for channels.

Step 10 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 table below.

Table 28: DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB

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

Step 11 For 802.11a/n/ac networks only, choose one of the following channel width options to specify the channel bandwidth supported for all 802.11n radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth.
- **40 MHz**—The 40-MHz channel bandwidth

Note If you choose 40 MHz, be sure to choose at least two adjacent channels from the DCA Channel List in *Step 13* (for example, a primary channel of 36 and an extension channel of 40). If you choose only one channel, that channel is not used for 40-MHz channel width.

Note If you choose 40 MHz, you can also configure the primary and extension channels used by individual access points.

Note To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode on the 802.11a/n Cisco APs > Configure page. if you then change the static RF channel assignment method to WLC Controlled on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

Note If you choose 40 MHz on the 802.11a radio, you cannot pair channels 116, 140, and 165 with any other channels.

- **80 MHz**—The 80-MHz bandwidth for the 802.11ac radios.
- **160 MHz**—The 160-MHz bandwidth for 802.11ac radios.
- **best**—It selects the best bandwidth suitable. This option is enabled for the 5-GHz radios only.

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.
- Last Auto Channel Assignment—The last time RRM evaluated the current channel assignments.

Step 12 Select the **Avoid check for non-DFS** channel to enable the controller to avoid checks for non-DFS channels. DCA configuration requires at least one non-DFS channel in the list. In the EU countries, outdoor deployments do not support non-DFS channels. Customers based in EU or regions with similar regulations must enable this option or at least have one non-DFS channel in the DCA list even if the channel is not supported by the APs.

Note This parameter is applicable only for deployments having outdoor access points such as 1522 and 1524.

Step 13 In the **DCA Channel List** area, the **DCA Channels** field shows the channels that are currently selected. To choose a channel, check its check box in the **Select** column. To exclude a channel, uncheck 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, 190, 196 802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

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

Note These extended UNII-2 channels in the 802.11a band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. If you have Cisco Aironet 1520 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, check the **Extended UNII-2 Channels** check box.

Step 14 If you are using Cisco Aironet 1520 series mesh access points in your network, you need to set the 4.9-GHz channels in the 802.11a band on which they are to operate. The 4.9-GHz band is for public safety client access traffic only. To choose a 4.9-GHz channel, check its check box in the **Select** column. To exclude a channel, uncheck its check box.

The ranges are as follows: 802.11a—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26

The defaults are as follows: 802.11a—20, 26

Step 15 Click **Apply**.

Step 16 Reenable the 802.11 networks as follows:

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

b. Check the **802.11a** (or **802.11b/g**) **Network Status** check box.

c. Click **Apply**.

Step 17 Click **Save Configuration**.

Note To see why the DCA algorithm changed channels, choose **Monitor** and then choose **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

Configuring Coverage Hole Detection (GUI)

Step 1 Disable the 802.11 network as follows:

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

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

c) Click **Apply**.

Step 2 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **RRM** > **Coverage** to open the 802.11a/ac (or 802.11b/g/n) > RRM > 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 –75 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 a 90-second period. 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 **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) **Global Parameters** page.
b) Select the **802.11a** (or **802.11b/g/n**) **Network Status** check box.
c) Click **Apply**.

Step 10 Click **Save Configuration**.

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

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **RRM** > **General** to open the 802.11a/n/ac (or 802.11b/g/n) > 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. Lightweight access points send an SNMP trap (or an alert) to the Cisco WLC when the 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 200, 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%.

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.

Note Neighbor Discovery Protocol (NDP) request is sent only on Dynamic Channel Assignment (DCA) channels.

Step 4 Configure monitor intervals as follows:

a. In the **Channel Scan Interval** 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 is 60 seconds for 802.11a radios and 180 seconds for the 802.11b/g radios.

Note If your Cisco WLC supports only OfficeExtend access points, we recommend that you set the channel scan interval to 1800 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

b. In the **Neighbor Packet Frequency** 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 your Cisco WLC supports only OfficeExtend access points, we recommend that you set the neighbor packet frequency to 600 seconds for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 60 to 3600 seconds can be used.

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 RRM (CLI)

Step 1 Disable the 802.11 network by entering this command:

config {**802.11a** | **802.11b**} **disable network**

Step 2 Choose the Transmit Power Control version by entering this command:

config advanced {**802.11a** | **802.11b**} **tpc-version** {**1** | **2**}

where:

- TPCv1: Coverage-optimal—(Default) Offers strong signal coverage and stability with negligent intercell interferences and sticky client syndrome.
- TPCv2: Interference-optimal—For scenarios where voice calls are extensively used. Tx power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there can be higher roaming delays and coverage hole incidents.

Step 3 Perform one of the following to configure transmit power control:

- Have RRM automatically set the transmit power for all 802.11 radios at periodic intervals by entering this command:

  config {**802.11a** | **802.11b**} **txPower global auto**

- Have RRM automatically reset the transmit power for all 802.11a or 802.11b/g radios one time by entering this command:

  config {**802.11a** | **802.11b**} **txPower global once**

- Configure the transmit power range that overrides the Transmit Power Control algorithm, use this command to enter the maximum and minimum transmit power used by RRM:

  config {**802.11a** | **802.11b**} **txPower global** {**max** | **min**} *txpower*

  where *txpower* is a value from –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 to exceed this transmit power (whether the maximum is set at RRM startup, 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.

- Manually change the default transmit power setting by entering this command:

  config advanced {**802.11a** | **802.11b**} {**tpcv1-thresh** | **tpcv2-thresh**} *threshold*

  where *threshold* is a value from –80 to –50 dBm. Increasing this value causes the access points to operate at higher transmit power rates. 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 in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients may have difficulty processing a large number of BSSIDs or a high beacon rate and may exhibit problematic behavior with the default threshold.

- Configure the Transmit Power Control Version 2 on a per-channel basis by entering this command:

config advanced {**802.11a** | **802.11b**} **tpcv2-per-chan** {**enable** | **disable**}

Step 4 Perform one of the following to configure dynamic channel assignment (DCA):

- Have RRM automatically configure all 802.11 channels based on availability and interference by entering this command:

  config {**802.11a** | **802.11b**} **channel global auto**

- Have RRM automatically reconfigure all 802.11 channels one time based on availability and interference by entering this command:

  config {**802.11a** | **802.11b**} **channel global once**

- Disable RRM and set all channels to their default values by entering this command:

  config {**802.11a** | **802.11b**} **channel global off**

- Restart aggressive DCA cycle by entering this command:

  config {**802.11a** | **802.11b**} **channel global restart**

- To specify the channel set used for DCA by entering this command:

  config advanced {**802.11a** | **802.11b**} **channel** {**add** | **delete**} *channel_number*

  You can enter only one channel number per command. This command 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 5 Configure additional DCA parameters by entering these commands:

- **config advanced** {**802.11a** | **802.11b**} **channel dca anchor-time** *value*—Specifies the time of day when the DCA algorithm is to start. value is a number between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.
- **config advanced** {**802.11a** | **802.11b**} **channel dca interval** *value*—Specifies how often the DCA algorithm is allowed to run. value is one of the following: 1, 2, 3, 4, 6, 8, 12, or 24 hours or 0, which is the default value of 10 minutes (or 600 seconds).

  Note If your Cisco WLC supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

- **config advanced** {**802.11a** | **802.11b**} **channel dca sensitivity** {**low** | **medium** | **high**}—Specifies how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channel.
  - **low** means that the DCA algorithm is not particularly sensitive to environmental changes.
  - **medium** means that the DCA algorithm is moderately sensitive to environmental changes.
  - **high** means that the DCA algorithm is highly sensitive to environmental changes.

The DCA sensitivity thresholds vary by radio band, as noted in following table.

Table 29: 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

- **config advanced 802.11a channel dca chan-width** {**20** | **40** | **80** | **80+80** }—Configures the DCA channel width for all 802.11n radios in the 5-GHz band.

  where

  - **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.

    Note If you choose **40**, be sure to set at least two adjacent channels in the **config advanced 802.11a channel** {**add** | **delete**} *channel_number* command in *Step 4* (for example, a primary channel of 36 and an extension channel of 40). If you set only one channel, that channel is not used for 40-MHz channel width.

    Note If you choose 40, you can also configure the primary and extension channels used by individual access points.

    Note To override the globally configured DCA channel width setting, you can configure an access point's radio mode using the **config 802.11a chan_width** *Cisco_AP* {**20** | **40** | **80**} command. If you change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

  - **80** sets the channel width for the 802.11ac radios to 80 MHz.
  - **80+80** sets the channel width for the 802.11 radio to 80+80 MHz.

- Configure slot-specific channel width by entering this command:

  config slot *slot-id* **chan_width***ap-name* {**20** | **40** | **80**}

- **config advanced {802.11a | 802.11b} channel outdoor-ap-dca {***enable* | *disable***}**—Enables or disables to the Cisco WLC to avoid checks for non-DFS channels.

  Note This parameter is applicable only for deployments having outdoor access points such as 1522 and 1524.

- **config advanced** {**802.11a** | **802.11b**} **channel foreign** {**enable** | **disable**}—Enables or disables foreign access point interference avoidance in the channel assignment.
- **config advanced** {**802.11a** | **802.11b**} **channel load** {**enable** | **disable**}—Enables or disables load avoidance in the channel assignment.
- **config advanced** {**802.11a** | **802.11b**} **channel noise** {**enable** | **disable**}—Enables or disables noise avoidance in the channel assignment.

- **config advanced** {**802.11a** | **802.11b**} **channel update**—Initiates an update of the channel selection for every Cisco access point.

Step 6 Configure coverage hole detection by entering these commands:

Note You can disable coverage hole detection on a per-WLAN basis.

- **config advanced** {**802.11a** | **802.11b**} **coverage** {**enable** | **disable**}—Enables or disables coverage hole detection. 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 enabled.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*—Specifies the minimum receive signal strength indication (RSSI) value for 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 or voice queue with an RSSI value below the value 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 for data packets and –75 dBm for voice packets. The access point takes RSSI measurements every 5 seconds and reports them to the Cisco WLC in 90-second intervals.
- **config advanced** {**802.11a** | **802.11b**} **coverage level global** *clients*—Specifies 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.
- **config advanced** {**802.11a** | **802.11b**} **coverage exception global** *percent*—Specifies 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%.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **packet-count** *packets*—Specifies the minimum failure count threshold for uplink data or voice packets. The valid range is 1 to 255 packets, and the default value is 10 packets.
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **fail-rate** *percent*—Specifies the failure rate threshold for uplink data or voice packets. The valid range is 1 to 100%, and the default value is 20%.

  Note If both the number and percentage of failed packets exceed the values entered in the **packet-count** and **fail-rate** commands 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 **coverage level global** and **coverage exception global** commands over a 90-second period. 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 7 Configure RRM NDP mode by entering this command:

config advanced 802.11{**a**|**b**} **monitor ndp-mode** {**protected** | **transparent**}

This command configures NDP mode. By default, the mode is set to “transparent”. The following options are available:

- Protected—Packets are encrypted.
- Transparent—Packets are sent as is.

Note See the discovery type by entering the **show advanced 802.11**{**a**|**b**} **monitor** command.

Step 8 Enable the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Note To enable the 802.11g network, enter **config 802.11b 11gSupport** *enable* after the **config 802.11b enable network** command.

Step 9 Save your settings by entering this command:

save config

Viewing RRM Settings (CLI)

To see 802.11a and 802.11b/g RRM settings, use these commands:

show advanced {**802.11a** | **802.11b**} ?

where ? is one of the following:

- **ccx** {*global* | *Cisco_AP*}—Shows the CCX RRM configuration.
- **channel**—Shows the channel assignment configuration and statistics.
- **coverage**—Shows the coverage hole detection configuration and statistics.
- **logging**—Shows the RF event and performance logging.
- **monitor**—Shows the Cisco radio monitoring.
- **profile** {*global* | *Cisco_AP*}—Shows the access point performance profiles.
- **receiver**—Shows the 802.11a or 802.11b/g receiver configuration and statistics.
- **summary**—Shows the configuration and statistics of the 802.11a or 802.11b/g access points.
- **txpower**—Shows the transmit power assignment configuration and statistics.

Debug RRM Issues (CLI)

Use these commands to troubleshoot and verify RRM behavior:

debug airewave-director *?*

where *?* is one of the following:

- **all**—Enables debugging for all RRM logs.
- **channel**—Enables debugging for the RRM channel assignment protocol.

- **detail**—Enables debugging for RRM detail logs.
- **error**—Enables debugging for RRM error logs.
- **group**—Enables debugging for the RRM grouping protocol.
- **manager**—Enables debugging for the RRM manager.
- **message**—Enables debugging for RRM messages.
- **packet**—Enables debugging for RRM packets.
- **power**—Enables debugging for the RRM power assignment protocol as well as coverage hole detection.
- **profile**—Enables debugging for RRM profile events.
- **radar**—Enables debugging for the RRM radar detection/avoidance protocol.
- **rf-change**—Enables debugging for RRM RF changes.

CHAPTER 126

Configuring RRM Neighbor Discovery Packets

- RRM NDP and RF Grouping, on page 879
- Configuring RRM NDP (CLI), on page 880

RRM NDP and RF Grouping

The Cisco Neighbor Discovery Packet (NDP) is the fundamental tool for RRM and other wireless applications that provides information about the neighbor radio information. You can configure the controller to encrypt neighbor discovery packets.

An RF group can only be formed between controllers that have the same encryption mechanism. That is, an access point associated to a controller that is encrypted can not be neighbors with an access point associated to a controller that is not encrypted. The two controllers and their access points will not recognize each other as neighbors and cannot form an RF group. It is possible to assign two controllers in a static RF group configuration that has mismatched encryption settings. In this case, the two controllers do not function as a single RF group because the access points belonging to the mismatched controllers do not recognize one another as neighbors in the group.

Guidelines

- This feature enables you to be compliant with the PCI specifications.
- An RF group can only be formed between controllers that have the same encryption mechanism. That is, an access point associated to a controller that is encrypted can not be neighbors with an access point associated to a controller that is not encrypted. The two controllers and their access points will not recognize each other as neighbors and cannot form an RF group. It is possible to assign two controllers in a static RF group configuration that has mismatched encryption settings. In this case, the two controllers do not function as a single RF group because the access points belonging to the mismatched controllers do not recognize one another as neighbors in the group.
- Ensure that the Cisco Wave 2 APs have an SSID enabled for the APs to send NDP packets. If only the AP radios are enabled but not SSID, then the APs cannot send NDP packets and thus RRM does not work as expected.

Configuring RRM NDP (CLI)

Procedure

	Command or Action	Purpose
Step 1	To configure RRM NDP using the Cisco WLC CLI, enter this command:	**config advanced 802.11**{**a**|**b**} **monitor ndp-mode** {**protected** | **transparent**} This command configures NDP mode. By default, the mode is set to "transparent". The following options are available: • Protected—Packets are encrypted. • Transparent—Packets are sent as is.
Step 2	To configure RRM NDP using the Cisco WLC CLI, enter this command:	**show advanced 802.11**{**a**|**b**} **monitor**

CHAPTER 127

Configuring RF Groups

- Information About RF Groups, on page 881
- Controllers and APs in RF Groups, on page 883
- Configuring RF Groups, on page 884
- Viewing the RF Group Status, on page 885
- Configuring Rogue Access Point Detection in RF Groups, on page 886

Information About RF Groups

An RF group is a logical collection of controllers 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 WLCs into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single WLC .

An RF group is created based on the 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 same RF group name validate messages from each other.

When access points on different controllers hear validated neighbor messages at a signal strength of –80 dBm or stronger, the controllers 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. .

Note RF groups and mobility groups are similar, in that, they both define clusters of controllers , 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 controller 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 *primary* 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 RF group members experience major changes).
- Static Mode—In this mode, a user selects a controller as an RF group leader manually. In this mode, the leader and the members are manually configured and 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 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 controllers in the RF group. The RRM algorithms ensure system-wide stability, and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

Note When a a controller becomes both leader and member for a specific radio, you get to view the IPv4 and IPv6 address as part of the group leader.

When a Controller A becomes a member and Controller B becomes a leader, the Controller A displays either IPv4 or IPv6 address of Controller B using the address it is connected.

So, if both leader and member are not the same, you get to view only one IPv4 or IPv6 address as a group leader in the member.

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 in the same DCA run rather than performing a single global search that is 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 in an 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 the 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 controller is configured in an RF group name, which is sent to all the access points joined to the controller 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 controllers to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a controller might hear RF transmissions from an access point on a different controller , you should configure the controller 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.

Controllers and APs in RF Groups

- Controller software supports up to 20 controllers and 6000 access points in an RF group.
- The RF group members are added based on the following criteria:
  - Maximum number of APs Supported: The maximum limit for the number of access points in an RF group is 6000. The number of access points that are supported is determined by the number of APs licensed to operate on the controller.

- Twenty controllers: Only 20 controllers (including the leader) can be part of an RF group if the sum of the access points of all controllers combined is less than or equal to the upper access point limit.

Table 30: Controller Model Information

	8500	7500	5500	WiSM2
Maximum APs per RRM Group	6000	6000	1000	1000
Maximum AP Groups	6000	6000	500	500

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 controllers 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 an RF Group Name (GUI)

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

Step 2 Enter a name for the RF group in the RF-Network Name text box. The name can contain up to 19 ASCII characters.

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 an RF Group Name (CLI)

Step 1 Create an RF group by entering the **config network rf-network-name name** command:

Note Enter up to 19 ASCII characters for the group name.

Step 2 See the RF group by entering the **show network** command.

Step 3 Save your settings by entering the **save config** command.

Step 4 Repeat this procedure for each controller that you want to include in the RF group.

Viewing the RF Group Status

This section describes how to view the status of the RF group through either the GUI or the CLI.

Note You can also view the status of RF groups using the Cisco Prime Infrastructure.

Viewing the RF Group Status (GUI)

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

This page shows the details of the RF group, displaying the configurable parameter **RF Group mode**, the **RF Group role** of this Cisco WLC, the **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/ac or 802.11b/g/n).

Viewing the RF Group Status (CLI)

Step 1 See which Cisco WLC is the RF group leader for the 802.11a RF network by entering this command:

show advanced 802.11a group

Information similar to the following appears:

```
Radio RF Grouping
  802.11a Group Mode.............................. STATIC
  802.11a Group Update Interval................... 600 seconds
  802.11a Group Leader............................ test (209.165.200.225)
```

```
  802.11a Group Member..................... test (209.165.200.225)
802.11a Last Run.......................... 397 seconds ago
```

This output shows the details of the RF group, specifically the grouping mode for the Cisco WLC, how often the group information is updated (600 seconds by default), the IP address of the RF group leader, the IP address of this Cisco WLC, and the last time the group information was updated.

Note If the IP addresses of the group leader and the group member are identical, this Cisco WLC is currently the group leader.

Note A * indicates that the Cisco WLC has not joined as a static member.

Step 2 See which Cisco WLC is the RF group leader for the 802.11b/g RF network by entering this command:

show advanced 802.11b group

Configuring Rogue Access Point Detection in RF Groups

Rogue Access Point Detection in RF Groups

After you have created an RF group of controller , you need to configure the access points connected to the controller to detect rogue access points. The access points will then select the beacon or 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 selection 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 controller .

Configuring Rogue Access Point Detection in RF Groups

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 **Wireless** to open the All APs page.

Step 3 Click the name of an access point to open the All APs > Details 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 **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.

Configuring Rogue Access Point Detection in RF Groups (CLI)

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 Configure a particular access point for local (normal) mode or monitor (listen-only) mode by entering this command:

config ap mode local *Cisco_AP* or **config ap mode monitor** *Cisco_AP*

Step 3 Save your changes by entering this command:

save config

Step 4 Repeat *Step 2* and *Step 3* for every access point connected to the Cisco WLC.

Step 5 Enable rogue access point detection by entering this command:

config wps ap-authentication

Step 6 Specify when a rogue access point alarm is generated by entering this command. 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.

config wps ap-authentication *threshold*

Note 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.

Step 7 Save your changes by entering this command:

save config

Step 8 Repeat *Step 5* through *Step 7* 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.

CHAPTER 128

Overriding RRM

- Overriding RRM, on page 889
- Prerequisites for Overriding RRM, on page 889
- Statically Assigning Channel and Transmit Power Settings to Access Point Radios, on page 890
- Disabling Dynamic Channel and Power Assignment Globally for a Cisco Wireless LAN Controller, on page 894

Overriding RRM

In some deployments, it is desirable to statically assign channel and transmit power settings to the access points instead of relying on the RRM algorithms provided by Cisco. Typically, this is true in challenging RF environments and non standard deployments but not the more typical carpeted offices.

Note If you choose to statically assign channels and power levels to your access points and/or to disable dynamic channel and power assignment, you should still use automatic RF grouping to avoid spurious rogue device events.

You can disable dynamic channel and power assignment globally for a Cisco WLC, or you can leave dynamic channel and power assignment enabled and statically configure specific access point radios with a channel and power setting. While you can specify a global default transmit power parameter for each network type that applies to all the access point radios on a Cisco WLC, you must set the channel for each access point radio when you disable dynamic channel assignment. You may also want to set the transmit power for each access point instead of leaving the global transmit power in effect.

This section contains the following subsections:

Prerequisites for Overriding RRM

We recommend that you assign different nonoverlapping channels to access points that are within close proximity to each other. The nonoverlapping channels in the U.S. are 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, and 161 in an 802.11a network and 1, 6, and 11 in an 802.11b/g network.

Statically Assigning Channel and Transmit Power Settings to Access Point Radios

Statically Assigning Channel and Transmit Power Settings (GUI)

Step 1 Choose **Wireless > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

This page shows all the 802.11a/n/ac or 802.11b/g/n access point radios that are joined to the Cisco WLC and their current settings. The Channel text box shows both the primary and extension channels and uses an asterisk to indicate if they are globally assigned.

Step 2 Hover your cursor over the blue drop-down arrow for the access point for which you want to modify the radio configuration and choose **Configure**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page appears.

Step 3 Specify the RF Channel Assignment from the following options:

- **Global**—Choose this to specify a global value.
- **Custom**—Choose this and then select a value from the adjacent drop-down list to specify a custom value.

Step 4 Configure the antenna parameters for this radio as follows:

a. From the Antenna Type drop-down list, choose **Internal** or **External** to specify the type of antennas used with the access point radio.

b. Select and unselect the check boxes in the Antenna text box to enable and disable the use of specific antennas for this access point, where A, B, and C are specific antenna ports. The D antenna appears for the Cisco 3600 Series Access Points. A is the right antenna port, B is the left antenna port, and C is the center antenna port. For example, to enable transmissions from antenna ports A and B and receptions from antenna port C, you would select the following check boxes: Tx: A and B and Rx: C. In 3600 APs, the valid combinations are A, A+B, A+B+C or A+B+C+D. When you select a dual mode antenna, you can only apply single spatial 802.11n stream rates: MCS 0 to 7 data rates. When you select two dual mode antennae, you can apply only the two spatial 802.11n stream rates: MCS 0 to 15 data rates.

c. In the Antenna Gain text box, enter a number to specify an external antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain is measured in 0.5 dBi units, and the default value is 7 times 0.5 dBi, or 3.5 dBi.

If you have a high-gain antenna, enter a value that is twice the actual dBi value (see *Cisco Aironet Antenna Reference Guide* for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4-dBi gain, multiply the 4.4 dBi by 2 to get 8.8 and then round down to enter only the whole number (8). The Cisco WLC reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country's regulations.

d. Choose one of the following options from the Diversity drop-down list:

Enabled—Enables the antenna connectors on both sides of the access point. This is the default value.

Side A or Right—Enables the antenna connector on the right side of the access point.

Side B or Left—Enables the antenna connector on the left side of the access point.

Step 5 In the RF Channel Assignment area, choose **Custom** for the Assignment Method under RF Channel Assignment and choose a channel from the drop-down list to assign an RF channel to the access point radio.

Step 6 In the Tx Power Level Assignment area, choose the **Custom** assignment method and choose a transmit power level from the drop-down list to assign a transmit power level to the access point radio.

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 in which the access points are deployed. The number of available power levels varies based on the access point model. However, power level 1 is always the maximum power level allowed per country code setting, with each successive power level representing 50% of the previous power level. For example, 1 = maximum power level in a particular regulatory domain, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and so on.

Note See the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, see the data sheet for your access point for the number of power levels supported.

Note If the access point is not operating at full power, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section.

Step 7 Choose **Enable** from the Admin Status drop-down list to enable this configuration for the access point.

Step 8 Click **Apply**.

Step 9 Have the Cisco WLC send the access point radio admin state immediately to Cisco Prime Infrastructure as follows:

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

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

c. Click **Apply**.

Step 10 Click **Save Configuration**.

Step 11 Repeat this procedure for each access point radio for which you want to assign a static channel and power level.

Statically Assigning Channel and Transmit Power Settings (CLI)

Step 1 Disable the radio of a particular access point on the 802.11a/n/ac or 802.11b/g/n network by entering this command:

config {**802.11a** | **802.11b**} **disable** *Cisco_AP*

Step 2 Configure the channel width for a particular access point by entering this command:

config {**802.11a** | **802.11b**} **chan_width** *Cisco_AP* {**20** | **40** | **80**}

where

- **20** allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels. This is the default value.
- **40** allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together. The radio uses the primary channel that you choose as well as its extension channel for faster throughput. Each channel has only one extension channel (36 and 40 are a pair, 44 and 48 are a pair, and so on). For example, if you choose

a primary channel of 44, the Cisco WLC would use channel 48 as the extension channel. If you choose a primary channel of 48, the Cisco WLC would use channel 44 as the extension channel.

Note This parameter can be configured only if the primary channel is statically assigned.

Note Statically configuring an AP's radio for one of the available modes overrides the globally configured DCA channel width setting (configured using the **config advanced 802.11a channel dca chan-width-11n** {**20** | **40** | **80**} command). If you ever change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using. It can take up to 30 minutes (depending on how often DCA is configured to run) for the change to take effect.

- **80** sets the channel width for the 802.11ac radios to 80 MHz.

Note Channels 116, 120, 124, and 128 are not available in the U.S. and Canada for 40-MHz channel bonding.

Note You should disable the operational and admin status of the slot 1 and slot 2 on the Cisco Aironet 3600 Series APs with 802.11 ac module before changing the channel width using the **config 802.11 {a | b} chan_width ap** *ap-name channel* command. We recommend that you use the **config 802.11 {a | b} disable ap** command to disable the operational and admin status.

Step 3 Enable or disable the use of specific antennas for a particular access point by entering this command:

config {**802.11a** | **802.11b**} **11nsupport antenna** {**tx** | **rx**} *Cisco_AP* {**A** | **B** | **C**} {**enable** | **disable**}

where A, B, and C are antenna ports. A is the right antenna port, B is the left antenna port, and C is the center antenna port. For example, to enable transmissions from the antenna in access point AP1's antenna port C on the 802.11a network, you would enter this command:

config 802.11a 11nsupport antenna tx AP1 C enable

Note You cannot enable or disable individual antennas for 802.11ac because the 802.11ac module antennas are internal.

Step 4 Specify the external antenna gain, which is a measure of an external antenna's ability to direct or focus radio energy over a region of space entering this command:

config {**802.11a** | **802.11b**} **antenna extAntGain** *antenna_gain Cisco_AP*

High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain is measured in 0.5 dBi units, and the default value is 7 times 0.5 dBi, or 3.5 dBi.

If you have a high-gain antenna, enter a value that is twice the actual dBi value (see *Cisco Aironet Antenna Reference Guide* for antenna dBi values). Otherwise, enter 0. For example, if your antenna has a 4.4-dBi gain, multiply the 4.4 dBi by 2 to get 8.8 and then round down to enter only the whole number (8). The Cisco WLC reduces the actual equivalent isotropic radiated power (EIRP) to make sure that the antenna does not violate your country's regulations.

Step 5 Configure beamforming for the 5-GHz radios for all APs or a specific by entering this command:

config 802.11a {**global** | **ap** *ap-name*} {**enable** | **disable**}

Step 6 Specify the channel that a particular access point is to use by entering this command:

config {**802.11a** | **802.11b**} **channel ap** *Cisco_AP channe*l

For example, to configure 802.11a channel 36 as the default channel on AP1, enter the **config 802.11a channel ap AP1 36** command.

The channel you choose is the primary channel (for example, channel 36), which is used for communication by legacy 802.11a radios and 802.11n 20-MHz radios. 802.11n 40-MHz radios use this channel as the primary channel but also use an additional bonded extension channel for faster throughput, if you chose 40 for the channel width.

Note Changing the operating channel causes the access point radio to reset.

Step 7 Specify the transmit power level that a particular access point is to use by entering this command:

config {**802.11a** | **802.11b**} **txPower ap** *Cisco_AP power_level*

For example, to set the transmit power for 802.11a AP1 to power level 2, enter the **config 802.11a txPower ap AP1 2** command.

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 in which the access points are deployed. The number of available power levels varies based on the access point model. However, power level 1 is always the maximum power level allowed per country code setting, with each successive power level representing 50% of the previous power level. For example, 1 = maximum power level in a particular regulatory domain, 2 = 50% power, 3 = 25% power, 4 = 12.5% power, and so on.

In certain cases, Cisco access points support only 7 power levels for certain channels, so that the Cisco Wireless Controller considers the 7th and 8th power levels as the same. If the 8th power level is configured on those channels, the configuration would fail since the controller considers the 7th power level as the lowest acceptable valid power level. These power values are derived based on the regulatory compliance limits and minimum hardware limitation which varies across different Cisco access points. For example, Cisco 3500, 1140, and 1250 series access points allow the configuration of last power levels because those access points report the "per path power" to the controller, whereas all next generation acess points such as Cisco 3700, 3600, 2600, and 1600 series access points report "total power value" to the controller, thereby decreasing the allowed power levels for newer generation products. For example, if the last power level in the 3600E access point has a power value of 4dbm (total power), then it actually means the power value is -2dbm (per path).

Note See the hardware installation guide for your access point for the maximum transmit power levels supported per regulatory domain. Also, see data sheet for your access point for the number of power levels supported.

Step 8 Save your settings by entering this command:

save config

Step 9 Repeat *Step 2* through *Step 7* for each access point radio for which you want to assign a static channel and power level.

Step 10 Reenable the access point radio by entering this command:

config {**802.11a** | **802.11b**} **enable** *Cisco_AP*

Step 11 Have the Cisco WLC send the access point radio admin state immediately to WCS by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Step 12 Save your changes by entering this command:

save config

Step 13 See the configuration of a particular access point by entering this command:

show ap config {**802.11a** | **802.11b**} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 7
Cisco AP Name.................................... AP1
```

```
...
Tx Power
Num Of Supported Power Levels ............. 8
      Tx Power Level 1 ........................... 20 dBm
      Tx Power Level 2 ........................... 17 dBm
      Tx Power Level 3 ........................... 14 dBm
      Tx Power Level 4 ........................... 11 dBm
      Tx Power Level 5 ........................... 8 dBm
      Tx Power Level 6 ........................... 5 dBm
      Tx Power Level 7 ........................... 2 dBm
      Tx Power Level 8 ........................... -1 dBm
      Tx Power Configuration ..................... CUSTOMIZED
      Current Tx Power Level ..................... 1

Phy OFDM parameters
      Configuration .............................. CUSTOMIZED
      Current Channel ............................ 36
      Extension Channel .......................... 40
      Channel Width.............................. 40 Mhz
      Allowed Channel List....................... 36,44,52,60,100,108,116,132,
        ..................................... 149,157
      TI Threshold ............................... -50
      Antenna Type............................... EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBi units).... 7
      Diversity.................................. DIVERSITY_ENABLED

802.11n Antennas
        Tx
         A..................................... ENABLED
         B..................................... ENABLED
        Rx
         A..................................... DISABLED
         B..................................... DISABLED
         C..................................... ENABLED
```

Disabling Dynamic Channel and Power Assignment Globally for a Cisco Wireless LAN Controller

Disabling Dynamic Channel and Power Assignment (GUI)

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **RRM** > **Auto RF** to open the 802.11a/n/ac (or 802.11b/g/n) Global Parameters > Auto RF page.

Step 2 Disable dynamic channel assignment by choosing **OFF** under RF Channel Assignment.

Step 3 Disable dynamic power assignment by choosing **Fixed** under Tx Power Level Assignment and choosing a default transmit power level from the drop-down list.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 If you are overriding the default channel and power settings on a per radio basis, assign static channel and power settings to each of the access point radios that are joined to the Cisco WLC.

Step 7 (Optional) Repeat this procedure for the network type that you did not select (802.11a/n/ac or 802.11b/g/n).

Disabling Dynamic Channel and Power Assignment (CLI)

Step 1 Disable the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **disable network**

Step 2 Disable RRM for all 802.11a or 802.11b/g radios and set all channels to the default value by entering this command:

config {**802.11a** | **802.11b**} **channel global off**

Step 3 Enable the 802.11a or 802.11b/g network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Note To enable the 802.11g network, enter the **config 802.11b 11gSupport enable** command after the **config 802.11b enable network** command.

Step 4 Save your changes by entering this command:

save config

CHAPTER 129

Configuring CCX Radio Management Features

- CCX Radio Management, on page 897
- Configuring CCX Radio Management, on page 898

CCX Radio Management

You can configure two parameters that affect client location calculations:

- Radio measurement requests
- Location calibration

These parameters are supported in Cisco Client Extensions (CCX) v2 and later releases. They are designed to enhance location accuracy and timeliness for participating CCX clients.

For the location features to operate properly, the access points must be configured for Local, Monitor, or FlexConnect mode. Location features will not work on FlexConnect APs that have lost their controller connection and entered Standalone mode.

This section contains the following subsections:

Radio Measurement Requests

When you enable the radio measurement requests feature, lightweight access points issue broadcast radio measurement request messages to clients running CCXv2 or later releases. The access points transmit these messages for every SSID over each enabled radio interface at a configured interval. In the process of performing 802.11 radio measurements, CCX clients send 802.11 broadcast probe requests on all the channels specified in the measurement request. Cisco location appliances use the uplink measurements based on these requests received at the access points to quickly and accurately calculate the client location. You do not need to specify on which channels the clients are to measure. The controller, access point, and client automatically determine which channels to use.

The radio measurement requests feature enables the controller to also obtain information on the radio environment from the client's perspective (rather than from just that of the access point). In this case, the access points issue unicast radio measurement requests to a particular CCXv4 or v5 client. The client then sends various measurement reports back to the access point and on to the controller. These reports include information about the radio environment and data used to interpret the location of the clients. To prevent the access points and controller from being overwhelmed by radio measurement requests and reports, only two clients per access point and up to 20 clients per controller are supported. You can view the status of radio

measurement requests for a particular access point or client as well as radio measurement reports for a particular client from the controller CLI.

The controller software improves the ability of the location appliance to accurately interpret the location of a device through a CCXv4 feature called location-based services. The controller issues a path-loss request to a particular CCXv4 or v5 client. If the client chooses to respond, it sends a path-loss measurement report to the controller. These reports contain the channel and transmit power of the client.

Note Non-CCX and CCXv1 clients ignore the CCX measurement requests and do not participate in the radio measurement activity.

Location Calibration

For CCX clients that need to be tracked more closely (for example, when a client calibration is performed), the Cisco WLC can be configured to command the access point to send unicast measurement requests to these clients at a configured interval and whenever a CCX client roams to a new access point. These unicast requests can be sent out more often to these specific CCX clients than the broadcast measurement requests, which are sent to all clients. When location calibration is configured for non-CCX and CCXv1 clients, the clients are forced to disassociate at a specified interval to generate location measurements.

Configuring CCX Radio Management

Configuring CCX Radio Management (GUI)

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

Step 2 Under CCX Location Measurement, select the **Mode** check box to globally enable CCX radio management. This parameter causes the access points connected to this Cisco WLC to issue broadcast radio measurement requests to clients running CCX v2 or later releases. The default value is disabled (or unselected).

Step 3 If you selected the Mode check box in the previous step, enter a value in the Interval text box to specify how often the access points are to issue the broadcast radio measurement requests.

The range is 60 to 32400 seconds.

The default is 60 seconds.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 Follow the instructions in *Step 2* of the Configuring CCX Radio Management (CLI) section below to enable access point customization.

Note To enable CCX radio management for a particular access point, you must enable access point customization, which can be done only through the Cisco WLC CLI.

Step 7 If desired, repeat this procedure for the other radio band (802.11a/n/ac or 802.11b/g/n).

Configuring CCX Radio Management (CLI)

Step 1 Globally enable CCX radio management by entering this command:

config advanced {**802.11a** | **802.11b**} **ccx location-meas global enable** *interval_seconds*

The range for the *interval_seconds* parameter is 60 to 32400 seconds, and the default value is 60 seconds. This command causes all access points connected to this Cisco WLC in the 802.11a or 802.11b/g network to issue broadcast radio measurement requests to clients running CCXv2 or later releases.

Step 2 Enable access point customization by entering these commands:

- **config advanced** {**802.11a** | **802.11b**} **ccx customize** *Cisco_AP* {**on** | **off**}

  This command enables or disables CCX radio management features for a particular access point in the 802.11a or 802.11b/g network.

- **config advanced** {**802.11a** | **802.11b**} **ccx location-meas ap** *Cisco_AP* **enable** *interval_seconds*

  The range for the *interval_seconds* parameter is 60 to 32400 seconds, and the default value is 60 seconds. This command causes a particular access point in the 802.11a or 802.11b/g network to issue broadcast radio measurement requests to clients running CCXv2 or higher.

Step 3 Save your settings by entering this command:

save config

Viewing CCX Radio Management Information (CLI)

- To see the CCX broadcast location measurement request configuration for all access points connected to this Cisco WLC in the 802.11a or 802.11b/g network, enter this command:

  show advanced {**802.11a** | **802.11b**} **ccx global**

- To see the CCX broadcast location measurement request configuration for a particular access point in the 802.11a or 802.11b/g network, enter this command:

  show advanced {**802.11a** | **802.11b**} **ccx ap** *Cisco_AP*

- To see the status of radio measurement requests for a particular access point, enter this command:

  show ap ccx rm *Cisco_AP* **status**

  Information similar to the following appears:

```
A Radio

  Beacon Request.............................. Enabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Disabled
```

```
  Path Loss Request.............................. Disabled
  Interval....................................... 60
  Iteration...................................... 5

B Radio

  Beacon Request................................. Disabled
  Channel Load Request........................... Enabled
  Frame Request.................................. Disabled
  Noise Histogram Request........................ Enabled
  Path Loss Request.............................. Disabled
  Interval....................................... 60
  Iteration..................................... 5
```

- To see the status of radio measurement requests for a particular client, enter this command:

  show client ccx rm *client_mac* **status**

  Information similar to the following appears:

```
Client Mac Address............................. 00:40:96:ae:53:b4
Beacon Request................................. Enabled
Channel Load Request........................... Disabled
Frame Request.................................. Disabled
Noise Histogram Request........................ Disabled
Path Loss Request.............................. Disabled
Interval....................................... 5
Iteration...................................... 3
```

- To see radio measurement reports for a particular client, enter these commands:

  show client ccx rm *client_mac* **report beacon**—Shows the beacon report for the specified client.

  show client ccx rm *client_mac* **report chan-load**—Shows the channel-load report for the specified client.

  show client ccx rm *client_mac* **report noise-hist**—Shows the noise-histogram report for the specified client.

  show client ccx rm *client_mac* **report frame**—Shows the frame report for the specified client.

- To see the clients configured for location calibration, enter this command:

  show client location-calibration summary

- To see the RSSI reported for both antennas on each access point that heard the client, enter this command:

  show client detail *client_mac*

Debugging CCX Radio Management Issues (CLI)

- Debug CCX broadcast measurement request activity by entering this command:

  debug airewave-director message {**enable** | **disable**}

- Debug client location calibration activity by entering this command:

  debug ccxrm [**all** | **error** | **warning** | **message** | **packet** | **detail** {**enable** | **disable**}]

- The CCX radio measurement report packets are encapsulated in Internet Access Point Protocol (IAPP) packets. Therefore, if the previous **debug ccxrm** command does not provide any debugs, enter this command to provide debugs at the IAPP level:

  debug iapp error {**enable** | **disable**}

- Debug the output for forwarded probes and their included RSSI for both antennas by entering this command:

  debug dot11 load-balancing

PART VIII

Cisco CleanAir

- Information About CleanAir, on page 905
- Prerequisites and Restrictions for CleanAir, on page 909
- Cisco CleanAir, on page 913
- Monitoring the Interference Devices, on page 921
- Configuring a Spectrum Expert Connection, on page 931

CHAPTER 130

Information About CleanAir

This chapter describes information about CleanAir.

- CleanAir, on page 905

CleanAir

Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all of the users of the shared spectrum (both native devices and foreign interferers). It also enables you or your network to act upon this information. For example, you could manually remove the interfering device, or the system could automatically change the channel away from the interference. CleanAir provides spectrum management and RF visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points, Cisco Wireless LAN Controllers, and Cisco Prime Infrastructure. These access points 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 Cisco WLC. The Cisco WLC controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure or a Cisco mobility services engine (MSE) upon request.

For every device operating in the unlicensed band, Cisco CleanAir tells you what it is, where it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF so that you do not have to be an RF expert.

Wireless LAN systems operate in unlicensed 2.4- and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect 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 into the Cisco Unified Wireless Network addresses this problem of radio frequency (RF) interference.

CleanAir is supported on mesh AP backhaul at a 5-GHz radio of mesh. You can enable CleanAir on backhaul radios and can provide report interference details and air quality.

This section contains the following subsections:

Role of the Cisco Wireless LAN Controller in a Cisco CleanAir System

The Cisco WLC performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (GUI, CLI, and SNMP) for configuring Cisco CleanAir features and retrieving data
- Displays spectrum data.
- Collects and processes air quality reports from the access point and stores them in the air quality database. The Air Quality Report (AQR) contains information about the total interference from all identified sources represented by the 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 enables you to take action in cases where the interference due to unclassified interfering devices is more.
- 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.

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.

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 interferences 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.

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 Cisco WLC 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 stores the information in the Cisco WLC. Local/Bridge mode AP detects interference devices on the serving channels only.

Persistent Devices Propagation

Persistent device information that is detected by local or monitor mode access points is propagated to the neighboring access points connected to the same Cisco WLC to provide better chance of handling and avoiding persistent devices. Persistent device detected by the CleanAir-enabled access point is propagated to neighboring non-CleanAir access points, thus enhancing channel selection quality.

Detecting Interferers by an Access Point

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.

CHAPTER 131

Prerequisites and Restrictions for CleanAir

This chapter describes the prerequisites and restrictions for configuring Cisco CleanAir.

- Prerequisites for CleanAir, on page 909
- Restrictions for CleanAir, on page 910

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. An AP can only measure air quality and interference when the AP is not busy transmitting wi-fi frames. This implies that CleanAir detections will be drastically lower if the AP is having a high channel utiliaztion.
- FlexConnect—When a FlexConnect access point is connected to the controller , its Cisco CleanAir functionality is identical to local mode.
- 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 channels are legal within a regulatory domain

Note Suppose you have two APs, one in the FlexConnect mode and the other in the monitor mode. Also suppose that you have created a profile enabling EAP attack against 802.1x auth. The Airmagnet (AM) tool, which can generate different types of attacks, fails to generate any attack even if you have provided valid AP MAC and STA MAC addresses. But if the AP MAC and STA MAC addresses in the AM tool are swapped, that is, the AP MAC address is specified in the STA MAC field and the STA MAC address is specified in the AP MAC field, then the tool is able to generate attacks, which the AP in the Monitor mode is also able to detect.

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 controller. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the controller. 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.

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 controller's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- Spectrum Expert (SE) Connect functionality is supported for local, FlexConnect, bridge, and monitor modes. The access point provides spectrum information to Spectrum Expert only for the current channel(s). For local, FlexConnect, and bridge modes, the spectrum data is available for the current active channel(s) and for the monitor mode, the common monitored channel list is available. The access point continues to send AQ (Air Quality) and IDR (Interference Device Reports) reports to the controller and perform normal activities according to the current mode. Sniffer and rogue detections access point modes are incompatible with all types of CleanAir spectrum monitoring.
- Monitor Mode access point in slot 2 operates at 2.4 GHz only. For 4800 AP slot 1 5ghz is dedicated and cannot be individually moved to monitor mode. However, slot 0 is XOR and can be moved to monitor as well as 2.4/5ghz. Slot 2 is dedicated monitor and will operate in 5ghz and in AP monitor mode, slot 2 will be disabled because a monitor radio is alreay available in both 2.4/5ghz. 3700 AP has dedicated 2.4ghz (slot0) and 5ghz (slot1).
- We recommend a ratio of 1 monitor-mode access point for every 5 local-mode access points; this can vary based on the network design and expert guidance for best coverage.

- Do not connect access points in SE connect mode directly to any physical port on Cisco 2500 Series Cisco WLCs.
- Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.
- CleanAir is not supported wherein the channel width is 160 MHz.

CHAPTER 132

Cisco CleanAir

- Configuring Cisco CleanAir on the Controller, on page 913
- Configuring Cisco CleanAir on an Access Point, on page 919

Configuring Cisco CleanAir on the Controller

Configuring Cisco CleanAir on Cisco WLC (GUI)

Step 1 Choose **Wireless** > **802.11a/n/ac or 802.11b/g/n > CleanAir** to open the **802.11a (or 802.11b) > CleanAir** page.

Step 2 Check the **CleanAir** check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or uncheck it to prevent the Cisco WLC from detecting spectrum interference. By default, this feature is in disabled state.

Step 3 Check the **Report Interferers** check box to enable the Cisco CleanAir system to report any detected sources of interference, or uncheck it to prevent the Cisco WLC from reporting interferers. By default, this feature is in enabled state.

Note Device Security alarms, Event Driven RRM, and the Persistence Device Avoidance algorithm do not work if Report Interferers are disabled.

Step 4 Check the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables you to propagate information about persistent devices to the neighboring APs connected to the same Cisco WLC. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times.

Step 5 Ensure that any sources of interference that need to be detected and reported by the Cisco CleanAir system appear in the **Interferences to Detect** box and any that do not need to be detected appear in the **Interferences to Ignore** box. By default, all interference sources are detected. The possible sources of interference that you can choose are as follows:

- **Bluetooth Paging Inquiry**—A Bluetooth discovery (802.11b/g/n only)
- **Bluetooth Sco Acl**—A Bluetooth link (802.11b/g/n only)
- **Generic DECT**—A digital enhanced cordless communication (DECT)-compatible phone
- **Generic TDD**—A time division duplex (TDD) transmitter
- **Generic Waveform**—A continuous transmitter
- **Jammer**—A jamming device
- **Microwave—**A microwave oven (802.11b/g/n only)
- **Canopy**—A canopy bridge device
- **Spectrum 802.11 FH—**An 802.11 frequency-hopping device (802.11b/g/n only)

- **Spectrum 802.11 inverted**—A device using spectrally inverted Wi-Fi signals
- **Spectrum 802.11 non std channel**—A device using nonstandard Wi-Fi channels
- **Spectrum 802.11 SuperG**—An 802.11 SuperAG device
- **Spectrum 802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **Video Camera**—An analog video camera
- **WiMAX Fixed**—A WiMAX fixed device (802.11a/n/ac only)
- **WiMAX Mobile**—A WiMAX mobile device (802.11a/n/ac only)
- **XBox**—A Microsoft Xbox (802.11b/g/n only)

Note When you include BLE Beacon in the **Interferences to Detect** list, the 2.4GHz serving radio periodically goes off channel for a scan.

Note APs that are associated to the Cisco WLC send interference reports only for the interferers that appear in the **Interferences to Detect** box. This functionality allows you to filter out interferers that you do not want as well as any that may be flooding the network and causing performance problems for the Cisco WLC or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 6 Configure Cisco CleanAir alarms as follows:

a) Check the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or uncheck the box to disable this feature. By default, this feature is in enabled state.

b) If you checked the **Enable AQI Trap** check box in *Step a*, enter a value between 1 and 100 (inclusive) in the **AQI Alarm Threshold** field to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

c) Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality reaches a threshold value. The default is 35. Valid range is from 1 and 100.

d) Check the **Enable trap for Unclassified Interferences** check box to enable the AQI alarm to be generated upon detection of unclassified interference beyond the severity threshond specified in the **AQI Alarm Threshold** field. Unclassified interferences are interferences that are detected but do not correspond to any of the identifiable interference types.

e) Enter the **Threshold for Unclassified category trap (1 to 99)**. Enter a value from 1 and 99. The default is 20. This is the severity index threshold for an unclassified interference category.

f) Check the **Enable Interference Type Trap** check box to trigger interferer alarms when the Cisco WLC detects specified device types, or uncheck it to disable this feature. By default, this feature is in enabled state.

g) Ensure that any sources of interference that need to trigger interferer alarms appear in the **Trap on These Types** box and any that do not need to trigger interferer alarms appear in the **Do Not Trap on These Types** box. By default, all interference sources trigger interferer alarms.

   For example, if you want the Cisco WLC to send an alarm when it detects a jamming device, check the **Enable Interference Type Trap** check box and move the jamming device to the **Trap on These Types** box.

Step 7 Click **Apply**.

Step 8 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled AP detects a significant level of interference as follows:

a) Look at the **EDRRM** field to see the current status of spectrum event-driven RRM and, if enabled, the Sensitivity Threshold field to see the threshold level at which event-driven RRM is invoked.

b) If you want to change the current status of event-driven RRM or the sensitivity level, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page is displayed.

c) Check the **EDRRM** check box to trigger RRM to run when an AP detects a certain level of interference, or uncheck it to disable this feature. By default, this feature is in enabled state.

d) If you checked the **EDRRM** check box in *Step c*, choose **Low**, **Medium**, **High,** or **Custom** from the **Sensitivity Threshold** drop-down list to specify the threshold at which you want RRM to be triggered. When the interference for the AP rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected AP radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

   If you selected the EDRRM sensitivity threshold as custom, you must set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35.

   The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60.

e) Save the configuration.

Configuring Cisco CleanAir on Cisco WLC (CLI)

Step 1 Configure Cisco CleanAir functionality on the 802.11 network by entering this command:

config {**802.11a** | **802.11b**} **cleanair** {**enable** | **disable**} *all*

If you disable this feature, the Cisco WLC does not receive any spectrum data. By default, this feature is in disabled state.

Step 2 Enable CleanAir on all associated access points in a network:

config {**802.11a** | **802.11b**} **cleanair enable network**

You can enable CleanAir on a 5-GHz radio of mesh access points.

Step 3 Configure interference detection and specify sources of interference that need to be detected by the Cisco CleanAir system by entering this command:

config {**802.11a** | **802.11b**} **cleanair device** {**enable** | **disable**} *type*

where you choose the *type* as one of the following:

- **802.11-fh**—An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv**—A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
- **802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **all**—All interference device types (this is the default value)
- **bt-discovery**—A bluetooth discovery (802.11b/g/n only)
- **bt-link**—A bluetooth link (802.11b/g/n only)
- **canopy**—A canopy device
- **cont-tx**—A continuous transmitter
- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **mw-oven**—A microwave oven (802.11b/g/n only)
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter

- **video camera**—An analog video camera
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device
- **xbox**—A Microsoft Xbox (802.11b/g/n only)

Note Access points that are associated to the Cisco WLC send interference reports only for the interference types specified in this command. This functionality allows you to filter out interferers that may be flooding the network and causing performance problems for the Cisco WLC or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 4 Configure the triggering of air quality alarms by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm air-quality** {**enable** | **disable**}

The default value is enabled.

Step 5 Specify the threshold at which you want the air quality alarm to be triggered by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm air-quality threshold** *threshold*

where *threshold* is a value between 1 and 100 (inclusive). When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Step 6 Enable the triggering of interferer alarms by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm device** {**enable** | **disable**}

The default value is enable.

Step 7 Specify sources of interference that trigger alarms by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm device** *type* {**enable** | **disable**}

where you choose the *type* as one of the following:

- **802.11-fh—**An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv**—A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
- **802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **all**—All interference device types (this is the default value)
- **bt-discovery**—A Bluetooth discovery (802.11b/g/n only)
- **bt-link**—A Bluetooth link (802.11b/g/n only)
- **canopy**—A canopy device
- **cont-tx**—A continuous transmitter
- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **mw-oven**—A microwave oven (802.11b/g/n only)
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter

- **video camera**—An analog video camera
- wimax-fixed—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device
- **xbox**—A Microsoft Xbox (802.11b/g/n only)

Step 8 Configure the triggering of air quality alarms for unclassified devices by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm unclassified** {**enable** | **disable**}

Step 9 Specify the threshold at which you want the air quality alarm to be triggered for unclassified devices by entering this command:

config {**802.11a** | **802.11b**} **cleanair alarm unclassified threshold** *threshold*

where *threshold* is a value from 1 and 99 (inclusive). When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

Step 10 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:

config advanced {**802.11a** | **802.11b**} **channel cleanair-event** {**enable** | **disable**}—Enables or disables spectrum event-driven RRM. The default value is disabled.

config advanced {**802.11a** | **802.11b**} **channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}—Specifies the threshold at which you want RRM to be triggered. When the interference level for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while high represents an increased sensitivity. You can also set the sensitivity to a custom level of your choice. The default value is medium.

config advanced {**802.11a** | **802.11b**} **channel cleanair-event sensitivity threshold** *thresholdvalue*—If you set the threshold sensitivity as custom, you must set a custom threshold value. The default is 35.

Step 11 Enable persistent devices propagation by entering this command:

config advanced {**802.11a** | **802.11b**} **channel pda-prop** {**enable** | **disable**}

Step 12 Save your changes by entering this command:

save config

Step 13 See the Cisco CleanAir configuration for the 802.11a/n or 802.11b/g/n network by entering this command:

show {**802.11a** | **802.11b**} **cleanair config**

Information similar to the following appears:

```
(Cisco Controller) >show 802.11a cleanair config

Clean Air Solution................................ Disabled
Air Quality Settings:
    Air Quality Reporting......................... Enabled
    Air Quality Reporting Period (min)............ 15
    Air Quality Alarms............................ Enabled
      Air Quality Alarm Threshold................. 35
      Unclassified Interference................... Disabled
      Unclassified Severity Threshold............. 20
```

```
Interference Device Settings:
    Interference Device Reporting..... Enabled
    Interference Device Types:
        TDD Transmitter..... Enabled
        Jammer..... Enabled
        Continuous Transmitter..... Enabled
        DECT-like Phone..... Enabled
        Video Camera..... Enabled
        WiFi Inverted..... Enabled
        WiFi Invalid Channel..... Enabled
        SuperAG..... Enabled
        Canopy..... Enabled
        WiMax Mobile..... Enabled
  WiMax Fixed..... Enabled
Interference Device Alarms..... Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter..... Disabled
        Jammer..... Enabled
        Continuous Transmitter..... Disabled
        DECT-like Phone..... Disabled
        Video Camera..... Disabled
        WiFi Inverted..... Enabled
        WiFi Invalid Channel..... Enabled
        SuperAG..... Disabled
        Canopy..... Disabled
        WiMax Mobile..... Disabled
        WiMax Fixed..... Disabled
Additional Clean Air Settings:
    CleanAir ED-RRM State..... Disabled
    CleanAir ED-RRM Sensitivity..... Medium
    CleanAir ED-RRM Custom Threshold..... 50
    CleanAir Persistent Devices state..... Disabled
    CleanAir Persistent Device Propagation..... Enabled
```

Step 14 See the spectrum event-driven RRM configuration for the 802.11a/n/ac or 802.11b/g/n network by entering this command:

show advanced {**802.11a** | **802.11b**} *channel*

Information similar to the following appears:

```
Automatic Channel Assignment
  Channel Assignment Mode..... AUTO
  Channel Update Interval..... 600 seconds [startup]
  Anchor time (Hour of the day)..... 0
  Channel Update Contribution..... SNI
  CleanAir Event-driven RRM option..... Enabled
CleanAir Event-driven RRM sensitivity..... Medium
```

Configuring Cisco CleanAir on an Access Point

Configuring Cisco CleanAir on an Access Point (GUI)

Step 1 Choose **Wireless** > **Access Points > Radios > 802.11a/n/ac or 802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 2 Hover your cursor over the blue drop-down arrow for the desired access point and click **Configure**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page appears.

The **CleanAir Capable** field shows whether this access point can support CleanAir functionality. If it can, go to the next step to enable or disable CleanAir for this access point. If the access point cannot support CleanAir functionality, you cannot enable CleanAir for this access point.

Note By default, the Cisco CleanAir functionality is enabled on the radios.

Step 3 Enable Cisco CleanAir functionality for this access point by choosing **Enable** from the CleanAir Status drop-down list. To disable CleanAir functionality for this access point, choose **Disable**. The default value is Enable. This setting overrides the global CleanAir configuration for this access point.

The **Number of Spectrum Expert Connections** text box shows the number of Spectrum Expert applications that are currently connected to the access point radio. Up to three active connections are possible.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 Click **Back** to return to the 802.11a/n/ac (or 802.11b/g/n) Radios page.

Step 7 View the Cisco CleanAir status for each access point radio by looking at the **CleanAir Status** text box on the 802.11a/n/ac (or 802.11b/g/n) Radios page.

The Cisco CleanAir status is one of the following:

- **UP**—The spectrum sensor for the access point radio is currently operational (error code 0).
- **DOWN**—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio.
- **ERROR**—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable Cisco CleanAir functionality on the radio.
- **N/A**—This access point radio is not capable of supporting Cisco CleanAir functionality.

Note You can create a filter to make the 802.11a/n/ac Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific Cisco CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP dialog box, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the 802.11a/n/ac Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).

Configuring Cisco CleanAir on an Access Point (CLI)

Step 1 Configure Cisco CleanAir functionality for a specific access point by entering this command:

config {**802.11a** | **802.11b**} **cleanair {enable | disable}***Cisco_AP*

Step 2 Save your changes by entering this command:

save config

Step 3 See the Cisco CleanAir configuration for a specific access point on the 802.11a/n/ac/ac or 802.11b/g/n/ac network by entering this command:

show ap config {802.11a | 802.11b} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500
...
Spectrum Management Information
        Spectrum Management Capable.............. Yes
        Spectrum Management Admin State.......... Enabled
        Spectrum Management Operation State...... Up
        Rapid Update Mode........................ Disabled
        Spectrum Expert connection............... Disabled
   Spectrum Sensor State................. Configured (Error code = 0)
```

CHAPTER 133

Monitoring the Interference Devices

- Prerequisites for Monitoring the Interference Devices, on page 921
- Monitoring the Interference Device (GUI), on page 921
- Monitoring the Interference Device (CLI), on page 923
- Monitoring Persistent Devices (GUI), on page 925
- Monitoring Persistent Devices (CLI), on page 925
- Monitoring the Air Quality of Radio Bands, on page 926

Prerequisites for Monitoring the Interference Devices

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Monitoring the Interference Device (GUI)

Step 1 Choose **Monitor > Cisco CleanAir > 802.11a/n or 802.11b/g/n > Interference Devices** to open the CleanAir > Interference Devices page.

This page shows the following information:

- **AP Name**—The name of the access point where the interference device is detected.
- **Radio Slot #**—Slot where the radio is installed.
- **Interferer Type**—Type of the interferer.
- **Affected Channel**—Channel that the device affects.
- **Detected Time**—Time at which the interference was detected.
- **Severity**—Severity index of the interfering device.
- **Duty Cycle (%)**—Proportion of time during which the interfering device was active.
- **RSSI**—Receive signal strength indicator (RSSI) of the access point.
- **DevID**—Device identification number that uniquely identified the interfering device.
- **ClusterID**—Cluster identification number that uniquely identifies the type of the devices.

Step 2 Click **Change Filter** to display the information about interference devices based on a particular criteria.

Step 3 Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of interference devices that are based on the following filtering parameters:

- **Cluster ID**—To filter based on the Cluster ID, select the check box and enter the Cluster ID in the text box next to this field.
- **AP Name**—To filter based on the access point name, select the check box and enter the access point name in the text box next to this field.
- **Interferer Type**—To filter based on the type of the interference device, select the check box and select the interferer device from the options.

  Select one of the interferer devices:

  - **BT Link**
  - **MW Oven**
  - **802.11 FH**
  - **BT Discovery**
  - **TDD Transmit**
  - **Jammer**
  - **Continuous TX**
  - **DECT Phone**
  - **Video Camera**
  - **802.15.4**
  - **WiFi Inverted**
  - **WiFi Inv. Ch**
  - **SuperAG**
  - **Canopy**
  - **XBox**
  - **WiMax Mobile**
  - **WiMax Fixed**
  - **WiFi ACI**
  - **Unclassified**

- **Activity Channels**
- **Severity**
- **Duty Cycle (%)**
- **RSSI**

Step 4 Click **Find**.

The current filter parameters are displayed in the Current Filter field.

Monitoring the Interference Device (CLI)

This section describes the commands that you can use to monitor the interference devices for the 802.11a/n or 802.11b/g/n radio band.

Detecting Interferers by an Access Point

See information for all of the interferers detected by a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair device ap** *Cisco_AP*

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.

Detecting Interferers by Device Type

See information for all of the interferers of a specific device type on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair device type** *type*

where you choose *type* as one of the following:

- **802.11a**
  - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
  - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
  - **canopy**—A canopy bridge device
  - **cont-tx**—A continuous transmitter

- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video**—A video device
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device

- **802.11b**
  - **bt-link**—A bluetooth link device
  - **bt-discovery**—A bluetooth discovery device
  - **ble-beacon**—A BLE beacon device
  - **mw-oven—**A microwave oven device
  - **802.11-fh—**An 802.11 frequency-hopping device
  - **802.15.4**—An 802.15.4 device
  - **tdd-tx**—A time division duplex (TDD) transmitter
  - **jammer**—A jamming device
  - **cont-tx**—A continuous transmitter
  - **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
  - **video**—A video device
  - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
  - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
  - **superag**—An 802.11 SuperAG device
  - **canopy**—A canopy bridge device
  - **wimax-mobile**—A WiMAX mobile device
  - **wimax-fixed**—A WiMAX fixed device
  - **msft-xbox**—A Microsoft Xbox device

Note No more than 25 interferers can be detected by a Cisco AP.

Detecting Persistent Sources of Interference

See a list of persistent sources of interference for a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show ap auto-rf {**802.11a** | **802.11b**} *Cisco_AP*

Monitoring Persistent Devices (GUI)

Choose **Wireless** > **Access Points > Radios > 802.11a/n/ac or 802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page. Hover your cursor over the blue drop-down arrow for the desired access point and click **Detail**. The 802.11a/n/ac (or 802.11b/g/n) AP Interfaces > Detail page is displayed.

This page displays the details of the access points along with the list of persistent devices detected by this access point. Details of the persistent devices is displayed under the Persistent Devices section.

The following information for each persistent device is available:

- Class Type—The class type of the persistent device.
- Channel—Channel this device is affecting.
- DC(%)—Duty cycle (in percentage) of the persistent device.
- RSSI(dBm)—RSSI indicator of the persistent device.
- Last Seen Time—Timestamp when the device was last active.

Monitoring Persistent Devices (CLI)

To view the list of persistent devices using the CLI, use the following command:

show ap auto-rf {**802.11a** | **802.11b**} *ap_name*

Information similar to the following appears:

```
Number Of Slots.................................. 2
AP Name.......................................... AP_1142_MAP
MAC Address...................................... c4:7d:4f:3a:35:38
  Slot ID........................................ 1
  Radio Type..................................... RADIO_TYPE_80211a
  Sub-band Type.................................. All
  Noise Information
. . ..
. . . .
Power Level.................................. 1
```

```
    RTS/CTS Threshold..................................... 2347
    Fragmentation Threshold............................... 2346
    Antenna Pattern....................................... 0

Persistent Interference Devices
  Class Type                Channel  DC (%%)  RSSI (dBm)  Last Update Time
  ------------------------  -------  ------  ----------  ------------------------
  Video Camera              149      100     -34         Tue Nov  8 10:06:25 2011
```

The following information for each persistent device is available:

- Class Type—The class type of the persistent device.
- Channel—Channel this device is affecting.
- DC(%)—Duty cycle (in percentage) of the persistent device.
- RSSI(dBm)—RSSI indicator of the persistent device.
- Last Seen Time—Timestamp when the device was last active.

Monitoring the Air Quality of Radio Bands

This section describes how to monitor the air quality of the 802.11a/n/ac and 802.11b/g/n radio bands using both the Cisco WLC GUI and CLI.

Monitoring the Air Quality of Radio Bands (GUI)

Choose **Monitor > Cisco CleanAir > 802.11a/n/ac or 802.11b/g/n >Air Quality Report** to open the **CleanAir > Air Quality Report** page.

This page shows the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands. Specifically, it shows the following information:

- AP Name—The name of the access point that reported the worst air quality for the 802.11a/n/ac or 802.11b/g/n radio band.
- Radio Slot—The slot number where the radio is installed.
- Channel—The radio channel where the air quality is monitored.
- Minimum AQ—The minimum air quality for this radio channel.
- Average AQ—The average air quality for this radio channel.
- Interferer—The number of interferers detected by the radios on the 802.11a/n/ac or 802.11b/g/n radio band.
- DFS—Dynamic Frequency Selection. This indicates if DFS is enabled or not.

Monitoring the Air Quality of Radio Bands (CLI)

This section describes the commands that you can use to monitor the air quality of the 802.11a/n/ac or 802.11b/g/n radio band.

Viewing a Summary of the Air Quality

See a summary of the air quality for the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality summary**

Viewing Air Quality for all Access Points on a Radio Band

See information for the 802.11a/n/ac or 802.11b/g/n access point with the air quality by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality**

Viewing Air Quality for an Access Point on a Radio Band (CLI)

See air quality information for a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality** *Cisco_AP*

Monitoring the Worst Air Quality of Radio Bands (GUI)

Step 1 Choose **Monitor** > **Cisco CleanAir** >**Worst Air-Quality** to open the **CleanAir > Worst Air Quality Report** page.

This page shows the air quality of both the 802.11a/n/ac and 802.11b/g/n radio bands. Specifically, it shows the following information:

- **AP Name**—The name of the access point that reported the worst air quality for the 802.11 radio band.
- **Channel Number**—The radio channel with the worst reported air quality.
- **Minimum Air Quality Index(1 to 100)**—The minimum air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Average Air Quality Index(1 to 100)**—The average air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Interference Device Count**—The number of interferers detected by the radios on the 802.11 radio band.

Step 2 See a list of persistent sources of interference for a specific access point radio as follows:

a) **Choose Wireless** > **Access Points** > **Radios** > **802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

b) Hover your cursor over the blue drop-down arrow for the desired access point radio and click **CleanAir-RRM**. The 802.11a/n/ac (or 802.11b/g/n) Cisco APs > *Access Point Name* > Persistent Devices page appears. This page lists the device types of persistent sources of interference detected by this access point radio. It also shows the channel on which the interference was detected, the percentage of time that the interferer was active (duty cycle), the received signal strength (RSSI) of the interferer, and the day and time when the interferer was last detected.

Monitoring the Worst Air Quality of Radio Bands (CLI)

This section describes the commands that you can use to monitor the air quality of the 802.11 radio band.

Viewing a Summary of the Air Quality (CLI)

See a summary of the air quality for the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality summary**

Viewing the Worst Air Quality Information for all Access Points on a Radio Band (CLI)

See information for the 802.11a/n/ac or 802.11b/g/n access point with the worst air quality by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality worst**

Viewing the Air Quality for an Access Point on a Radio Band (CLI)

See the air quality information for a specific access point on the 802.11 radio band by entering this command:

show {**802.11a** | **802.11b**} **cleanair air-quality** *Cisco_AP*

Viewing the Air Quality for an Access Point by Device Type (CLI)

- See information for all of the interferers detected by a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

  show {802.11a | 802.11b} cleanair device ap *Cisco_AP*

- See information for all of the interferers of a specific device type on the 802.11a/n or 802.11b/g/n radio band by entering this command:

  show {802.11a | 802.11b} cleanair device type *type*

  where you choose *type* as one of the following:

  - **802.11a**
    - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
    - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
    - **canopy**—A canopy bridge device
    - **cont-tx**—A continuous transmitter

- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video**—A video device
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device

- **802.11b**
  - **bt-link**—A bluetooth link device
  - **bt-discovery**—A bluetooth discovery device
  - **ble-beacon**—A BLE beacon device
  - **mw-oven—**A microwave oven device
  - **802.11-fh—**An 802.11 frequency-hopping device
  - **802.15.4**—An 802.15.4 device
  - **tdd-tx**—A time division duplex (TDD) transmitter
  - **jammer**—A jamming device
  - **cont-tx**—A continuous transmitter
  - **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
  - **video**—A video device
  - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
  - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
  - **superag**—An 802.11 SuperAG device
  - **canopy**—A canopy bridge device
  - **wimax-mobile**—A WiMAX mobile device
  - **wimax-fixed**—A WiMAX fixed device
  - **msft-xbox**—A Microsoft Xbox device

Detecting Persistent Sources of Interference (CLI)

See a list of persistent sources of interference for a specific access point on the 802.11a/n/ac or 802.11b/g/n radio band by entering this command:

show ap auto-rf {**802.11a** | **802.11b**} *Cisco_AP*

CHAPTER 134

Configuring a Spectrum Expert Connection

- Spectrum Expert Connection, on page 931
- Configuring Spectrum Expert (GUI), on page 931

Spectrum Expert Connection

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 Spectrum Expert application (referred to as a *Spectrum Expert console*). You can initiate the Spectrum Expert connection semi-automatically from Prime Infrastructure or by manually launching it from the controller. This section provides instructions for the latter.

Note The Cisco Aironet Access Point Module for Wireless Security and Spectrum Intelligence (WSSI) for the Cisco Aironet 3600 Series Access Point tightly couples data connectivity, spectrum analysis, and security threat detection and mitigation into a single, multipurpose access point. With WSSI you have to use Metageek Chanalyzer Pro with CleanAir support and not Spectrum expert for wIPS, CleanAir and spectrum analysis.

This section contains the following subsections:

Configuring Spectrum Expert (GUI)

Before you begin

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.

Step 1 Ensure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.

Step 2 Configure the access point for SE-Connect mode using the controller GUI or CLI.

Note The SE-Connect mode is set for the entire access point, not just a single radio. However, the Spectrum Expert console connects to a single radio at a time.

If you are using the controller GUI, follow these steps:

a) Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.
b) Click the name of the desired access point to open the All APs > Details for page.
c) Choose **SE-Connect** from the AP Mode drop-down list. This mode is available only for access points that are capable of supporting Cisco CleanAir functionality. For the SE-Connect mode to appear as an available option, the access point must have at least one spectrum-capable radio in the Enable state.
d) Click **Apply** to commit your changes.
e) Click **OK** when prompted to reboot the access point.

If you are using the CLI, follow these steps:

a) To configure the access point for SE-Connect mode, enter this command:

   config ap mode se-connect *Cisco_AP*

b) When prompted to reboot the access point, enter **Y.**
c) To verify the SE-Connect configuration status for the access point, enter this command:

   show ap config {**802.11a** | **802.11b**} *Cisco_AP*

   Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500
...
Spectrum Management Information
        Spectrum Management Capable.............. Yes
        Spectrum Management Admin State.......... Enabled
        Spectrum Management Operation State...... Up
        Rapid Update Mode........................ Disabled
        Spectrum Expert connection............... Enabled
   Spectrum Sensor State.................. Configured (Error code = 0)
```

Step 3 On the Windows PC, access the Cisco Software Center from this URL:

http://www.cisco.com/cisco/software/navigator.html

Step 4 Click **Product > Wireless > Cisco Spectrum Intelligence** > **Cisco Spectrum Expert** > **Cisco Spectrum Expert Wi-Fi**, and then download the Spectrum Expert 4.0 executable (*.exe) file.

Step 5 Run the Spectrum Expert application on the PC.

Step 6 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.

Note 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.

Note On the controller GUI, the NSI key appears in the Network Spectrum Interface Key field (below the Port Number field) on the All APs > Details for page. To view the NSI key from the controller CLI, enter the **show ap config** {**802.11a** | **802.11b**} *Cisco_AP* command.

When an access point in SE-Connect mode joins a controller, it sends a Spectrum Capabilities notification message, and the controller responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key

generated by the controller for use in NSI authentication. The controller 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. The Number of Spectrum Expert Connections text box on the 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page of the controller GUI shows the number of Spectrum Expert applications that are currently connected to the access point radio.

Step 7 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.

Step 8 Use the Spectrum Expert application to view and analyze spectrum data from the access point.

PART IX

FlexConnect

- FlexConnect, on page 937
- Configuring FlexConnect ACLs, on page 957
- Configuring FlexConnect Groups, on page 963
- Configuring AAA Overrides for FlexConnect, on page 975
- FlexConnect AP Image Upgrades, on page 981

CHAPTER 135

FlexConnect

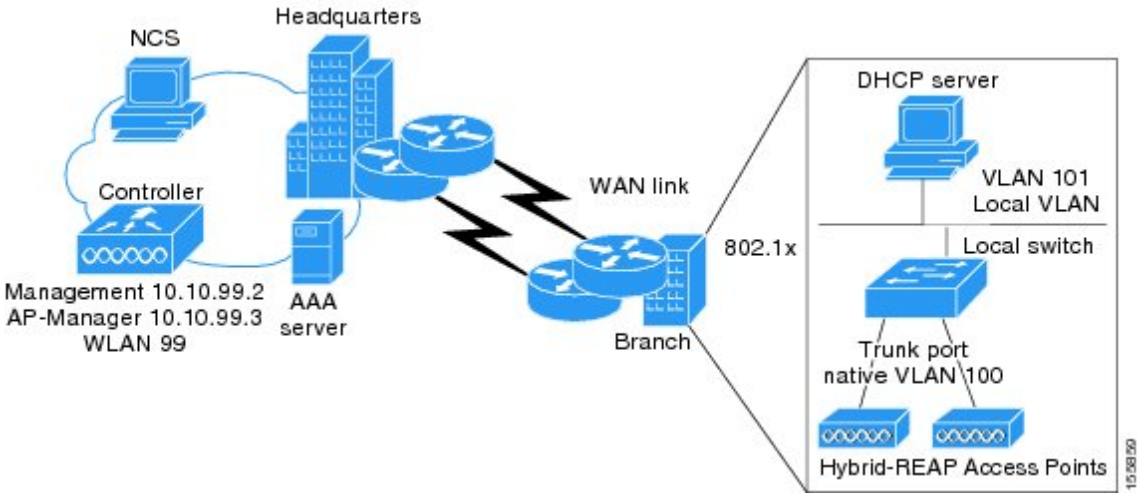
- Information About FlexConnect, on page 937
- Restrictions on FlexConnect, on page 942
- Configuring FlexConnect, on page 944

Information About FlexConnect

FlexConnect (previously known as Hybrid Remote Edge Access Point or H-REAP) is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points (AP) in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect access point can also perform local authentication.

Figure 61: FlexConnect Deployment

The figure below shows a typical FlexConnect deployment.



The controller software has a more robust fault tolerance methodology to FlexConnect access points. In previous releases, whenever a FlexConnect access point disassociates from a controller, it moves to the standalone mode. The clients that are centrally switched are disassociated. However, the FlexConnect access point continues to serve locally switched clients. When the FlexConnect access point rejoins the controller

(or a standby controller), all clients are disconnected and are authenticated again. This functionality has been enhanced and the connection between the clients and the FlexConnect access points are maintained intact and the clients experience seamless connectivity. When both the access point and the controller have the same configuration, the connection between the clients and APs is maintained.

After the client connection has been established, the controller does not restore the original attributes of the client. The client username, current rate and supported rates, and listen interval values are reset to the default values only after the session timer expires.

There is no deployment restriction on the number of FlexConnect access points per location. Multiple FlexConnect groups can be defined in a single location.

The controller can send multicast packets in the form of unicast or multicast packets to the access point. In FlexConnect mode, the access point can receive multicast packets only in unicast form.

FlexConnect access points support a 1-1 network address translation (NAT) configuration. They also support port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option. FlexConnect access points also support a many-to-one NAT/PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.

Note Although NAT and PAT are supported for FlexConnect access points, they are not supported on the corresponding controller. Cisco does not support configurations in which the controller is behind a NAT/PAT boundary.

VPN and PPTP are supported for locally switched traffic if these security types are accessible locally at the access point.

FlexConnect access points support multiple SSIDs.

Workgroup bridges and Universal Workgroup bridges are supported on FlexConnect access points for locally switched clients.

FlexConnect supports IPv6 clients by bridging the traffic to local VLAN, similar to IPv4 operation. FlexConnect supports Client Mobility for a group of up to 100 access points.

The access point does not have to reboot when moving from local to FlexConnect mode.

Note For the Cisco Flex 7510 WLC, auto convert mode is available on the CLI. The auto convert mode triggers the change on all the connected APs. The change of the mode from Local to FlexConnect and the reboot works in conjunction with the auto convert mode for the Cisco Flex 7510 WLC.

Note When AP is changed from local to FlexConnect it will not reboot, but when it is changed from FlexConnect to local it reboots and displays the following error message, "Warning: Changing AP Mode will reboot the AP and will rejoin the controller afer a few minutes. Are you sure you want to continue?" but CLI remains the same. Changing the AP's mode will also cause the AP to reboot.

FlexConnect Authentication Process

When an access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image and configuration from the controller, and initializes the radio. It saves the downloaded configuration in nonvolatile memory for use in standalone mode.

Note Once the access point is rebooted after downloading the latest controller software, it must be converted to the FlexConnect mode.

Note 802.1X is not supported on the AUX port for Cisco 2700 series APs.

A FlexConnect access point can learn the controller IP address in one of these ways:

- If the access point has been assigned an IP address from a DHCP server, it can discover a controller through the regular CAPWAP or LWAPP discovery process.

  Note OTAP is not supported.

- If the access point has been assigned a static IP address, it can discover a controller through any of the discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast, we recommend DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.
- If you want the access point to discover a controller from a remote network where CAPWAP or LWAPP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point CLI) the controller to which the access point is to connect.

  Note For more information about how access points find controllers, see the controller deployment guide at: http://www.cisco.com/c/en/us/td/docs/wireless/technology/controller/deployment/guide/dep.html.

When a FlexConnect access point can reach the controller (referred to as the connected mode), the controller assists in client authentication. When a FlexConnect access point cannot access the controller, the access point enters the standalone mode and authenticates clients by itself.

Note The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

When a client associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication

(open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- central authentication, central switching—In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.
- central authentication, local switching—In this state, the controller handles client authentication, and the FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.

  Note For the FlexConnect local switching, central authentication deployments, if there is a passive client with a static IP address, it is recommended to disable the Learn Client IP Address feature under the **WLAN** > **Advanced** tab.

- local authentication, local switching—In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

  In connected mode, the access point provides minimal information about the locally authenticated client to the controller. The following information is not available to the controller:

  - Policy type
  - Access VLAN
  - VLAN name
  - Supported rates
  - Encryption cipher

    Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 576 bytes. In local authentication, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.

    Note Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode.

  - Notes about local authentication are as follows:
    - Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.
    - Local RADIUS on the controller is not supported.
    - Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information.
    - Local authentication in connected mode requires a WLAN configuration.

Note When locally switched clients that are connected to a FlexConnect access point renew the IP addresses, on joining back, the client continues to stay in the run state. These clients are not reauthenticated by the controller.

- authentication down, switch down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected mode.
- authentication down, local switching—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a FlexConnect access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the "local authentication, local switching" state and continue new client authentications. In controller software release 4.2 or later releases, this configuration is also correct for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or CCKM, but these authentication types require that an external RADIUS server be configured. You can also configure a local RADIUS server on a FlexConnect access point to support 802.1X in a standalone mode or with local authentication.

Other WLANs enter either the "authentication down, switching down" state (if the WLAN was configured for central switching) or the "authentication down, local switching" state (if the WLAN was configured for local switching).

When FlexConnect access points are connected to the controller (rather than in standalone mode), the controller uses its primary RADIUS servers and accesses them in the order specified on the RADIUS Authentication Servers page or in the **config radius auth add** CLI command (unless the server order is overridden for a particular WLAN). However, to support 802.1X EAP authentication, FlexConnect access points in standalone mode need to have their own backup RADIUS server to authenticate clients.

Note A controller does not use a backup RADIUS server. The controller uses the backup RADIUS server in local authentication mode.

You can configure a backup RADIUS server for individual FlexConnect access points in standalone mode by using the controller CLI or for groups of FlexConnect access points in standalone mode by using either the GUI or CLI. A backup server configured for an individual access point overrides the backup RADIUS server configuration for a FlexConnect.

When web-authentication is used on FlexConnect access points at a remote site, the clients get the IP address from the remote local subnet. To resolve the initial URL request, the DNS is accessible through the subnet's default gateway. In order for the controller to intercept and redirect the DNS query return packets, these packets must reach the controller at the data center through a CAPWAP connection. During the web-authentication process, the FlexConnect access points allows only DNS and DHCP messages; the access points forward the DNS reply messages to the controller before web-authentication for the client is complete. After web-authentication for the client is complete, all the traffic is switched locally.

Note If your controller is configured for NAC, clients can associate only when the access point is in connected mode. When NAC is enabled, you need to create an unhealthy (or quarantined) VLAN so that the data traffic of any client that is assigned to this VLAN passes through the controller, even if the WLAN is configured for local switching. After a client is assigned to a quarantined VLAN, all of its data packets are centrally switched. See the Configuring Dynamic Interfaces section for information about creating quarantined VLANs and the Configuring NAC Out-of-Band section for information about configuring NAC out-of-band support.

When a FlexConnect access point enters into a standalone mode, the following occurs:

- The access point checks whether it is able to reach the default gateway via ARP. If so, it will continue to try and reach the controller.

If the access point fails to establish the ARP, the following occurs:

- The access point attempts to discover for five times and if it still cannot find the controller, it tries to renew the DHCP on the ethernet interface to get a new DHCP IP.
- The access point will retry for five times, and if that fails, the access point will renew the IP address of the interface again, this will happen for three attempts.
- If the three attempts fail, the access point will fall back to the static IP and will reboot (only if the access point is configured with a static IP).
- Reboot is done to remove the possibility of any unknown error the access point configuration.

Once the access point reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and allows client connectivity again.

Restrictions on FlexConnect

- You can deploy a FlexConnect access point with either a static IP address or a DHCP address. In the case of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- FlexConnect supports up to four fragmented packets or a minimum 576-byte maximum transmission unit (MTU) WAN link.
- Round-trip latency must not exceed 300 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. In cases where you cannot achieve the 300 milliseconds round-trip latency, you can configure the access point to perform local authentication.
- Client connections are restored only for locally switched clients that are in the RUN state when the access point moves from standalone mode to connected mode.
- The configuration on the controller must be the same between the time the access point went into standalone mode and the time the access point came back to connected mode. Similarly, if the access point is falling back to a secondary or backup controller, the configuration between the primary and secondary or backup controller must be the same.
- A newly connected access point cannot be booted in FlexConnect mode.
- To use CCKM fast roaming with FlexConnect access points, you must configure FlexConnect Groups.

- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- The primary and secondary controllers for a FlexConnect access point must have the same configuration. Otherwise, the access point might lose its configuration, and certain features (such as WLAN overrides, VLANs, static channel number, and so on) might not operate correctly. In addition, make sure to duplicate the SSID of the FlexConnect access point and its index number on both controllers.
- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are properly configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Do not connect access points in FlexConnect mode directly to a 2504 WLC.
- If you configure a FlexConnect access point with a syslog server configured on the access point, after the access point is reloaded and the native VLAN other than 1, at time of initialization, few syslog packets from the access point are tagged with VLAN ID 1. This is a known issue.
- MAC Filtering is not supported on FlexConnect access points in standalone mode. However, MAC Filtering is supported on FlexConnect access points in connected mode with local switching and central authentication. Also, Open SSID, MAC Filtering, and RADIUS NAC for a locally switched WLAN with FlexConnect access points is a valid configuration where MAC is checked by ISE.
- FlexConnect does not support IPv6 ACLs, neighbor discovery caching, and DHCPv6 snooping of IPv6 NDP packets.
- FlexConnect does not display any IPv6 client addresses within the client detail page.
- FlexConnect Access Points with Locally Switched WLAN cannot perform IP Source Guard and prevent ARP spoofing. For Centrally Switched WLAN, the wireless controller performs the IP Source Guard and ARP Spoofing.
- To prevent ARP spoofing attacks in FlexConnect AP with Local Switching, we recommend that you use ARP Inspection.
- When you enable local switching on WLAN for the FlexConnect APs, then APs perform local switching. However, for the APs in local mode, central switching is performed.

  A scenario where the roaming of a client between FlexConnect mode AP and Local mode AP is not supported. The client may not get correct IP address due to VLAN difference after the move. Also, L2 and L3 roaming between FlexConnect mode AP and Local mode AP are not supported.
- For Wi-Fi Protected Access version 2 (WPA2) in FlexConnect standalone mode or local-auth in connected mode or CCKM fast-roaming in connected mode, only Advanced Encryption Standard (AES) is supported.
- For Wi-Fi Protected Access (WPA) in FlexConnect standalone mode or local-auth in connected mode or CCKM fast-roaming in connected mode, only Temporal Key Integrity Protocol (TKIP) is supported.
- WPA2 with TKIP and WPA with AES is not supported in standalone mode, local-auth in connected mode, and CCKM fast-roaming in connected mode.
- AVC is not supported on APs in FlexConnect local switched mode.

- Flexconnect access points in WIPS mode can significantly increase the bandwidth utilization depending on the activity detected by the access points. If the rules have forensics enabled, the link utilization can go up by almost 100kbps.
- Local authentication fall back is not supported when user is not available in the external RADIUS server.
- For WLAN configured for the FlexConnect AP in the local switching and local authentication, synchronization of dot11 clients information is supported.
- It is not possible for the Cisco WLC to detect if an AP has dissociated and with that whether the radio is in operational state or non-operational state.

  When a FlexConnect AP dissociates from the Cisco WLC, the AP can still serve the clients with the radios being operational; however, with all other AP modes, the radios go into non-operational state.
- When you apply a configuration change to a locally switched WLAN, the access point resets the radio, causing associated client devices to disassociate (including the clients that are not associated with the modified WLAN). However, this behavior does not occur if the modified WLAN is centrally switched. We recommend that you modify the configuration only during a maintenance window. This is also applicable when a centrally switched WLAN is changed to a locally switched WLAN.
- ACL override is not supported in TKIP encrypted clients.
- IRCM is not supported in FlexConnect deployments.

Configuring FlexConnect

Note The configuration tasks must be performed in the order in which they are listed.

Configuring the Switch at a Remote Site

Step 1 Attach the access point that will be enabled for FlexConnect to a trunk or access port on the switch.

Note The sample configuration in this procedure shows the FlexConnect access point connected to a trunk port on the switch.

Step 2 See the sample configuration in this procedure to configure the switch to support the FlexConnect access point.

In this sample configuration, the FlexConnect access point is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers/resources on VLAN 101. A DHCP pool is created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched. The bolded text in the sample configuration shows these settings.

A sample local switch configuration is as follows:

```
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
```

```
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.201.224 255.255.255.224
   default-router 209.165.201.225
   dns-server 192.168.100.167
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 209.165.202.225 255.255.255.224
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 101
 switchport mode trunk
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
 ip address 209.165.201.226 255.255.255.229
end
!
```

Configuring the Controller for FlexConnect

You can configure the controller for FlexConnect in two environments:

- Centrally switched WLAN
- Locally switched WLAN

The controller configuration for FlexConnect consists of creating centrally switched and locally switched WLANs. This table shows three WLAN scenarios.

Table 31: WLANs Example

WLAN	Security	Authentication	Switching	Interface Mapping (VLAN)
employee	WPA1+WPA2	Central	Central	management (centrally switched VLAN)
employee-local	WPA1+WPA2 (PSK)	Local	Local	101 (locally switched VLAN)
guest-central	Web authentication	Central	Central	management (centrally switched VLAN)
employee -local-auth	WPA1+WPA2	Local	Local	101 (locally switched VLAN)

Configuring the Controller for FlexConnect for a Centrally Switched WLAN Used for Guest Access

Before you begin

You must have created guest user accounts. For more information about creating guest user accounts, see the *Cisco Wireless LAN Controller System Management Guide*.

Step 1 Choose **WLANs** to open the **WLANs** page.

Step 2 From the drop-down list, choose **Create New** and click **Go** to open the **WLANs > New page** .

Step 3 From the **Type** drop-down list, choose **WLAN**.

Step 4 In the **Profile Name** text box, enter **guest-central**.

Step 5 In the **WLAN SSID** text box, enter **guest-central**.

Step 6 From the **WLAN ID** drop-down list, choose an ID for the WLAN.

Step 7 Click **Apply**. The **WLANs > Edit** page appears.

Step 8 In the **General** tab, select the **Status** check box to enable the WLAN.

Step 9 In the **Security > Layer 2** tab, choose **None** from the **Layer 2 Security** drop-down list.

Step 10 In the **Security > Layer 3** tab:

a) Choose **None** from the **Layer 3 Security** drop-down list.

b) Choose the **Web Policy** check box.

c) Choose **Authentication**.

If you are using an external web server, you must configure a preauthentication access control list (ACL) on the WLAN for the server and then choose this ACL as the WLAN preauthentication ACL on the Layer 3 tab.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring the Controller for FlexConnect (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 From the drop-down list, choose **Create New** and click **Go** to open the **WLANs > New** page.

Step 3 From the **Type** drop-down list, choose **WLAN**.

Step 4 In the **Profile Name** text box, enter a unique profile name for the WLAN.

Step 5 In the **WLAN SSID** text box, enter a name for the WLAN.

Step 6 From the **WLAN ID** drop-down list, choose the ID number for this WLAN.

Step 7 Click **Apply**.
The **WLANs > Edit** page is displayed.

Step 8 You can configure the controller for FlexConnect in both centrally switched and locally switched WLANs:

Note Do not enable ip-learn on FlexConnect local switched WLAN. When several sites use similar local subnets or overlapping subnets that are terminated on the same WLC, you will see ip-theft false positives. If ip-theft exclusion is enabled on the WLC, the clients might be put in a blocked list or a similar message is displayed to convey the feature behavior.

To configure the controller for FlexConnect in a centrally switched WLAN:

a) In the **General** tab, check the **Status** check box to enable the WLAN.
b) If you have enabled NAC and have created a quarantined VLAN and want to use it for this WLAN, select the interface from the Interface/Interface Group(G) drop-down list in the **General** tab.
c) In the **Security > Layer 2** tab, choose **WPA+WPA2** from the **Layer 2 Security** drop-down list and then set the WPA+WPA2 parameters as required.

To configure the controller for FlexConnect in a locally switched WLAN:

a) In the **General** tab, check the **Status** check box to enable the WLAN.
b) If you have enabled NAC and have created a quarantined VLAN and want to use it for this WLAN, select the interface from the Interface/Interface Group(G) drop-down list in the General tab.
c) In the **Security** > **Layer2** tab, choose **WPA+WPA2** from the **Layer 2 Security** drop-down list and then set the WPA+WPA2 parameters as required.
d) In the **Advanced** tab:

- Check or uncheck the **FlexConnect Local Switching** check box to enable or disable local switching of client data associated with the APs in FlexConnect mode.

  Note The guidelines and limitations for this feature are as follows:

  - When you enable local switching, any FlexConnect access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).
  - When you enable FlexConnect local switching, the controller is enabled to learn the client's IP address by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client's IP address, and the controller periodically drops the client. Disable the client IP address learning feature so that the controller maintains the client connection without waiting to learn the client's IP address. The ability to disable this option is supported only with FlexConnect local switching; it is not supported with FlexConnect central switching.
  - For FlexConnect access points, the interface mapping at the controller for WLANs that is configured for FlexConnect Local Switching is inherited at the access point as the default VLAN tagging. This mapping can be changed per SSID and per FlexConnect access point. Non-FlexConnect access points tunnel all traffic back to the controller, and VLAN tagging is determined by each WLAN's interface mapping.

- Select or unselect the **FlexConnect Local Auth** check box to enable or disable local authentication for the WLAN.
- Select or unselect the **Learn Client IP Address** check box to enable or disable the IP address of the client to be learned.
- Select or unselect the **VLAN based Central Switching** check box to enable or disable central switching on a locally switched WLAN based on AAA overridden VLAN.

Note These are the guidelines and limitations for this feature:

- VLAN based central switching is not supported by mac filter.
- Multicast on overridden interfaces is not supported.
- This feature is available only on a per-WLAN basis, where the WLAN is locally switched.
- IPv6 ACLs, CAC, NAC, and IPv6 are not supported.
- IPv4 ACLs are supported only with VLAN-based central switching enabled and applicable only to central switching clients on the WLAN.
- This feature is applicable to APs in FlexConnect mode in locally switched WLANs.
- This feature is not applicable to APs in Local mode.
- This feature is not supported on APs in FlexConnect mode in centrally switched WLANs.
- This feature is supported on central authentication only.
- This features is not supported on web authentication security clients.
- Layer 3 roaming for local switching clients is not supported.

- Select or unselect the **Central DHCP Processing** check box to enable or disable the feature. When you enable this feature, the DHCP packets received from AP are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
- Select or unselect the **Override DNS** check box to enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.
- Select or unselect the **NAT-PAT** check box to enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.

Step 9 Save the configuration.

Related Topics

Configuring IP-MAC Context Distribution For FlexConnect Local Switching Clients (GUI)

Configuring the Controller for FlexConnect (CLI)

Step 1 **config wlan flexconnect local-switching** *wlan_id* **enable**—Configures the WLAN for local switching.

Note When you enable FlexConnect local switching, the controller waits to learn the client IP address by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Use the **config wlan flexconnect learn-ipaddr** *wlan_id* **disable** command to disable the client IP address learning feature so that the controller maintains the client connection without waiting to learn the client's IP address. The ability to disable this feature is supported only with FlexConnect local switching; it is not supported with FlexConnect central switching. To enable this feature, enter the **config wlan flexconnect learn-ipaddr** *wlan_id* **enable** command.

Note When a WLAN is locally switched (LS), you must use the **config wlan flexconnect learn-ipaddr** *wlan-id* {**enable** | **disable**} command. When the WLAN is centrally switched (CS), you must use the **config wlan learn-ipaddr-cswlan** *wlan-id* {**enable** | **disable**} command.

Step 2 **config wlan flexconnect local-switching** *wlan_id* {**enable** | **disable**}—Configures the WLAN for central switching.

Step 3 **config wlan flexconnect vlan-central-switching** *wlan_id* {**enable** | **disable**}—Configures central switching on a locally switched WLAN based on an AAA overridden VLAN.

The guidelines and limitations for this feature are as follows:

- VLAN based central switching is not supported by mac filter.
- Multicast on overridden interfaces is not supported.
- This feature is available only on a per-WLAN basis, where the WLAN is locally switched.
- IPv6 ACLs, CAC, NAC, and IPv6 are not supported.
- IPv4 ACLs are supported only with VLAN-based central switching enabled and applicable only to central switching clients on the WLAN.
- This feature is applicable to APs in FlexConnect mode in locally switched WLANs.
- This feature is not applicable to APs in Local mode.
- This feature is not supported on APs in FlexConnect mode in centrally switched WLANs.
- This feature is supported on central authentication only.
- This features is not supported on web authentication security clients.
- Layer 3 roaming for local switching clients is not supported.

Step 4 Use these commands to get FlexConnect information:

- **show ap config general** *Cisco_AP*—Shows VLAN configurations.
- **show wlan** *wlan_id*—Shows whether the WLAN is locally or centrally switched.
- **show client detail** *client_mac*—Shows whether the client is locally or centrally switched.

Step 5 Use these commands to obtain debug information:

- **debug flexconnect aaa** {**event** | **error**} {**enable** | **disable**}—Enables or disables debugging of FlexConnect backup RADIUS server events or errors.
- **debug flexconnect cckm** {**enable** | **disable**}—Enables or disables debugging of FlexConnect CCKM.
- **debug flexconnect** {**enable** | **disable**}—Enables or disables debugging of FlexConnect Groups.
- **debug pem state** {**enable** | **disable**}—Enables or disables debugging of the policy manager state machine.
- **debug pem events** {**enable** | **disable**}—Enables or disables debugging of policy manager events.

Configuring an Access Point for FlexConnect

Configuring an Access Point for FlexConnect (GUI)

Before you begin

Ensure that the access point has been physically added to your network.

Note The AP will reboot when you change the AP behavior from Flexconnect to Local.

Step 1 Choose **Wireless** to open the All APs page.

Step 2 Click the name of the desired access point. The **All APs >** > **Details** page appears.

Step 3 From the **AP Mode** drop-down list, choose **FlexConnect** to enable FlexConnect for this access point.

Note The last parameter in the **Inventory** tab indicates whether the access point can be configured for FlexConnect.

Step 4 Click **Apply** to commit your changes and to cause the access point to reboot.

Step 5 Choose the **FlexConnect** tab to open the **All APs > Details for (FlexConnect)** page.

If the access point belongs to a FlexConnect group, the name of the group appears in the **FlexConnect Name** text box.

Step 6 To configure WLAN VLAN mapping, choose from the following options in the drop-down list:

- **Make AP Specific**
- **Remove AP Specific**

Step 7 Select the **VLAN Support** check box and enter the number of the native VLAN on the remote network (such as 100) in the Native VLAN ID text box.

Note By default, a VLAN is not enabled on the FlexConnect access point. After FlexConnect is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller.

Note If PMIPv6 MAG on FlexConnect AP is configured, VLAN Support can be checked or unchecked on the FlexConnect AP. If you check the VLAN Support check box, enter the number of the native VLAN on the remote network in the Native VLAN ID text box.

Note To preserve the VLAN mappings in the access point after an upgrade or downgrade, it is necessary that the access point join is restricted to the controller for which it is primed. That is, no other discoverable controller with a different configuration should be available by other means. Similarly, at the time the access point joins, if it moves across controllers that have different VLAN mappings, the VLAN mappings at the access point may get mismatched.

Note For Cisco 1140 access point, when the native VLAN ID is set, it disconnects and joins back the Cisco 8510 WLC. And after resuming the admin mode for the AP, is disabled.

Step 8 Click **Apply**. The access point temporarily loses its connection to the controller while its Ethernet port is reset.

Step 9 Click the name of the same access point and then click the **FlexConnect** tab.

Step 10 Click **VLAN Mappings** to open the **All APs** > *Access Point Name* **> VLAN Mappings** page.

Step 11 Enter the number of the VLAN from which the clients will get an IP address when doing local switching (VLAN 101, in this example) in the **VLAN ID** text box.

Step 12 To configure Web Authentication ACLs, do the following:

a) Click the **External WebAuthentication ACLs** link to open the ACL mappings page. The ACL Mappings page lists details of WLAN ACL mappings and web policy ACLs.

b) In the **WLAN Id** box, enter the WLAN ID.

c) From the **WebAuth ACL** drop-down list, choose the FlexConnect ACL.

Note To create a FlexConnect ACL, choose **Wireless > FlexConnect Groups > FlexConnect ACLs**, click **New**, enter the FlexConnect ACL name, and click **Apply**.

d) Click **Add**.

e) Click **Apply**.

Step 13 To configure Local Split ACLs:

a) Click the **Local Split ACLs** link to open the ACL Mappings page.

b) In the **WLAN Id** box, enter the WLAN ID.

c) From the **Local-Split ACL** drop-down list, choose the FlexConnect ACL.

Note To create a FlexConnect ACL, choose **Wireless > FlexConnect Groups > FlexConnect ACLs**, click **New**, enter the FlexConnect ACL name, and click **Apply**.

If a client that connects over a WAN link associated with a centrally switched WLAN has to send some traffic to a device present in the local site, the client has to send traffic over CAPWAP to the controller and then get the same traffic back to the local site either over CAPWAP or using some offband connectivity. This process unnecessarily consumes WAN link bandwidth. To avoid this issue, you can use the split tunneling feature, which allows the traffic sent by a client to be classified based on the packet contents. The matching packets are locally switched and the rest of the traffic is centrally switched. The traffic that is sent by the client that matches the IP address of the device present in the local site can be classified as locally switched traffic and the rest of the traffic as centrally switched.

To configure local split tunneling on an AP, ensure that you have enabled DCHP Required on the WLAN, which ensures that the client associating with the split WLAN does DHCP.

Note Local split tunneling is not supported on Cisco 1500 Series, Cisco 1130, and Cisco 1240 access points, and does not work for clients with static IP address.

d) Click **Add**.

Step 14 To configure Central DHCP processing:

a) In the WLAN Id box, enter the WLAN ID with which you want to map Central DHCP.

b) Select or unselect the **Central DHCP** check box to enable or disable Central DHCP for the mapping.

c) Select or unselect the **Override DNS** check box to enable or disable overriding of DNS for the mapping.

d) Select or unselect the **NAT-PAT** check box to enable or disable network address translation and port address translation for the mapping.

e) Click **Add** to add the Central DHCP - WLAN mapping.

Step 15 To map a locally switched WLAN with a WebAuth ACL, follow these steps:

a) In the **WLAN Id** box, enter the WLAN ID.

b) From the **WebAuth ACL** drop-down list, choose the FlexConnect ACL.

Note To create a FlexConnect ACL, choose **Wireless > FlexConnect Groups > FlexConnect ACLs**, click **New**, enter the FlexConnect ACL name, and click **Apply**.

c) Click **Add**.

Note The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.

Step 16 From the **WebPolicy ACL** drop-down list, choose a FlexConnect ACL and then click **Add** to configure the FlexConnect ACL as a web policy.

Note You can configure up to 16 Web Policy ACLs that are specific to an access point.

Step 17 Click **Apply**.

Step 18 Click **Save Configuration**.

Note Repeat this procedure for any additional access points that need to be configured for FlexConnect at the remote site.

Configuring an Access Point for FlexConnect (CLI)

Note The AP will reboot when you change the AP behavior from Flexconnect to Local.

- **config ap mode flexconnect** *Cisco_AP*—Enables FlexConnect for this access point.
- **config ap flexconnect radius auth set** {**primary | secondary**} *ip_address auth_port secret Cisco_AP*—Configures a primary or secondary RADIUS server for a specific FlexConnect access point.

  Note Only the Session Timeout RADIUS attribute is supported in standalone mode. All other attributes as well as RADIUS accounting are not supported.

  Note To delete a RADIUS server that is configured for a FlexConnect access point, enter the **config ap flexconnect radius auth delete** {**primary | secondary**} *Cisco_AP* command.

- **config ap flexconnect vlan wlan** *wlan_id vlan-id Cisco_AP*—Enables you to assign a VLAN ID to this FlexConnect access point. By default, the access point inherits the VLAN ID associated to the WLAN.
- **config ap flexconnect vlan** {**enable | disable**} *Cisco_AP*—Enables or disables VLAN tagging for this FlexConnect access point. By default, VLAN tagging is not enabled. After VLAN tagging is enabled on the FlexConnect access point, WLANs that are enabled for local switching inherit the VLAN assigned at the controller.

- **config ap flexconnect vlan native** *vlan-id Cisco_AP*—Enables you to configure a native VLAN for this FlexConnect access point. By default, no VLAN is set as the native VLAN. One native VLAN must be configured per FlexConnect access point (when VLAN tagging is enabled). Make sure the switch port to which the access point is connected has a corresponding native VLAN configured as well. If the FlexConnect access point's native VLAN setting and the upstream switch port native VLAN do not match, the access point cannot transmit packets to and from the controller.

  Note To save the VLAN mappings in the access point after an upgrade or downgrade, you should restrict the access point to join the controller for which it is primed. No other discoverable controller with a different configuration should be available by other means. Similarly, at the time the access point joins, if it moves across controllers that have different VLAN mappings, the VLAN mappings at the access point might get mismatched.

- Configure the mapping of a Web-Auth or a Web Passthrough ACL to a WLAN for an access point in FlexConnect mode by entering this command:

  config ap flexconnect web-auth wlan *wlan_id cisco_ap acl_name* {**enable** | **disable**}

  Note The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.

- Configure a Policy ACL on an AP in FlexConnect mode by entering this command:

  config ap flexconnect policy acl {**add** | **delete**} *acl_name cisco_ap*

  Note You can configure up to 16 Policy ACLs that are specific to an access point.

- To configure local split tunneling on a per-AP basis, enter this command:

  config ap local-split {**enable** | **disable**} *wlan-id* **acl** *acl-name ap-name*

- Configure central DHCP on the AP per WLAN by entering this command:

  config ap flexconnect central-dhcp *wlan-id ap-name* {**enable override dns** | **disable** | **delete**}

  Note The gratuitous ARP for the gateway is sent by the access point to the client, which obtained an IP address from the central site. This is performed to proxy the gateway by the access point.

Use these commands on the FlexConnect access point to get status information:

- **show capwap reap status**—Shows the status of the FlexConnect access point (connected or standalone).
- **show capwap reap association**—Shows the list of clients associated with this access point and their SSIDs.

Use these commands on the FlexConnect access point to get debug information:

- **debug capwap reap**—Shows general FlexConnect activities.
- **debug capwap reap mgmt**—Shows client authentication and association messages.
- **debug capwap reap load**—Shows payload activities, which are useful when the FlexConnect access point boots up in standalone mode.
- **debug dot11 mgmt interface**—Shows 802.11 management interface events.
- **debug dot11 mgmt msg**—Shows 802.11 management messages.
- **debug dot11 mgmt ssid**—Shows SSID management events.
- **debug dot11 mgmt state-machine**—Shows the 802.11 state machine.
- **debug dot11 mgmt station**—Shows client events.

Configuring an Access Point for Local Authentication on a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID of the WLAN. The **WLANs > Edit** page appears.

Step 3 Clicked the **Advanced** tab to open the **WLANs** > **Edit (WLAN Name)** page.

Step 4 Select the **FlexConnect Local Switching** check box to enable FlexConnect local switching.

Step 5 Select the **FlexConnect Local Auth** check box to enable FlexConnect local authentication.

Caution Do not connect access points in FlexConnect mode directly to 2500 Series Controllers.

Step 6 Click **Apply** to commit your changes.

Configuring an Access Point for Local Authentication on a WLAN (CLI)

Before you begin

Before you begin, you must have enabled local switching on the WLAN where you want to enable local authentication for an access point. For instructions on how to enable local switching on the WLAN, see the Configuring the Controller for FlexConnect (CLI) section.

Procedure

- **config wlan flexconnect ap-auth** *wlan_id* {**enable** | **disable**}—Configures the access point to enable or disable local authentication on a WLAN.

Caution Do not connect the access points in FlexConnect mode directly to Cisco 2500 Series Controllers.

- **show wlan** *wlan-id* —Displays the configuration for the WLAN. If local authentication is enabled, the following information appears:

```
. . .
. . .
Web Based Authentication..................... Disabled
   Web-Passthrough........................... Disabled
   Conditional Web Redirect.................. Disabled
   Splash-Page Web Redirect.................. Disabled
   Auto Anchor............................... Disabled
   FlexConnect Local Switching.................... Enabled
   FlexConnect Local Authentication............... Enabled
   FlexConnect Learn IP Address................... Enabled
   Client MFP................................ Optional
   Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping................................. Disabled
Roamed Call Re-Anchor Policy.................. Disabled
. . .
. . .
```

Connecting Client Devices to WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created in the Configuring the Controller for FlexConnect section.

In the example scenarios (see the Configuring the Controller for FlexConnect section), there are three profiles on the client:

1. To connect to the “employee” WLAN, create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. After the client becomes authenticated, the client gets an IP address from the management VLAN of the controller.
2. To connect to the “local-employee” WLAN, create a client profile that uses WPA/WPA2 authentication. After the client becomes authenticated, the client gets an IP address from VLAN 101 on the local switch.
3. To connect to the “guest-central” WLAN, create a client profile that uses open authentication. After the client becomes authenticated, the client gets an IP address from VLAN 101 on the network local to the access point. After the client connects, the local user can type any HTTP address in the web browser. The user is automatically directed to the controller to complete the web-authentication process. When the web login page appears, the user enters the username and password.

To determine if a client’s data traffic is being locally or centrally switched, choose **Monitor > Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the **Data Switching** parameter under **AP Properties**.

CHAPTER 136

Configuring FlexConnect ACLs

- FlexConnect Access Control Lists, on page 957
- Restrictions for FlexConnect Access Control Lists, on page 957
- Configuring FlexConnect Access Control Lists (GUI), on page 959
- Configuring FlexConnect Access Control Lists (CLI), on page 960
- Viewing and Debugging FlexConnect Access Control Lists (CLI), on page 962

FlexConnect Access Control Lists

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs enable access control of network traffic. After ACLs are configured on the controller, you can apply them to the management interface, the AP-Manager interface, any of the dynamic interfaces, or a WLAN. ACLs enable you to control data traffic to and from wireless clients or to the controller CPU. You can configure ACLs on FlexConnect access points to enable effective usage and access control of locally switched data traffic on an access point.

The FlexConnect ACLs can be applied to VLAN interfaces on access points in both the Ingress and Egress mode.

Existing interfaces on an access point can be mapped to ACLs. The interfaces can be created by configuring a WLAN-VLAN mapping on a FlexConnect access point.

The FlexConnect ACLs can be applied to an access point's VLAN only if VLAN support is enabled on the FlexConnect access point.

Related Information

- To set up location authentication, see the FlexConnect chapter of the *Enterprise Mobility Design Guide*.
- Wireless BYOD for FlexConnect Deployment Guide

This section contains the following subsections:

Restrictions for FlexConnect Access Control Lists

- FlexConnect ACLs can be applied only to FlexConnect access points. The configurations applied are per AP and per VLAN.

- FlexConnect ACLs are supported on the native VLAN.

Note FlexConnect ACLs are not supported on native VLAN when setting comes from FlexConnect Group.

- You can configure up to 512 ACLs on a Cisco Wireless Controller. Each rule has parameters that affect its action. When a packet matches all the parameters pertaining to a rule, the action set pertaining to that rule is applied to the packet.
  - You can define 64 IPv4 address based rules in each ACL.
- Non-FlexConnect ACLs that are configured on the controller cannot be applied to a FlexConnect AP.
- FlexConnect ACLs do not support direction per rule. Unlike normal ACLs, Flexconnect ACLs cannot be configured with a direction. An ACL as a whole needs to be applied to an interface as ingress or egress.
- ACLs in your network might have to be modified because Control and Provisioning of Wireless Access Points (CAPWAP) use ports that are different from the ones used by the Lightweight Access Point Protocol (LWAPP).
- All ACLs have an implicit *deny all rule* as the last rule. If a packet does not match any of the rules, it is dropped by the corresponding access point.
- ACLs mapping on the VLANs that are created on an AP using WLAN-VLAN mapping, should be performed on a per-AP basis only. VLANs can be created on a FlexConnect group for AAA override. These VLANs will not have any mapping for a WLAN.
- ACLs for VLANs that are created on a FlexConnect group should be mapped only on the FlexConnect group. If the same VLAN is present on the corresponding AP as well as the FlexConnect group, AP VLAN will take priority. This means that if no ACL is mapped on the AP, the VLAN will not have any ACL, even if the ACL is mapped to the VLAN on the FlexConnect group.
- Ensure the FlexConnect ACL and the regular ACL names are not the same while configuring a WLAN for FlexConnect local switching.
- AAA client ACL support:
  - Before the AAA sends the client ACL, ensure that the ACL is created on a FlexConnect group or an AP. The ACL is not downloaded to the AP dynamically when the client gets associated with the AP.
  - A maximum of 96 ACLs can be configured on an AP. Each ACL can have a maximum of 64 rules.
  - FlexConnect ACLs do not have directions. The entire ACL is applied as ingress or egress.
  - The ACL returned by the AAA is applied on both ingress and egress on the 802.11 side of the client.

Note A Local Switching WLAN is configured and ACL is mapped to a FlexConnect group with an ACL. The ACL has set of 'deny and permit' rules. When you associate a client to the WLAN, the client needs to have DHCP permit rule added for getting the IP address.

Configuring FlexConnect Access Control Lists (GUI)

Step 1 Choose **Security** > **Access Control Lists** > **FlexConnect Access Control Lists**.

The **FlexConnect ACL** page is displayed.

This page lists all the FlexConnect ACLs configured on the controller. This page also shows the FlexConnect ACLs created on the corresponding controller. To remove an ACL, hover your mouse over the blue drop-down arrow that is next to the corresponding ACL name and choose **Remove**.

Step 2 Add a new ACL by clicking **New**.

The **Access Control Lists** > **New** page is displayed.

Step 3 In the **Access Control List Name** field, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

Step 5 Click the name of the new ACL after the **Access Control Lists** page is displayed again.

When the **Access Control Lists > Edit** page appears, click **Add New Rule**.

The **Access Control Lists** > **Rules** > **New** page is displayed.

Step 6 Configure an IP address based rule for a given FlexConnect ACL as follows:

a) Choose **IP Rule** to create an IP address based rule.

The **Access Control Lists** > **Rules** > **New** page is displayed.

b) The controller supports up to 64 rules for each IP address-based ACL. These rules are listed in order from 1 to 64. In the **Sequence** field, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

Note If rules 1 to 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number of a rule, the sequence numbers of the other rules are automatically adjusted to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

c) From the **Source** drop-down list, choose one of these options to specify the source of the packets to which this ACL is applicable:

- **Any**—Any source (This is the default value.).
- **IP Address**—A specific source. If you choose this option, enter the IP address and netmask of the source in the corresponding fields.

d) From the **Destination** drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- **Any**—Any destination (This is the default value.).
- **IP Address**—A specific destination. If you choose this option, enter the IP address and the details of the destination in the relevant fields.

e) From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can use are the following:

- **Any**—Any protocol (This is the default value.).
- **TCP**
- **UDP**
- **ICMP**—Internet Control Message Protocol
- **ESP**—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP in IP**—Permits or denies IP-in-IP packets
- **Eth Over IP**—Ethernet-over-Internet Protocol
- **OSPF**—Open Shortest Path First
- **Other**—Any other Internet-Assigned Numbers Authority (IANA) protocol

Note If you choose Other, enter the number of the desired protocol in the **Protocol** field. You can find the list of available protocols in the INAI website.

The controller can permit or deny only the IP packets in an ACL. Other types of packets (such as Address Resolution Protocol (ARP) packets) cannot be specified.

If you choose TCP or UDP, two more parameters—Source Port and Destination Port, are displayed. These parameters enable you to choose a specific source port and destination port or port range. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications, such as Telnet, SSH, HTTP, and so on.

f) From the **DSCP** drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header field that can be used to define the quality of service across the Internet.

- **Any**—Any DSCP (This is the default value.).
- **Specific**—A specific DSCP from 0 to 63, which you enter in the **DSCP** field.

g) From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets, or **Permit** to cause this ACL to allow packets. The default value is **Deny**.

h) Click **Apply**.

The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.

i) Repeat this procedure to add more rules, if required, for this ACL.

Configuring FlexConnect Access Control Lists (CLI)

Use the following commands on the controller to configure FlexConnect ACLs:

Procedure

- Create or delete an ACL on a FlexConnect access point by entering this command:

  config flexconnect acl { **create | delete** } *name*

  The IPv4 ACL name of up to 32 characters is supported.

- Associate a FlexConnect ACL to a WLAN.
  a) Enable web authentication by entering this command:

     config wlan security web-auth enable *wlan_id*

  b) Configure the FlexConnect ACL to a WLAN by entering this command:

     config wlan security web-auth flexacl *wlan_id acl_name*

- Configure an IP address based rule for an ACL
  a) Add an IP address based rule to the FlexConnect ACL by entering this command:

     config flexconnect acl rule add *acl-name rule-index*

  b) Configure a rule's source IP address and netmask by entering this command:

     config flexconnect acl rule source address *acl-name rule-index ipv4-addr subnet-mask*

  c) Configure a rule's source port range by entering this command:

     config flexconnect acl rule source port range *acl-name rule-index start-port end-port*

  d) Configure a rule's destination IP address and netmask by entering this command:

     IPv4—**config flexconnect acl rule destination address** *acl-name rule-index ipv4-addr subnet-mask*

  e) Configure a rule's destination port range by entering this command:

     config flexconnect acl rule destination port range*acl-name rule-index start-port end-port*

  f) Configure the rule's IP protocol by entering this command:

     config flexconnect acl rule protocol *acl-name rule-index* **protocol**

     Specify an index value between 0 and 64. Specify the protocol value between 0 and 255 or 'any'. The default is 'any.'

  g) Specify the differentiated services code point (DSCP) value of the rule index by entering this command:

     config flexconnectacl rule dscp *acl-name rule-index dscp-value*

     DSCP is an IP header that can be used to define the quality of service across the Internet. Enter a value between 0 and 63 or the value **any**. The default value is **any**.

  h) Set the Permit or deny action to the rule by entering this command:

     config flexconnect acl rule actionacl-name *rule-index* **{permit |deny}**

  i) Change the index value for an ACL rule by entering this command:

     config flexconnectacl rule change index *acl-name old-index new-index*

  j) Swap the index values between two rules by entering this command:

config flexconnect acl rule swap *acl-name index-1 index-2*

k) Delete a rule from the FlexConnect ACL by entering this command:

config flexconnect acl rule delete *name*

l) Apply an ACL to the FlexConnect access point by entering this command:

config flexconnect acl apply *acl-name*

- [Optional] Add a VLAN on a FlexConnect access point by entering this command:

  config ap flexconnect vlan add *acl vlan-id ingress-aclname egress-acl-name ap-name*

Viewing and Debugging FlexConnect Access Control Lists (CLI)

Use the following commands on the controller to view information related to FlexConnect ACLs:

Procedure

- **show flexconnect acl summary**—Displays a summary of the ACLs.
- **show client detail** *mac-address*—Displays AAA override ACL.
- **show flexconnect acl detailed acl-name**—Displays the detailed information about the ACL.
- **debug flexconnect acl {enable | disable}**—Enables or disables the debugging of FlexConnect ACL.
- **debug capwap reap**—Enables debugging of CAPWAP.

CHAPTER 137

Configuring FlexConnect Groups

- Information About FlexConnect Groups, on page 963
- Configuring FlexConnect Groups, on page 966
- Configuring VLAN-ACL Mapping on FlexConnect Groups, on page 971
- Configuring WLAN-VLAN Mappings on FlexConnect Groups, on page 972

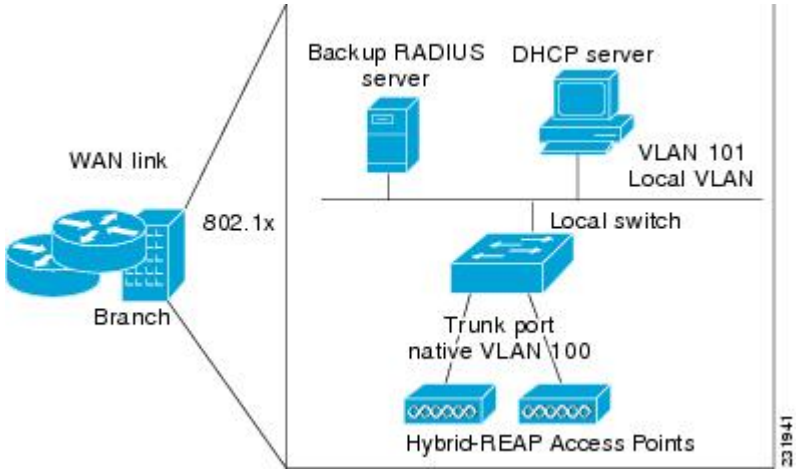
Information About FlexConnect Groups

To organize and manage your FlexConnect access points, you can create FlexConnect Groups and assign specific access points to them.

All of the FlexConnect access points in a group share the same backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple FlexConnect access points in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a FlexConnect rather than having to configure the same server on each access point.

Figure 62: FlexConnect Group Deployment

The following figure shows a typical FlexConnect deployment with a backup RADIUS server in the branch office.



FlexConnect Groups and Backup RADIUS Servers

You can configure the controller to allow a FlexConnect access point in standalone mode to perform full 802.1X authentication to a backup RADIUS server. You can configure a primary backup RADIUS server or both a primary and secondary backup RADIUS server. These servers can be used when the FlexConnect access point is in of these two modes: standalone or connected.

FlexConnect Groups and CCKM

FlexConnect Groups are required for CCKM fast roaming to work with FlexConnect access points. CCKM fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that might associate, sending the CCKM cache for all 100 clients is not practical. If you create a FlexConnect that includes a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM cache is distributed among those four access points only when the clients associate to one of them.

Note CCKM fast roaming among FlexConnect and non-FlexConnect access points is not supported.

Note FlexConnect Groups is needed for CCKM to work. Flex group needs to be created for CCKM, 11r , and OKC , only then the caching can happen on an AP. The group name must be same between APS for a fast roaming to happen for 11r/CCKM. The group can be different for OKC as final check is done at Cisco WLC.

FlexConnect Groups and Opportunistic Key Caching

Starting with the Cisco Wireless LAN Controller Release 7.0.116.0, FlexConnect groups accelerate Opportunistic Key Caching (OKC) to enable fast roaming of clients. OKC facilitates fast roaming by using PMK caching in access points that are in the same FlexConnect group.

OKC prevents the need to perform a full authentication as the client roams from one access point to another. FlexConnect groups store the cached key on the APs of the same group, accelerating the process. However, they are not required, as OKC will still happen between access points belonging to different FlexConnect groups and will use the cached key present on the Cisco WLC, provided that Cisco WLC is reachable and APs are in connected mode.

To see the PMK cache entries at the FlexConnect access point, use the **show capwap reap pmk** command. This feature is supported on Cisco FlexConnect access points only. The PMK cache entries cannot be viewed on Non-FlexConnect access points.

Note The FlexConnect access point must be in connected mode when the PMK is derived during WPA2/802.1x authentication.

When using FlexConnect groups for OKC or CCKM, the PMK-cache is shared only across the access points that are part of the same FlexConnect group and are associated to the same controller. If the access points are in the same FlexConnect group but are associated to different controllers that are part of the same mobility group, the PMK cache is not updated and CCKM roaming will fail but OKC roaming will still work.

Note Fast roaming works only if the APs are in the same FlexConnect group for APs in FlexConnect mode, 802.11r .

FlexConnect Groups and Local Authentication

You can configure the controller to allow a FlexConnect access point in standalone mode to perform LEAP, EAP-FAST, PEAP, or EAP-TLS authentication for up to 100 statically configured users. The controller sends the static list of usernames and passwords to each FlexConnect access point when it joins the controller. Each access point in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous access point network to a lightweight FlexConnect access point network and are not interested in maintaining a large user database or adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.

Note

- You can configure LEAP, EAP-FAST, PEAP, or EAP-TLS authentication only if AP local authentication is enabled.

You have to provision a certificate to the AP because the AP has to send the certificate to the client. You must download the Vendor Device Certificate and the Vendor Certification Authority Certificate to the controller. The controller then pushes these certificates to the AP. If you do not configure a Vendor Device Certificate and the Vendor CA Certificate on the controller, the APs associating with the FlexConnect group download the self-signed certificate of the controller, which may not be recognized by many wireless clients.

With EAP-TLS, AP does not recognize and accept client certificate if the client root CA is different from the AP root CA. When you use Enterprise public key infrastructures (PKI), you must download a Vendor Device Certificate and Vendor CA Certificate to the controller so that the controller can push the certificates to the AP in the FlexConnect group. Without a common client and AP root CA, EAP-TLS fails on the local AP. The AP cannot check an external CA and relies on its own CA chain for client certificate validation.

The space on the AP for the local certificate and the CA certificate is around 7 Kb, which means that only short chains are adapted. Longer chains or multiple chains are not supported.

Note This feature can be used with the FlexConnect backup RADIUS server feature. If a FlexConnect is configured with both a backup RADIUS server and local authentication, the FlexConnect access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the FlexConnect access point itself (if the primary and secondary are not reachable).

For information about the number of FlexConnect groups and access point support for a Cisco WLC model, see the data sheet of the respective Cisco WLC model.

Configuring FlexConnect Groups

Configuring FlexConnect Groups (GUI)

Note If the same IPv4 ACLs is mapped to a FlexConnect group and to an AP, then the controller uses the Flex group ACL. However, if the controller is downgraded to an older version, the AP reboots to the older version and pushes the AP specific ACL. This time the controller uses the AP specific ACL ignoring the FlexConnect Group ACL.

Step 1 Choose **Wireless** > **FlexConnect Groups** to open the **FlexConnect Groups** page.

This page lists any FlexConnect groups that have already been created.

Note If you want to delete an existing group, hover your cursor over the blue drop-down arrow for that group and choose **Remove**.

Step 2 Click **New** to create a new FlexConnect Group.

Step 3 On the **FlexConnect Groups** > **New** page, enter the name of the new group in the **Group Name** text box. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**. The new group appears on the **FlexConnect Groups** page.

Step 5 To edit the properties of a group, click the name of the desired group. The **FlexConnect Groups** > **Edit** page appears.

Step 6 If you want to configure a primary RADIUS server for this group (for example, the access points are using 802.1X authentication), choose the desired server from the Primary RADIUS Server drop-down list. Otherwise, leave the text box set to the default value of None.

Note IPv6 RADIUS Server is not configurable. Only IPv4 configuration is supported.

Step 7 If you want to configure a secondary RADIUS server for this group, choose the server from the Secondary RADIUS Server drop-down list. Otherwise, leave the field set to the default value of None.

Step 8 Configure the RADIUS server for the FlexConnect group by doing the following:

a) Enter the RADIUS server IP address.
b) Choose the server type as either Primary or Secondary.
c) Enter a shared secret to log on to the RADIUS server and confirm it.

The maximum number of characters allowed for the shared secret is 63.

d) Enter the port number.
e) Click **Add**.

Step 9 To add an access point to the group, click **Add AP**. Additional fields appear on the page under **Add AP**.

Step 10 Perform one of the following tasks:

- To choose an access point that is connected to this controller, select the **Select APs from Current Controller** check box and choose the name of the access point from the AP Name drop-down list.

  Note If you choose an access point on this controller, the MAC address of the access point is automatically entered in the Ethernet MAC text box to prevent any mismatches from occurring.

- To choose an access point that is connected to a different controller, leave the **Select APs from Current Controller** check box unselected and enter its MAC address in the Ethernet MAC text box.

  Note If the FlexConnect access points within a group are connected to different controllers, all of the controllers must belong to the same mobility group.

Step 11 Click **Add** to add the access point to this FlexConnect group. The access point's MAC address, name, and status appear at the bottom of the page.

Note If you want to delete an access point, hover your cursor over the blue drop-down arrow for that access point and choose **Remove**.

Step 12 Click **Apply**.

Step 13 Enable local authentication for a FlexConnect Group as follows:

a) Ensure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None**.
b) Select the **Enable AP Local Authentication** check box to enable local authentication for this FlexConnect Group. The default value is unselected.
c) Click **Apply**.
d) Choose the **Local Authentication** tab to open the **FlexConnect** > **Edit (Local Authentication > Local Users)** page.
e) To add clients that you want to be able to authenticate using LEAP, EAP-FAST, PEAP, or EAP-TLS, perform one of the following:
f) Upload a comma-separated values (CSV) file by selecting the **Upload CSV File** check box, clicking the **Browse** button to browse to an CSV file that contains usernames and passwords (each line of the file needs to be in the following format: username, password), and clicking **Add** to upload the CSV file. The clients' names appear on the left side of the page under the "User Name" heading.
g) Add clients individually by entering the client's username in the User Name text box and a password for the client in the Password and Confirm Password text boxes, and clicking **Add** to add this client to the list of supported local users. The client name appears on the left side of the page under the "User Name" heading.

   Note You can add up to 100 clients.

h) Click **Apply**.
i) Choose the **Protocols** tab to open the **FlexConnect** > **Edit (Local Authentication > Protocols)** page.
j) To allow a FlexConnect access point to authenticate clients using LEAP, select the **Enable LEAP Authentication** check box.
k) To allow a FlexConnect access point to authenticate clients using EAP-FAST, select the **Enable EAP-FAST Authentication** check box. The default value is unselected.

l) To allow a FlexConnect access point to authenticate clients using PEAP Authentication, select the **Enable PEAP Authentication** check box.

You can configure PEAP authentication only when AP local authentication is configured.

m) To allow a FlexConnect access point to authenticate clients using EAP-TLS, select the **Enable EAP TLS Authentication** check box.

You can configure EAP-TLS authentication only when AP local authentication is configured.

Enabling the EAP-TLS authentication results in enabling the downloading of EAP root and device certificate to the access point. You can unselect the **EAP TLS Certificate download** check box if you do not want to download the certificate.

n) Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the server key used to encrypt and decrypt PACs in the Server Key and Confirm Server Key text boxes. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Enable Auto Key Generation** check box

o) In the Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
p) In the Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.
q) To specify a PAC timeout value, select the **PAC Timeout** check box and enter the number of seconds for the PAC to remain viable in the text box. The default value is unselected, and the valid range is 2 to 4095 seconds when enabled.
r) Click **Apply**.

Step 14 In the **WLAN-ACL Mapping** tab, you can do the following:

a) Under **Web Auth ACL Mapping**, enter the **WLAN ID**, choose the **WebAuth ACL**, and click **Add** to map the web authentication ACL and the WLAN.
b) Under **Local Split ACL Mapping**, enter the **WLAN ID**, and choose the **Local Split ACL**, and click **Add** to map the Local Split ACL to the WLAN.

Note You can configure up to 16 WLAN-ACL combinations for local split tunneling. Local split tunneling does not work for clients with static IP address.

Step 15 In the Central DHCP tab, you can do the following:

a) In the WLAN Id box, enter the WLAN ID with which you want to map Central DHCP.
b) Select or unselect the **Central DHCP** check box to enable or disable Central DHCP for the mapping.
c) Select or unselect the **Override DNS** check box to enable or disable overriding of DNS for the mapping.
d) Select or unselect the **NAT-PAT** check box to enable or disable network address translation and port address translation for the mapping.
e) Click **Add** to add the Central DHCP - WLAN mapping.

Note When the overridden interface is enabled for the FlexConnect Group DHCP, the DHCP broadcast to unicast is optional for locally switched clients.

Step 16 Click **Save Configuration**.

Step 17 Repeat this procedure if you want to add more FlexConnects.

Note To see if an individual access point belongs to a FlexConnect Group, you can choose **Wireless** > **Access Points** > **All APs >** the name of the desired access point in the FlexConnect tab. If the access point belongs to a FlexConnect, the name of the group appears in the FlexConnect Name text box.

Configuring FlexConnect Groups (CLI)

Note If the same IPv4 ACLs is mapped to a FlexConnect group and to an AP, then the controller uses the Flex group ACL. However, if the controller is downgraded to an older version, the AP reboots to the older version and pushes the AP specific ACL. This time the controller uses the AP specific ACL ignoring the FlexConnect Group ACL.

Step 1 Add add or delete a FlexConnect Group by entering this command:

config flexconnect group *group_name* {**add** | **delete**}

Step 2 Configure a primary or secondary RADIUS server for the FlexConnect group by entering this command:

config flexconect group *group-name* **radius server auth** {{**add** {**primary** | **secondary**} *ip-addr auth-port secret*} | {**delete** {**primary** | **secondary**}}}

The maximum number of characters allowed for the shared secret is 63.

Step 3 Add an access point to the FlexConnect Group by entering this command:

config flexconnect *group_name* **ap** {**add** | **delete**} *ap_mac*

Step 4 Configure local authentication for a FlexConnect as follows:

a) Make sure that a primary and secondary RADIUS server are not configured for the FlexConnect Group.

b) To enable or disable local authentication for this FlexConnect group, enter this command:

config flexconnect group *group_name* **radius ap** {**enable** | **disable**}

c) Enter the username and password of a client that you want to be able to authenticate using LEAP, EAP-FAST, PEAP, or EAP-TLS by entering this command:

config flexconnect group *group_name* **radius ap user add** *username* **password** *password*

Note You can add up to 100 clients.

d) Allow a FlexConnect access point group to authenticate clients using LEAP or to disable this behavior by entering this command:

config flexconnect group *group_name* **radius ap leap** {**enable** | **disable**}

e) Allow a FlexConnect access point group to authenticate clients using EAP-FAST or to disable this behavior by entering this command:

config flexconnect group *group_name* **radius ap eap-fast** {**enable** | **disable**}

f) To download EAP Root and Device certificate to AP, enter this command:

config flexconnect group *group_name* **radius ap eap-cert download**

g) Allow a FlexConnect access point group to authenticate clients using EAP-TLS or to disable this behavior by entering this command:

config flexconnect group *group_name* **radius ap eap-tls** {**enable** | **disable**}

h) Allow a FlexConnect access point group to authenticate clients using PEAP or to disable this behavior by entering this command:

config flexconnect group *group_name* **radius ap peap** {**enable** | **disable**}

i) Allow a FlexConnect access point group to authenticate clients using PEAP or to disable this behavior by entering this command:

config flexconnect group *group_name* **radius ap peap** {**enable** | **disable**}

j) Allow a FlexConnect access point group to authenticate clients using EAP-TLS or to disable this behavior by entering this command:

config flexconnect group *group_name* **radius ap eap-tls** {**enable** | **disable**}

k) Download the EAP root and device certificate by entering this command:

config flexconnect group *group_name* **radius ap eap-cert download**

l) Enter one of the following commands, depending on how you want PACs to be provisioned:

- **config flexconnect group** *group_name* **radius ap server-key** *key*—Specifies the server key used to encrypt and decrypt PACs. The key must be 32 hexadecimal characters.
- **config flexconnect group** *group_name* **radius ap server-key auto**—Allows PACs to be sent automatically to clients that do not have one during PAC provisioning.

m) To specify the authority identifier of the EAP-FAST server, enter this command:

config flexconnect group *group_name* **radius ap authority id** *id*

where *id* is 32 hexadecimal characters.

n) To specify the authority identifier of the EAP-FAST server in text format, enter this command:

config flexconnect group *group_name* **radius ap authority info** *info*

where *info* is up to 32 hexadecimal characters.

o) To specify the number of seconds for the PAC to remain viable, enter this command:

config flexconnect group *group_name* **radius ap pac-timeout** *timeout*

where *timeout is a value between 2 and* 4095 seconds (inclusive) or 0. A value of 0, which is the default value, disables the PAC timeout.

Step 5 Configure a Policy ACL on a FlexConnect group by entering this command:

config flexconnect group *group-name* **policy acl** {**add** | **delete**} *acl-name*

Step 6 Configure local split tunneling on a per-FlexConnect group basis by entering this command:

config flexconnect group *group_name* **local-split wlan** *wlan-id* **acl** *acl-name flexconnect-group-name* {**enable** | **disable**}

Step 7 To set multicast/broadcast across L2 broadcast domain on overridden interface for locally switched clients, enter this command:

config flexconnect group *group_name* **multicast overridden-interface** {**enable** | **disable**}

Step 8 Configure central DHCP per WLAN by entering this command:

config flexconnect group *group-name* **central-dhcp** *wlan-id* {**enable override dns** | **disable** | **delete**}

Step 9 Configure the DHCP overridden interface for FlexConnect group, use the **config flexconnect group flexgroup dhcp overridden-interface enable**command.

Step 10 Configure policy acl on FlexConnect group by entering this command:

config flexconnect group *group_name* **policy acl** {**add** | **delete**} *acl-name*

Step 11 Configure web-auth acl on flexconnect group by entering this command:

config flexconnect group *group_name* **web-auth wlan** *wlan-id* **acl** *acl-name* {**enable** | **disable**}

Step 12 Configure wlan-vlan mapping on flexconnect group by entering this command:

config flexconnect group *group_name* **wlan-vlan wlan** *wlan-id*{**add** | **delete**}**vlan** *vlan-id*

Step 13 To set efficient upgrade for group, enter this command:

config flexconnect group *group_name* **predownload** {**enable** | **disable** | **master** | **slave**} *ap-name* **retry-count** *maximum retry count* **ap-name** *ap-name*

Step 14 Save your changes by entering this command:

save config

Step 15 See the current list of flexconnect groups by entering this command:

show flexconnect group summary

Step 16 See the details for a specific FlexConnect Groups by entering this command:

show flexconnect group detail *group_name*

Configuring VLAN-ACL Mapping on FlexConnect Groups

Configuring VLAN-ACL Mapping on FlexConnect Groups (GUI)

Step 1 Choose **Wireless** > **FlexConnect Groups**.

The **FlexConnect Groups** page appears. This page lists the access points associated with the controller.

Step 2 Click the **Group Name** link of the FlexConnect Group for which you want to configure VLAN-ACL mapping.

Step 3 Click the **VLAN-ACL Mapping** tab.

The VLAN-ACL Mapping page for that FlexConnect group appears.

Step 4 Enter the **Native VLAN ID** in the **VLAN ID** text box.

Step 5 From the **Ingress ACL** drop-down list, choose the **Ingress ACL**.

Step 6 From the **Egress ACL** drop-down list, choose the **Egress ACL**.

Step 7 Click **Add** to add this mapping to the **FlexConnect Group**.

The **VLAN ID** is mapped with the required ACLs. To remove the mapping, hover your mouse over the blue drop-down arrow and choose **Remove**.

Note The Access Points inherit the VLAN-ACL mapping on the FlexConnect groups if the WLAN VLAN mapping is also configured on the groups.

Configuring VLAN-ACL Mapping on FlexConnect Groups (CLI)

Procedure

- **config flexconnect group** *group-name* **vlan add** *vlan-id* **acl** *ingress-acl egress acl*

  Add a VLAN to a FlexConnect group and map the ingress and egress ACLs by entering this command:

Viewing VLAN-ACL Mappings (CLI)

Procedure

- **show flexconnect group detail** *group-name*

  View FlexConnect group details.
- **show ap config general** *ap-name*

  View VLAN-ACL mappings on the AP.

Configuring WLAN-VLAN Mappings on FlexConnect Groups

Configuring WLAN-VLAN Mapping on FlexConnect Groups (GUI)

Following are a few guidelines:

- The individual AP settings have precedence over FlexConnect group and global WLAN settings. The FlexConnect group settings have precedence over global WLAN settings.
- The AP level configuration is stored in flash; WLAN and FlexConnect group configuration is stored in RAM.
- When an AP moves from one controller to another, the AP can keep its individual VLAN mappings. However, the FlexConnect group and global mappings will be from the new controller. If the WLAN SSID differs between the two controllers, then the WLAN-VLAN mapping is not applied.
- In a downstream traffic, VLAN ACL is applied first and then the client ACL is applied. In an upstream traffic, the client ACL is applied first and then the VLAN ACL is applied.

- The ACL must be present on the AP at the time of 802.1X authentication. If the ACL is not present on the AP, a client might be denied authentication by the AP even if the client successfully passes 802.1X authentication.

ACL Present on AP	ACL Name sent from AAA	Result of 802.1X Authentication
No	No	Authenticated, no ACL applied
No	Yes	Authentication Denied
Yes	No	Authenticated, no ACL applied
Yes	Yes	Authenticated, client ACL applied

- After client authentication, if the ACL name is changed in the RADIUS server, the client must go through a full authentication again to get the correct client ACL.
- The WLAN-VLAN mapping on FlexConnect groups is not supported on Cisco APs 1131 and 1242.

Before you begin

Ensure that the WLAN is locally switched. The configuration is applied to the AP only if the WLAN is broadcast on the AP.

Step 1 Choose **Wireless** > **FlexConnect Groups**.

Step 2 Click the group name.

The **FlexConnect Groups > Edit** page is displayed.

Step 3 Click the **WLAN VLAN Mapping** tab.

Step 4 Enter the WLAN ID and the VLAN ID and click **Add**.

The mapping is displayed in the same tab.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring WLAN-VLAN Mapping on FlexConnect Groups (CLI)

Before you begin

Ensure that the WLAN is locally switched. The configuration is applied to the AP only if the WLAN is broadcast on the AP.

Procedure

- **config flexconnect group** *group-name* **wlan-vlan wlan** *wlan-id* {**add** | **delete**} **vlan** *vlan-id*

  Configure WLAN-VLAN mapping on a FlexConnect group by entering this command.

CHAPTER 138

Configuring AAA Overrides for FlexConnect

- Authentication, Authorization, Accounting Overrides, on page 975
- Restrictions on AAA Overrides for FlexConnect, on page 977
- Configuring AAA Overrides for FlexConnect on an Access Point (GUI), on page 979
- Configuring VLAN Overrides for FlexConnect on an Access Point (CLI), on page 979

Authentication, Authorization, Accounting Overrides

The Allow Authentication, Authorization, Accouting (AAA) Override option of a WLAN enables you to configure the WLAN for authentication. It enables you to apply VLAN tagging, QoS, and ACLs to individual clients based on the returned RADIUS attributes from the AAA server.

AAA overrides for FlexConnect access points introduce a dynamic VLAN assignment for locally switched clients. AAA overrides for FlexConnect also support fast roaming (Opportunistic Key Caching [OKC]/ Cisco Centralized Key management [CCKM]) of overridden clients.

VLAN overrides for FlexConnect are applicable for both centrally and locally authenticated clients. VLANs can be configured on FlexConnect groups.

If a VLAN on the AP is configured using the WLAN-VLAN, the AP configuration of the corresponding ACL is applied. If the VLAN is configured using the FlexConnect group, the corresponding ACL configured on the FlexConnect group is applied. If the same VLAN is configured on the FlexConnect group and also on the AP, the AP configuration, with its ACL takes precedence. If there is no slot for a new VLAN from the WLAN-VLAN mapping, the latest configured FlexConnect group VLAN is replaced.

If the VLAN that was returned from the AAA is not present on the AP, the client falls back to the default VLAN configured for the WLAN.

Before configuring a AAA override, the VLAN must be created on the access points. These VLANs can be created by using the existing WLAN-VLAN mappings on the access points, or by using the FlexConnect group VLAN-ACL mappings.

AAA Override for IPv6 ACLs

In order to support centralized access control through a centralized AAA server such as the Cisco Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis using AAA Override attributes. In order to use this feature, the IPv6 ACL must be configured on the controller and the WLAN must be configured with the AAA Override feature enabled. The AAA attribute for an IPv6 ACL is *Airespace-IPv6-ACL-Name* similar to the *Airespace-ACL-Name* attribute used for provisioning an IPv4-based

ACL. The AAA attribute-returned contents should be a string that is equal to the name of the IPv6 ACL as configured on the controller.

AAA Overrides of Bidirectional Rate Limiting on an AP and Controller

You can have AAA overrides for FlexConnect APs to dynamically assign QoS levels and/or bandwidth contracts for both locally switched traffic on web-authenticated WLANs and 802.1X-authenticated WLANs. Both upstream and downstream parameters are sent to the corresponding AP.

Table 32: Bidirectional Rate-Limiting Implementation

Upstream/Downstream	Local Mode	FlexConnect Central Switching	FlexConnect Local Switching	FlexConnect Standalone
Per-Client Downstream	AP	AP	AP	AP
Per-Client Upstream	AP	AP	AP	AP
Per-SSID Downstream	AP	AP	AP	AP
Per-SSID Upstream	AP	AP	AP	AP

There is an option to select the downstream rate limit through the QoS profile page. Users that already make use of QoS profiles functionality have additional granularity and capabilities.

The trade-off with configuring the rate limits under the QoS profile is that there are only four QoS profiles available. Thus, there are only four sets of configuration options to use.

Also, because the QoS profile is applied to all clients on the associated SSID, all clients connected to the same SSID will have the same rate limited parameters.

Table 33: Rate-Limiting Parameters

AAA	QoS Profile of AAA	WLAN	QoS Profile of WLAN	Applied to Client
100 Kbps	200 Kbps	300 Kbps	400 Kbps	100 Kbps
X	—	—	—	200 Kbps
X	X	—	—	300 Kbps
X	X	X	—	400 Kbps
X	X	X	X	Unlimited

Important Guidelines

- Rate limiting is supported for APs in Local and FlexConnect mode (both Central and Local switching).
- When the controller is connected and central switching is used, the controller handles the downstream enforcement of per-client rate limit only.
- APs handle the enforcement of the upstream traffic and per-SSID rate limit for downstream traffic.

- For the locally switched environment, both upstream and downstream rate limits will be enforced on the AP. The enforcement on the AP will take place in the dot11 driver. This is where the current classification exists.
- In both directions, per-client rate limit is applied/checked first and per-SSID rate limit is applied/checked second.
- The WLAN rate limiting will always supercede the global QoS setting for WLAN and user.
- Rate limiting works only for TCP and UDP traffic. Other types of traffic (IPSec, GRE, ICMP, CAPWAP, etc) cannot be limited.
- Using AVC rule, you can limit the bandwidth of a particular application for all the clients joined on the WLAN. These bandwidth contracts coexist with per-client downstream rate limiting. The per-client downstream rate limits takes precedence over the per-application rate limits.
- Bidirectional rate limiting (BDRL) configuration in a mobility Anchor-Foreign setup needs to be done both on Anchor and Foreign controller. As a best practice, we recommend that you do identical configuration on both the controllers to avoid breakage of any feature.
- Per WLAN BDRL is supported on these currently supported Cisco Wave1 APs: 1600, 2600, 3600, 1700, 2700, 3700, and 3500.
- For information about BDRL support on Cisco Wave 2 APs, see the *FlexConnect Feature Matrix* section in the Feature Matrix for Cisco Wave 2 Access Points and Wi-Fi 6 (802.11ax) Access Points.
- BDRL is not supported in mesh platforms. On Cisco Virtual Wireless Controller (vWLC), per-client downstream rate limiting is not supported in FlexConnect central switching.
- In Release 8.5, in anchor-foreign scenario with Cisco Wave 2 APs, only per-client downstream works. The per-client upstream, per-SSID downstream, and per-SSID upstream are not supported. However, all of these are supported in Cisco Wave 1 APs.

  In Release 8.8, in anchor-foreign scenario with Cisco Wave 2 APs, all both per-client upstream and downstream and per-SSID upstream and downstream are supported, provided that the configuration is the same in both and anchor and foreign controllers.

Related Documentation: Wireless Bi-Directional Rate Limiting Deployment Guide

This section contains the following subsections:

Restrictions on AAA Overrides for FlexConnect

- Before configuring a AAA override, VLANs must be created on the access points. These VLANs can be created by using the existing WLAN-VLAN mappings on the access points, or by using the FlexConnect group VLAN-ACL mappings.
- At any given point, an AP has a maximum of 16 VLANs. First, the VLANs are selected as per the AP configuration (WLAN-VLAN), and then the remaining VLANs are pushed from the FlexConnect group in the order that they are configured or displayed in the FlexConnect group. If the VLAN slots are full, an error message is displayed.
- VLAN, ACL, QoS, Rate limiting are supported with local and central switching WLAN.

- Dynamic VLAN assignment is not supported for web authentication from a controller with Access Control Server (ACS).
- AAA override of bidirectional rate limiting on an AP and the controller is supported on all the following 802.11n nonmesh access points:
  - 1040
  - 1140
  - 1250
  - 1260
  - 1600
  - 1700
  - 2600
  - 2700
  - 3500
  - 3600
  - 3700

  This feature is not supported on the mesh and legacy AP platforms:
  - 1130
  - 1240
  - 1520
  - 1550
- For bidirectional rate limiting:
  - If bidirectional rate limiting is not present, AAA override cannot occur.
  - The QoS profile of a client can be Platinum even if the QoS profile of the corresponding WLAN is Silver. The AP allows the client to send packets in a voice queue. However, Session Initiation Protocol (SIP) snooping is disabled on the WLAN to ensure that the traffic for a SIP client does not go to the voice queue.
  - The ISE server is supported.
  - The upstream rate limit parameter is equal to the downstream parameter, from AAA override.
  - Local authentication is not supported.
- If you assign multiple VLAN names to a VLAN ID, the client display represents the first matching VLAN name that is assigned to the VLAN ID.

Configuring AAA Overrides for FlexConnect on an Access Point (GUI)

Step 1 Choose **Wireless** > **All** > **APs**.

The **All APs** page is displayed. This page lists the access points associated with the controller.

Step 2 Click the corresponding AP name.

Step 3 Click the **FlexConnect** tab.

Step 4 Enter a value for **Native VLAN ID**.

Step 5 Click the **VLAN Mappings** button to configure the AP VLANs mappings.

The following parameters are displayed:

- **AP Name**—The access point name.
- **Base Radio MAC**—The base radio of the AP.
- **WLAN-SSID-VLAN ID Mapping**—For each WLAN configured on the controller, the corresponding SSID and VLAN IDs are listed. Change a WLAN-VLAN ID mapping by editing the VLAN ID column for a WLAN.
- **Centrally Switched WLANs**—If centrally switched WLANs are configured, WLAN–VLAN mapping is listed.
- **AP Level VLAN ACL Mapping**—The following parameters are available:
  - VLAN ID—The VLAN ID.
  - Ingress ACL—The Ingress ACL corresponding to the VLAN.
  - Egress ACL—The Egress ACL corresponding to the VLAN.

  Change the ingress ACL and egress ACL mappings by selecting the mappings from the drop-down list for each ACL type.
- **Group Level VLAN ACL Mapping**—The following group level VLAN ACL mapping parameters are available:
  - VLAN ID—The VLAN ID.
  - Ingress ACL—The ingress ACL for this VLAN.
  - Egress ACL—The egress ACL for this VLAN.

Step 6 Click **Apply**.

Configuring VLAN Overrides for FlexConnect on an Access Point (CLI)

To configure VLAN overrides on a FlexConnect access point, use the following command:

config ap flexconnect vlan add *vlan-id* **acl** *ingress-acl egress-acl ap_name*

CHAPTER 139

FlexConnect AP Image Upgrades

- Information About FlexConnect AP Image Upgrades, on page 981
- Restrictions on FlexConnect AP Image Upgrades, on page 981
- Configuring FlexConnect AP Upgrades (GUI), on page 982
- Configuring FlexConnect AP Upgrades (CLI), on page 983

Information About FlexConnect AP Image Upgrades

Normally, when upgrading the image of an AP, you can use the preimage download feature to reduce the amount of time the AP is unavailable to serve clients. However, it also increases the downtime because the AP cannot serve clients during an upgrade. The preimage download feature can be used to reduce this downtime. However, in the case of a branch office set up, the upgrade images are still downloaded to each AP over the WAN link, which has a higher latency.

A more efficient way is to use the FlexConnect AP Image Upgrade feature. When this feature is enabled, one access point of each model in the local network first downloads the upgrade image over the WAN link. It works similarly to the primary-subordinate or client-server model. This access point then becomes the primary for the remaining access point of the similar model. The remaining access points then download the upgrade image from the primary access point using the pre-image download feature over the local network, which reduces the WAN latency.

Restrictions on FlexConnect AP Image Upgrades

- The primary and secondary controllers in the network must have the same set of primary and backup images.
- If you configured a FlexConnect group, all access points in that group must be within the same subnet or must be accessible through NAT.
- A FlexConnect group can have a maximum of 100 APs on Cisco 7510 Controller, and 25 APs on Cisco 5508 Controller.
- A FlexConnect group can have one primary AP per AP model. If a primary AP is not selected manually, the AP that has the least MAC address value is automatically chosen as the primary AP for that model.
- A maximum of 3 subordinate APs of the same model can download the image from their primary AP (a maximum of 3 TFTP connections can serve at a time). The rest of the subordinate APs use the random

back-off timer to retry for the primary AP to download the image. The random back-off value is more than 100 seconds. After a subordinate AP downloads the image, the AP informs the controller about the completion of the download. After random back-off, the waiting subordinate AP can occupy the empty TFTP slot at the primary AP.

If a subordinate AP fails to download the image from its primary AP even after the subordinate retry count that you have configured is exhausted, the subordinate AP reaches out to the controller to fetch the new image.

- This feature works only with CAPWAP APs.
- This feature does not work if a primary AP is connected over CAPWAP6.
- If you upgrade from a release that is prior to Release 7.5 directly to Release 7.6.X or a later release, the predownload process on Cisco AP2600 and AP3600 fails. After the controller is upgraded to Release 7.6.X or a later release, the new image is loaded on Cisco AP2600 and AP3600. After the upgrade to a Release 7.6.X image, the predownload functionality works as expected. The predownload failure is only a one-time failure.
- A Cisco Wave 2 AP working as the primary AP downloads the software image from the controller, even if the software image version is the same.

Configuring FlexConnect AP Upgrades (GUI)

Step 1 Choose **Wireless** > **FlexConnect Groups**.

The FlexConnect Groups page appears. This page lists the FlexConnect Groups configured on the controller.

Step 2 Click the **Group Name** link on which you want to configure the image upgrade.

Step 3 Click the **Image Upgrade** tab.

Step 4 Check the **FlexConnect AP Upgrade** check box to enable a FlexConnect AP Upgrade.

Step 5 If you enabled the FlexConnect AP upgrade in the previous step, you must enable the following parameters:

- **Slave Maximum Retry Count**—The number of attempts the subordinate access point must try to connect to the primary access point for downloading the upgrade image. If the image download does not occur for the configured retry attempts, the image is upgraded over the WAN. The default value is 44; the valid range is between 1 and 63.
- **Upgrade Image**—Select the upgrade image. The options are **Primary**, **Backup**, and **Abort**.

Step 6 From the **AP Name** drop-down list, click **Add Master** to add the primary access point.

You can manually assign primary access points in the FlexConnect group by selecting the access points.

Step 7 Click **Apply**.

Step 8 Click **FlexConnect Upgrade** to upgrade.

Configuring FlexConnect AP Upgrades (CLI)

- **config flexconnect group** *group-name* **predownload {enable | disable}**—Enables or disables the FlexConnect AP upgrade.
- **config flexconnect group** *group-name* **predownload master** *ap-name*—Sets the AP as the primary AP for the model.
- **config flexconnect group** *group-name* **predownload slave ap-name** *ap-name*—Sets the AP as a subordinate AP.
- **config flexconnect group** *group-name* **predownload slave retry-count** *max-retry-count* —Sets the retry count for subordinate APs.
- **config flexconnect group** *group-name* **predownload start** {**abort** | **primary** | **backup**}—Initiates the image (primary or backup) download on the access points in the FlexConnect group, or terminates an image download process.
- **show flexconnect group** *group-name*—Displays the summary of the FlexConnect group configuration.
- **show ap image all**—Displays the details of the images on the access point.

PART X

Mobility Groups

- Mobility Groups, on page 987
- Viewing Mobility Group Statistics, on page 999
- Auto-Anchor Mobility, on page 1003
- Validating WLAN Mobility Security Values, on page 1009
- Using Symmetric Mobility Tunneling, on page 1011
- Running Mobility Ping Tests, on page 1013
- Configuring Dynamic Anchoring for Clients with Static IP Addresses, on page 1015
- Configuring Foreign Mappings, on page 1019
- Configuring Proxy Mobile IPv6, on page 1021
- Configuring New Mobility, on page 1029

CHAPTER 140

Mobility Groups

- Information About Mobility Groups, on page 987
- Prerequisites for Configuring Mobility Groups, on page 990
- Configuring Mobility Groups (GUI), on page 992
- Configuring Mobility Groups (CLI), on page 994
- Viewing Mobility Group Statistics (GUI), on page 995
- Viewing Mobility Group Statistics (CLI), on page 997

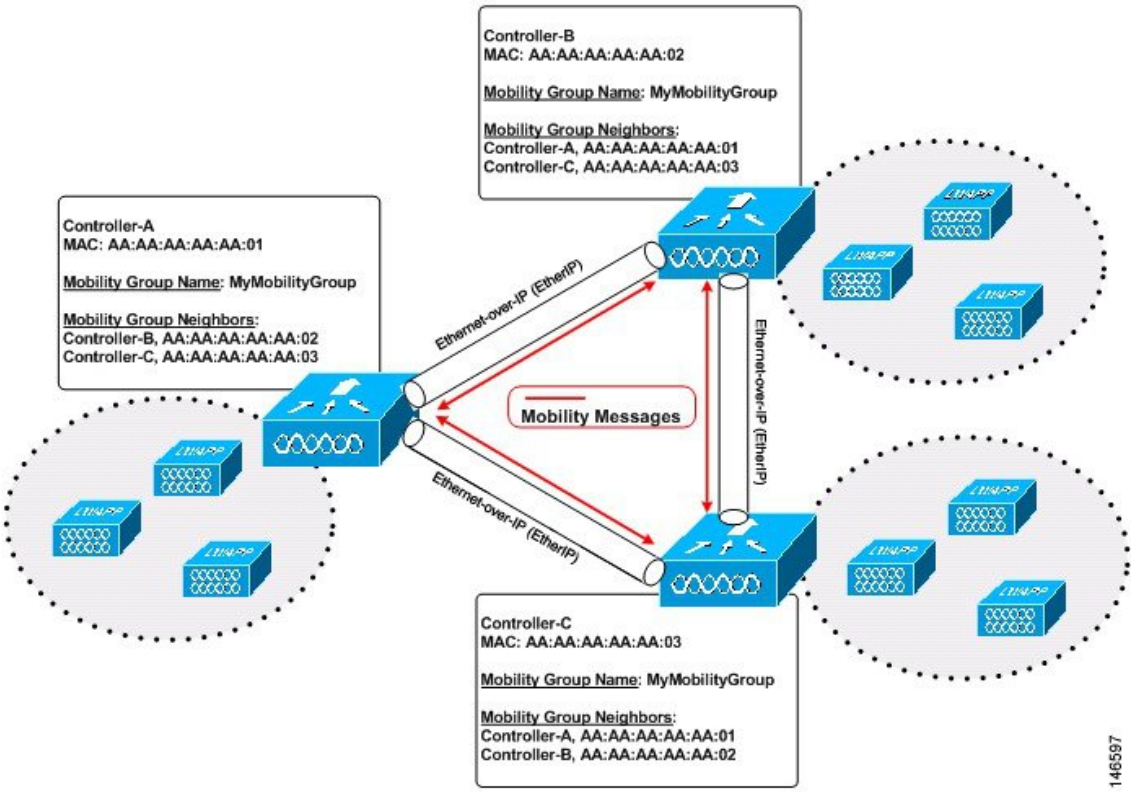
Information About Mobility Groups

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

Note When an AP moves from one controller to another controller (when both controllers are mobility peers), a client associated to the first controller before the move may be anchored to it even after the move. To prevent such a scenario, you should remove the mobility peer configuration of the controller.

Note Controllers do not have to be of the same model to be a member of a mobility group. Mobility groups can be comprised of any combination of controller platforms.

Figure 63: Example of a Single Mobility Group



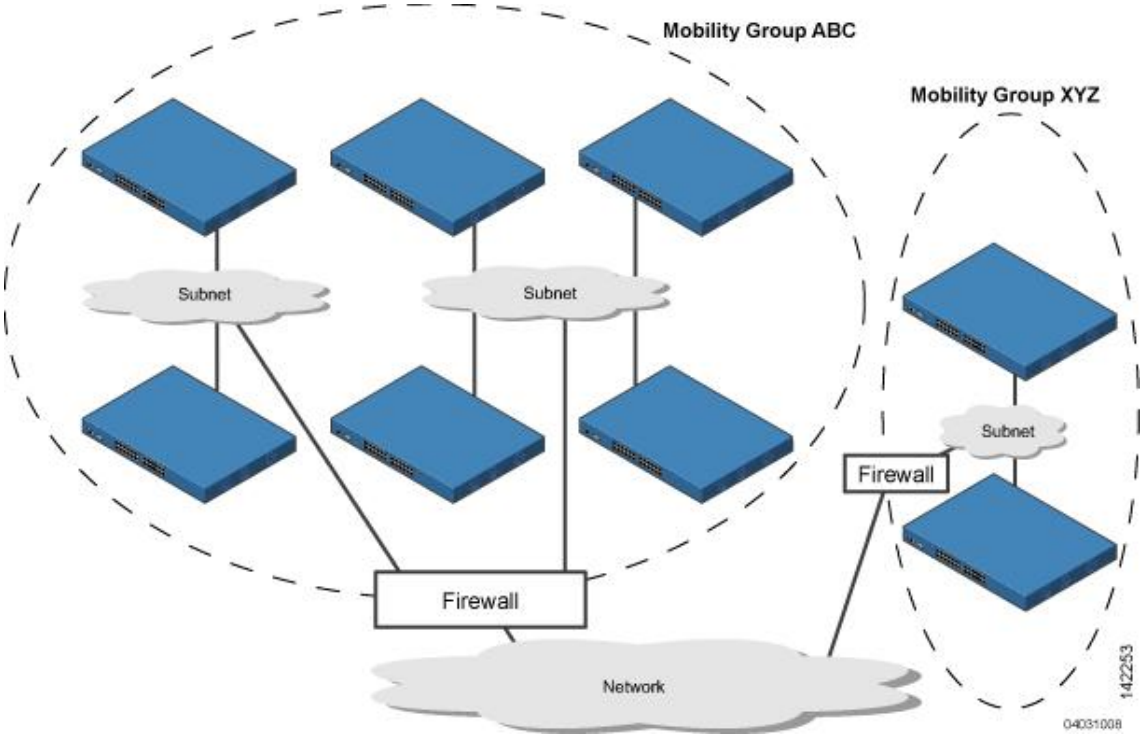
As shown above, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message (or multicast message if mobility multicast is configured) to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client.

For example, if a controller supports 6000 access points, a mobility group that consists of 24 such controllers supports up to 144,000 access points (24 * 6000 = 144,000 access points).

Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless network.

Figure 64: Two Mobility Groups

This figure shows the results of creating distinct mobility group names for two groups of controllers.



The controllers in the ABC mobility group share access point and client information with each other. The controllers in the ABC mobility group do not share the access point or client information with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not share access point or client information with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network.

Every controller maintains information about its peer controllers in a mobility list. Controllers can communicate across mobility groups and clients may roam between access points in different mobility groups if the controllers are included in each other's mobility lists. In the following example, controller 1 can communicate with either controller 2 or 3, but controller 2 and controller 3 can communicate only with controller 1 and not with each other. Similarly, clients can roam between controller 1 and controller 2 or between controller 1 and controller 3 but not between controller 2 and controller 3.

Table 34: Example

Controller 1	Controller 2	Controller 3
Mobility group: A	Mobility group: A	Mobility group: C
Mobility list:	Mobility list:	Mobility list:
Controller 1 (group A)	Controller 1 (group A)	Controller 1 (group A)
Controller 2 (group A)	Controller 2 (group A)	Controller 3 (group C)
Controller 3 (group C) ?		

In a mobility list, the following combinations of mobility groups and members are allowed:

- 3 mobility groups with 24 members in each group
- 12 mobility groups with 6 members in each group
- 24 mobility groups with 3 members in each group
- 72 mobility groups with 1 member in each group

The controller supports seamless roaming across multiple mobility groups. During seamless roaming, the client maintains its IP address across all mobility groups; however, Cisco Centralized Key Management (CCKM) and proactive key caching (PKC) are supported only for inter-mobility-group roaming. When a client crosses a mobility group boundary during a roam, the client is fully authenticated, but the IP address is maintained, and mobility tunneling is initiated for Layer 3 roaming.

Note When a controller is added to a mobility group, some of the APs (which are running in local mode) do not get the complete controllers list updated, those APs are connected to controllers that are in the same mobility group. You can view the controller list in the APs using the command "show capwap client config" AP-NAME command. For example, if the mobility group is for 19 controllers and then you add two more controllers to the mobility group, the AP shows 19 controllers instead of 21 in its list. To address this issue, you can reboot the AP or move it to another controller that is part of the same mobility group to get the controller list updated. This issue is observed in AP1242 connected to different Cisco 5508 WLCs running code 7.6.120.0.

Note When client moves to a non anchored SSID from an anchored sSSID on foreign, there is a stale entry on foreign .This happens when multicast mobile announce does not reach from foreign to guest anchor due to whatsoever reason, due to this the service is not impacted and configuration goes unnoticed but silently leaks MSCB on GA .There is no debug or error message shown nor does the GA runs a timer per client to cleanup. A HandoffEnd needs to be sent from foreign to Anchor since there is no timer.

Prerequisites for Configuring Mobility Groups

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- IP connectivity must exist between the management interfaces of all controllers.

Note You can verify IP connectivity by pinging the controllers.

Note Mobility control packets can use any interface address as the source, based on routing table. It is recommended that all controllers in the mobility group should have the management interface in the same subnet. A topology where one controller's management interface and other controller's dynamic interface are on same subnet not recommended for seamless mobility.

- When controllers in the mobility list use different software versions, Layer 2 or Layer 3 clients have limited roaming support. Layer 2 or Layer 3 client roaming is supported only between controllers that use the same version or with controllers that run versions 7.X.X.

Note If you inadvertently configure a controller with a failover controller that runs a different software release, the access point might take a long time to join the failover controller because the access point starts the discovery process in CAPWAP and then changes to LWAPP discovery.

- All controllers must be configured with the same virtual interface IP address.

Note If necessary, you can change the virtual interface IP address by editing the virtual interface name on the Controller > Interfaces page.

Note If all the controllers within a mobility group are not using the same virtual interface, inter-controller roaming may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time.

- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.

Note You can find the MAC and IP addresses of the other controllers to be included in the mobility group on the Controller > Mobility Groups page of each controller's GUI.

- When you configure mobility groups using a third-party firewall, for example, Cisco PIX, or Cisco ASA, you must open port 16666, and IP protocol 97.
- For intercontroller CAPWAP data and control traffic, you must open the ports 5247 and 5246.

This table lists the protocols and port numbers that must be used for management and operational purposes:

Table 35: Protocol/Service and Port Number

Protocol/Service	Port Number
SSH/Telnet	TCP Port 22 or 29
TFTP	UDP Port 69
NTP/SNTP	UDP Port 123

Protocol/Service	Port Number
SNMP	UDP Port 161 for gets and sets and UDP port 162 for traps.
HTTPS/HTTP	TCP port 443 for HTTPS and port 80 for HTTP
Syslog	TCP port 514
Radius Auth/Account	UDP port 1812 and 1813

Note To view information on mobility support across controllers with different software versions, see the http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html. .

Note You cannot perform port address translation (PAT) on the firewall. You must configure one-to-one network address translation (NAT).

Configuring Mobility Groups (GUI)

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Groups** to open the Static Mobility Group Members page.

This page shows the mobility group name in the Default Mobility Group text box and lists the MAC address and IPv4/IPv6 address of each controller that is currently a member of the mobility group. The first entry is the local controller, which cannot be deleted.

Note If you want to delete any of the remote controllers from the mobility group, hover your cursor over the blue drop-down arrow for the desired controller and choose **Remove**.

Step 2 Perform one of the following to add controllers to a mobility group:

- If you are adding only one controller or want to individually add multiple controllers, click **New**.

  OR

- If you are adding multiple controllers and want to add them in bulk, click **EditAll**.

Note The EditAll option enables you to enter the MAC and IPv4/IPv6 addresses of all the current mobility group members and then copy and paste all the entries from one controller to the other controllers in the mobility group.

Step 3 Click **New** to open the **Mobility Group Member** > **New** page.

Step 4 Add a controller to the mobility group as follows:

a. In the Member IP Address text box, enter the management interface IPv4/IPv6 address of the controller to be added.

Note If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IPv4/IPv6 address that is sent to the controller from the NAT device rather than the controller's management interface IPv4/IPv6 address. Otherwise, mobility will fail among controllers in the mobility group.

b. In the **Member MAC Address** text box, enter the MAC address of the controller to be added.

c. In the **Group Name** text box, enter the name of the mobility group.

Note The mobility group name is case sensitive.

d. In the **Hash** text box, enter the hash key of the peer mobility controller, which should be a virtual controller in the same domain.

You must configure the hash only if the peer mobility controller is a virtual controller in the same domain.

Note Hash is not supported for IPv6 members.

e. Click **Apply** to commit your changes. The new controller is added to the list of mobility group members on the **Static Mobility Group Members** page.

f. Click **Save Configuration**.

g. Repeat Step a through Step e to add all of the controllers in the mobility group.

h. Repeat this procedure on every controller to be included in the mobility group. All controllers in the mobility group must be configured with the MAC address and IPv4/IPv6 address of all other mobility group members.

The **Mobility Group Members** > **EditAll** page lists the MAC address, IPv4/IPv6 address, and mobility group name (optional) of all the controllers currently in the mobility group. The controllers are listed one per line with the local controller at the top of the list.

Note If desired, you can edit or delete any of the controllers in the list.

Step 5 Add more controllers to the mobility group as follows:

a. Click inside the edit box to start a new line.

b. Enter the MAC address, the management interface IPv4/IPv6 address, and the name of the mobility group for the controller to be added.

Note You should enter these values on one line and separate each value with one or two spaces.

Note The mobility group name is case sensitive.

c. Repeat Step a and Step b for each additional controller that you want to add to the mobility group.

d. Highlight and copy the complete list of entries in the edit box.

e. Click **Apply** to commit your changes. The new controllers are added to the list of mobility group members on the **Static Mobility Group Members** page.

f. Click **Save Configuration**to save your changes.

g. Paste the list into the text box on the Mobility Group Members > Edit All page of all the other controllers in the mobility group and click **Apply** and **Save Configuration**.

Step 6 Choose **Mobility Management** > **Multicast Messaging** to open the **Mobility Multicast Messaging** page.

The names of all the currently configured mobility groups appear in the middle of the page.

Step 7 On the **Mobility Multicast Messaging** page, check the **Enable Multicast Messaging** check box to enable the controller to use multicast mode to send Mobile Announce messages to the mobility members. If you leave it unselected, the controller uses unicast mode to send the Mobile Announce messages. The default value is unselected.

Step 8 If you enabled multicast messaging in the previous step, enter the multicast group IPv4 address for the local mobility group in the **Local Group Multicast IPv4 Address** text box. This address is used for multicast mobility messaging.

Note In order to use multicast messaging, you must configure the IPv4 address for the local mobility group.

Note In release 8.0, IPv6 is not supported for mobility multicast.

Step 9 Click **Apply** to commit your changes.

Step 10 If desired, you can also configure the multicast group IPv4 address for non-local groups within the mobility list. To do so, click the name of a non-local mobility group to open the Mobility Multicast Messaging > Edit page, and enter the multicast group IPv4 address for the non-local mobility group in the Multicast IP Address text box.

Note If you do not configure the multicast IPv4 address for non-local groups, the controller uses unicast mode to send mobility messages to those members.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring Mobility Groups (CLI)

Step 1 Check the current mobility settings by entering this command:

show mobility summary

Step 2 Create a mobility group by entering this command:

config mobility group domain *domain_name*

Note Enter up to 31 case-sensitive ASCII characters for the group name. Spaces are not allowed in mobility group names.

Step 3 Add a group member by entering this command:

config mobility group member add *mac_address ip_address*

Note If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address that is sent to the controller from the NAT device rather than the controller's management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

Note Enter the **config mobility group member delete** *mac_address* command if you want to delete a group member.

Step 4 To configure the hash key of a peer mobility controller, which is a virtual controller in the same domain, enter this command:

config mobility group member hash *peer-ip-address key*

Step 5 Enable or disable multicast mobility mode by entering this command:

config mobility multicast-mode {**enable** | **disable**} *local_group_multicast_address*

where *local_group_multicast_address* is the multicast group IPv4 address for the local mobility group. This address is used for multicast mobility messaging.

Note In order to use multicast messaging, you must configure the IPv4 address for the local mobility group.

Note In release 8.0, IPv6 is not supported for mobility multicast.

If you enable multicast mobility mode, the controller uses multicast mode to send Mobile Announce messages to the local group. If you disable multicast mobility mode, the controller uses unicast mode to send the Mobile Announce messages to the local group. The default value is disabled.

Step 6 (Optional) You can also configure the multicast group IPv4 address for non-local groups within the mobility list. To do so, enter this command:

config mobility group multicast-address *group_name IP_address*

If you do not configure the multicast IPv4 address for non-local groups, the controller uses unicast mode to send mobility messages to those members.

Step 7 Verify the mobility configuration by entering this command:

show mobility summary

Step 8 To see the hash key of mobility group members in the same domain, enter this command:

show mobility group member hash

Step 9 Save your changes by entering this command:

save config

Step 10 Repeat this procedure on every controller to be included in the mobility group. All controllers in the mobility group must be configured with the MAC address and IP address of all other mobility group members.

Step 11 Enable or disable debugging of multicast usage for mobility messages by entering this command:

debug mobility multicast {**enable** | **disable**}

Viewing Mobility Group Statistics (GUI)

Step 1 Choose **Monitor > Statistics > Mobility Statistics** to open the Mobility Statistics page.

This page contains the following fields

- Global Mobility Statistics
  - Rx Errors—Generic protocol packet receive errors, such as packet too short or format incorrect.
  - Tx Errors—Generic protocol packet transmit errors, such as packet transmission fail.
  - Responses Retransmitted—Mobility protocol that uses UDP and resends requests several times if it does not receive a response. Because of network or processing delays, the responder may receive one or more retry requests after it initially responds to a request. This text box shows a count of the response resends.

- Handoff Requests Received—Total number of handoff requests received, ignored, or responded to.
- Handoff End Requests Received—Total number of handoff end requests received. These requests are sent by the anchor or foreign controller to notify the other about the close of a client session.
- State Transitions Disallowed—Policy enforcement module (PEM) that has denied a client state transition, usually resulting in the handoff being terminated.
- Resource Unavailable—Necessary resource, such as a buffer, was unavailable, resulting in the handoff being terminated.

- Mobility Initiator Statistics
  - Handoff Requests Sent—Number of clients that have associated to the controller and have been announced to the mobility group.
  - Handoff Replies Received—Number of handoff replies that have been received in response to the requests sent.
  - Handoff as Local Received—Number of handoffs in which the entire client session has been transferred.
  - Handoff as Foreign Received—Number of handoffs in which the client session was anchored elsewhere.
  - Handoff Denys Received—Number of handoffs that were denied.
  - Anchor Request Sent—Number of anchor requests that were sent for a three-party (foreign-to-foreign) handoff. The handoff was received from another foreign controller, and the new controller is requesting the anchor to move the client.
  - Anchor Deny Received—Number of anchor requests that were denied by the current anchor.
  - Anchor Grant Received—Number of anchor requests that were approved by the current anchor.
  - Anchor Transfer Received—Number of anchor requests that closed the session on the current anchor and transferred the anchor back to the requestor.

- Mobility Responder Statistics
  - Handoff Requests Ignored—Number of handoff requests or client announcements that were ignored because the controller had no knowledge of that client.
  - Ping Pong Handoff Requests Dropped—Number of handoff requests that were denied because the handoff period was too short (3 seconds).
  - Handoff Requests Dropped—Number of handoff requests that were dropped due to either an incomplete knowledge of the client or a problem with the packet.
  - Handoff Requests Denied—Number of handoff requests that were denied.
  - Client Handoff as Local—Number of handoff responses sent while the client is in the local role.
  - Client Handoff as Foreign—Number of handoff responses sent while the client is in the foreign role.
  - Anchor Requests Received—Number of anchor requests received.
  - Anchor Requests Denied—Number of anchor requests denied.
  - Anchor Requests Granted—Number of anchor requests granted.

- Anchor Transferred—Number of anchors transferred because the client has moved from a foreign controller to a controller on the same subnet as the current anchor.

Step 2 If you want to clear the current mobility statistics, click **Clear Stats**.

Viewing Mobility Group Statistics (CLI)

Step 1 See mobility group statistics by entering this command:

show mobility statistics

Step 2 Clear the current mobility statistics by entering this command:

clear stats mobility

CHAPTER 141

Viewing Mobility Group Statistics

- Viewing Mobility Group Statistics (GUI), on page 999
- Viewing Mobility Group Statistics (CLI), on page 1000

Viewing Mobility Group Statistics (GUI)

Step 1 Choose **Monitor > Statistics > Mobility Statistics** to open the Mobility Statistics page.

This page contains the following fields

- Global Mobility Statistics
  - Rx Errors—Generic protocol packet receive errors, such as packet too short or format incorrect.
  - Tx Errors—Generic protocol packet transmit errors, such as packet transmission fail.
  - Responses Retransmitted—Mobility protocol that uses UDP and resends requests several times if it does not receive a response. Because of network or processing delays, the responder may receive one or more retry requests after it initially responds to a request. This text box shows a count of the response resends.
  - Handoff Requests Received—Total number of handoff requests received, ignored, or responded to.
  - Handoff End Requests Received—Total number of handoff end requests received. These requests are sent by the anchor or foreign controller to notify the other about the close of a client session.
  - State Transitions Disallowed—Policy enforcement module (PEM) that has denied a client state transition, usually resulting in the handoff being terminated.
  - Resource Unavailable—Necessary resource, such as a buffer, was unavailable, resulting in the handoff being terminated.
- Mobility Initiator Statistics
  - Handoff Requests Sent—Number of clients that have associated to the controller and have been announced to the mobility group.
  - Handoff Replies Received—Number of handoff replies that have been received in response to the requests sent.
  - Handoff as Local Received—Number of handoffs in which the entire client session has been transferred.

- Handoff as Foreign Received—Number of handoffs in which the client session was anchored elsewhere.
- Handoff Denys Received—Number of handoffs that were denied.
- Anchor Request Sent—Number of anchor requests that were sent for a three-party (foreign-to-foreign) handoff. The handoff was received from another foreign controller, and the new controller is requesting the anchor to move the client.
- Anchor Deny Received—Number of anchor requests that were denied by the current anchor.
- Anchor Grant Received—Number of anchor requests that were approved by the current anchor.
- Anchor Transfer Received—Number of anchor requests that closed the session on the current anchor and transferred the anchor back to the requestor.

• Mobility Responder Statistics

- Handoff Requests Ignored—Number of handoff requests or client announcements that were ignored because the controller had no knowledge of that client.
- Ping Pong Handoff Requests Dropped—Number of handoff requests that were denied because the handoff period was too short (3 seconds).
- Handoff Requests Dropped—Number of handoff requests that were dropped due to either an incomplete knowledge of the client or a problem with the packet.
- Handoff Requests Denied—Number of handoff requests that were denied.
- Client Handoff as Local—Number of handoff responses sent while the client is in the local role.
- Client Handoff as Foreign—Number of handoff responses sent while the client is in the foreign role.
- Anchor Requests Received—Number of anchor requests received.
- Anchor Requests Denied—Number of anchor requests denied.
- Anchor Requests Granted—Number of anchor requests granted.
- Anchor Transferred—Number of anchors transferred because the client has moved from a foreign controller to a controller on the same subnet as the current anchor.

Step 2 If you want to clear the current mobility statistics, click **Clear Stats**.

Viewing Mobility Group Statistics (CLI)

Step 1 See mobility group statistics by entering this command:

show mobility statistics

Step 2 Clear the current mobility statistics by entering this command:

clear stats mobility

CHAPTER 142

Auto-Anchor Mobility

- Information about Auto-Anchor Mobility, on page 1003
- Restrictions for Auto-Anchor Mobility, on page 1004
- Configuring Auto-Anchor Mobility (GUI), on page 1005
- Configuring Auto-Anchor Mobility (CLI), on page 1006

Information about Auto-Anchor Mobility

You can use auto-anchor mobility (also called guest tunneling) to improve load balancing and security for roaming clients on your wireless LANs. Under normal roaming conditions, client devices join a wireless LAN and are anchored to the first controller that they contact. If a client roams to a different subnet, the controller to which the client roamed sets up a foreign session for the client with the anchor controller. However, when you use the auto-anchor mobility feature, you can specify a controller or set of controllers as the anchor points for clients on a wireless LAN.

In auto-anchor mobility mode, a subset of a mobility group is specified as the anchor controllers for a WLAN. You can use this feature to restrict a WLAN to a single subnet, regardless of a client's entry point into the network. Clients can then access a guest WLAN throughout an enterprise but still be restricted to a specific subnet. Auto-anchor mobility can also provide geographic load balancing because the WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on), effectively creating a set of home controllers for a WLAN. Instead of being anchored to the first controller that they happen to contact, mobile clients can be anchored to controllers that control access points in a particular vicinity.

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the client is announced to the other controllers in the mobility list. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

If multiple controllers are added as mobility anchors for a particular WLAN on a foreign controller, the foreign controller internally sorts the controller by their IP address. The controller with the lowest IP address is the

first anchor. For example, a typical ordered list would be 172.16.7.25, 172.16.7.28, 192.168.5.15. If the first client associates to the foreign controller's anchored WLAN, the client database entry is sent to the first anchor controller in the list, the second client is sent to the second controller in the list, and so on, until the end of the anchor list is reached. The process is repeated starting with the first anchor controller. If any of the anchor controller is detected to be down, all the clients anchored to the controller are deauthenticated, and the clients then go through the authentication/anchoring process again in a round-robin manner with the remaining controller in the anchor list. This functionality is also extended to regular mobility clients through mobility failover. This feature enables mobility group members to detect failed members and reroute clients.

Restrictions for Auto-Anchor Mobility

- Mobility list members can send ping requests to one another to check the data and control paths among them to find failed members and reroute clients. You can configure the number and interval of ping requests that are sent to each anchor controller. This functionality provides guest N+1 redundancy for guest tunneling and mobility failover for regular mobility.
- You must add controllers to the mobility group member list before you can designate them as mobility anchors for a WLAN.
- You can configure multiple controllers as mobility anchors for a WLAN.
- Auto-anchor mobility supports web authentication but does not support other Layer 3 security types.
- You must configure the WLANs on both the foreign controller and the anchor controller with mobility anchors. On the anchor controller, configure the anchor controller itself as a mobility anchor. On the foreign controller, configure the anchor as a mobility anchor.
- It is not possible for clients, WGB, and wired clients to directly connect to a DMZ guest anchor and move to a foreign controller.
- Auto-anchor mobility is not supported for use with DHCP option 82.
- When using the guest N+1 redundancy and mobility failover features with a firewall, make sure that the following ports are open:
  - UDP 16666 for tunnel control traffic
  - IP Protocol 97 for user data traffic
  - UDP 161 and 162 for SNMP
- In case of roaming between anchor controller and foreign mobility, the client addresses learned at the anchor controller is shown at the foreign controller. You must check the foreign controller to view the RA throttle statistics.
- For Layer 3 RADIUS authentication, the RADIUS requests for authentication are sent by the anchor controller.
- The mobility anchor is not supported on virtual wireless LAN controllers.
- In a guest anchor Cisco WLC deployment, ensure that the foreign Cisco WLC does not have a WLAN mapped to a VLAN that is associated with the guest anchor Cisco WLC.
- In Old Mobility, when roaming from foreign to anchor WLC, the other foreign WLCs in the mobility group do not receive mobile announce messages.

Configuring Auto-Anchor Mobility (GUI)

Step 1 Configure the controller to detect failed anchor controllers within a mobility group as follows:

a) Choose **Controller** > **Mobility Management** > **Mobility Anchor Config** to open the Mobility Anchor Config page.

b) In the Keep Alive Count text box, enter the number of times a ping request is sent to an anchor controller before the anchor is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.

c) In the Keep Alive Interval text box, enter the amount of time (in seconds) between each ping request that is sent to an anchor controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.

d) In the DSCP Value text box, enter the DSCP value. The default is 0.

Note While configuring the Mobility DSCP value, the mobility control socket (i.e control messages exchanged between mobility peers only and not the data) is also updated. The configured value must reflect in the IPV4 header TOS field. This is a global configuration on the controller that is used to communicate among configured mobility peers only.

e) Click **Apply** to commit your changes.

Step 2 Choose **WLANs** to open the WLANs page.

Step 3 Click the blue drop-down arrow for the desired WLAN or wired guest LAN and choose **Mobility Anchors**. The Mobility Anchors page appears.

This page lists the controllers that have already been configured as mobility anchors and shows the current state of their data and control paths. Controllers within a mobility group communicate among themselves over a well-known UDP port and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. They send mpings, which test mobility control packet reachability over the management interface over mobility UDP port 16666 and they send epings, which test the mobility data traffic over the management interface over EoIP port 97. The Control Path text box shows whether mpings have passed (up) or failed (down), and the Data Path text box shows whether epings have passed (up) or failed (down). If the Data or Control Path text box shows “down,” the mobility anchor cannot be reached and is considered failed.

Step 4 Select the IPv4/IPv6 address of the controller to be designated a mobility anchor in the Switch IP Address (Anchor) drop-down list.

Step 5 Click **Mobility Anchor Create**. The selected controller becomes an anchor for this WLAN or wired guest LAN.

Note To delete a mobility anchor for a WLAN or wired guest LAN, hover your cursor over the blue drop-down arrow for the anchor and choose **Remove**.

Step 6 Click **Save Configuration**.

Step 7 Repeat *Step 4* and *Step 6* to set any other controllers as mobility anchors for this WLAN or wired guest LAN.

Step 8 Configure the same set of mobility anchors on every controller in the mobility group.

Configuring Auto-Anchor Mobility (CLI)

Procedure

	Command or Action	Purpose
Step 1	The controller is programmed to always detect failed mobility list members. To change the parameters for the ping exchange between mobility members, enter these commands:	• **config mobility group keepalive count** *count*—Specifies the number of times a ping request is sent to a mobility list member before the member is considered to be unreachable. The valid range is 3 to 20, and the default value is 3. • **config mobility group keepalive interval** *seconds*—Specifies the amount of time (in seconds) between each ping request sent to a mobility list member. The valid range is 1 to 30 seconds, and the default value is 10 seconds.
Step 2	Disable the WLAN or wired guest LAN for which you are configuring mobility anchors by entering this command:	**config {wlan | guest-lan} disable** {*wlan_id* | *guest_lan_id*}
Step 3	Create a new mobility anchor for the WLAN or wired guest LAN by entering one of these commands:	• **config mobility group anchor add** {**wlan | guest-lan**} {*wlan_id* | *guest_lan_id*} *anchor_controller_ip_address* • **config** {**wlan | guest-lan**} **mobility anchor add** {*wlan_id* | *guest_lan_id*} *anchor_controller_ip_address* **Note** The *wlan_id* or *guest_lan_id* must exist and be disabled, and the *anchor_controller_ip_address* must be a member of the default mobility group. Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.
Step 4	Delete a mobility anchor for the WLAN or wired guest LAN by entering one of these commands:	• **config mobility group anchor delete {wlan | guest-lan} {wlan_id | guest_lan_id}** anchor_controller_ip_address • **config {wlan | guest-lan} mobility anchor delete {wlan_id | guest_lan_id}** anchor_controller_ip_address **Note** The *wlan_id* or *guest_lan_id* must exist and be disabled. Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.

	Command or Action	Purpose
Step 5	Save your settings by entering this command:	**save config**
Step 6	See a list and status of controllers configured as mobility anchors for a specific WLAN or wired guest LAN by entering this command:	**show mobility anchor** {**wlan** | *guest-lan*} {*wlan_id* | *guest_lan_id*} **Note** The *wlan_id* and *guest_lan_id* parameters are optional and constrain the list to the anchors in a particular WLAN or guest LAN. To see all of the mobility anchors on your system, enter the **show mobility anchor** command. The Status text box shows one of these values: UP—The controller is reachable and able to pass data. CNTRL_PATH_DOWN—The mpings failed. The controller cannot be reached through the control path and is considered failed. DATA_PATH_DOWN—The epings failed. The controller cannot be reached and is considered failed. CNTRL_DATA_PATH_DOWN—Both the mpings and epings failed. The controller cannot be reached and is considered failed.
Step 7	See the status of all mobility group members by entering this command:	**show mobility summary**
Step 8	Troubleshoot mobility issues by entering these commands:	• **debug mobility handoff** {**enable** | **disable**}—Debugs mobility handoff issues. • **debug mobility keep-alive** {**enable** | **disable**} **all**—Dumps the keepalive packets for all mobility anchors. • **debug mobility keep-alive** {**enable** | **disable**} *IP_address*—Dumps the keepalive packets for a specific mobility anchor.

CHAPTER 143

Validating WLAN Mobility Security Values

- WLAN Mobility Security Values, on page 1009

WLAN Mobility Security Values

For any anchoring or mobility event, the WLAN security policy values on each controller must match. These values can be validated in the controller debugs. This table lists the WLAN mobility security values and their corresponding security policy.

Table 36: WLAN Mobility Security Values

Security Hexadecimal Value	Security Policy
0x00000000	Security_None
0x00000001	Security_WEP
0x00000002	Security_802_1X
0x00000004	Security_IPSec*
0x00000008	Security_IPSec_Passthrough*
0x00000010	Security_Web
0x00000020	Security_PPTP*
0x00000040	Security_DHCP_Required
0x00000080	Security_WPA_NotUsed
0x00000100	Security_Cranite_Passthrough*
0x00000200	Security_Fortress_Passthrough*
0x00000400	Security_L2TP_IPSec*
0x00000800	Security_802_11i_NotUsed **Note** Controllers running software release 6.0 or later do not support this security policy.

Security Hexadecimal Value	Security Policy
0x00001000	Security_Web_Passthrough

CHAPTER 144

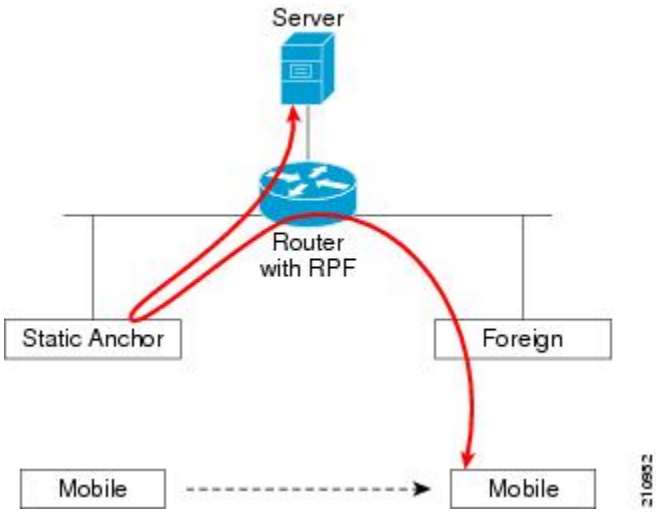
Using Symmetric Mobility Tunneling

- Information About Symmetric Mobility Tunneling, on page 1011
- Guidelines and Limitations, on page 1012
- Verifying Symmetric Mobility Tunneling (GUI), on page 1012
- Verifying if Symmetric Mobility Tunneling is Enabled (CLI), on page 1012

Information About Symmetric Mobility Tunneling

When symmetric mobility tunneling is enabled, all client traffic is sent to the anchor controller and can then successfully pass the RPF check.

Figure 65: Symmetric Mobility Tunneling or Bi-Directional Tunneling



Symmetric mobility tunneling is also useful in the following situations:

- If a firewall installation in the client packet path drops packets because the source IP address does not match the subnet on which the packets are received.
- If the access-point group VLAN on the anchor controller is different than the WLAN interface VLAN on the foreign controller. In this case, client traffic could be sent on an incorrect VLAN during mobility events.

Guidelines and Limitations

- Symmetric mobility tunneling is enabled by default.

Verifying Symmetric Mobility Tunneling (GUI)

Step 1 Choose **Controller** > **Mobility Management** > **Mobility Anchor Config** to open the Mobility Anchor Config page.

Step 2 The Symmetric Mobility Tunneling Mode text box shows Enabled.

Verifying if Symmetric Mobility Tunneling is Enabled (CLI)

Verify that symmetric mobility tunneling is enabled by entering this command:

show mobility summary

CHAPTER 145

Running Mobility Ping Tests

- Mobility Ping Tests, on page 1013
- Restrictions for Mobility Ping Tests, on page 1013
- Running Mobility Ping Tests (CLI), on page 1014

Mobility Ping Tests

Controllers in a mobility list communicate with each other by controlling information over a well-known UDP port and exchanging data traffic through an Ethernet-over-IP (EoIP) tunnel. Because UDP and EoIP are not reliable transport mechanisms, there is no guarantee that a mobility control packet or data packet will be delivered to a mobility peer. Mobility packets may be lost in transit due to a firewall filtering the UDP port or EoIP packets or due to routing issues.

Restrictions for Mobility Ping Tests

- You can test the mobility communication environment by performing mobility ping tests. These tests may be used to validate connectivity between members of a mobility group (including guest controllers). Two ping tests are available:
  - Mobility ping over UDP—This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.
  - Mobility ping over EoIP—This test runs over EoIP. It tests the mobility data traffic over the management interface.
- Only one mobility ping test per controller can be run at a given time.
- These ping tests are not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

Note Any ICMP packet greater than 1280 bytes will always be responded with a packet that is truncated to 1280 bytes. For example, a ping with a packet that is greater than 1280 bytes from a host to the management interface is always responded with a packet that is truncated to 1280 bytes.

- Mobility pings on ports 16666 and 16667 are notable exemptions and these ports cannot be blocked by any ACL.

Running Mobility Ping Tests (CLI)

Step 1 To test the mobility UDP control packet communication between two controllers, enter this command:

mping *mobility_peer_IP_address*

The *mobility_peer_IP_address* parameter must be the IP address of a controller that belongs to the mobility list.

Step 2 To test the mobility EoIP data packet communication between two controllers, enter this command:

eping *mobility_peer_IP_address*

The *mobility_peer_IP_address* parameter must be the IP address of a controller that belongs to the mobility list.

Step 3 To troubleshoot your controller for mobility ping, enter these commands:

config logging buffered debugging

show logging

Step 4 To troubleshoot your controller for mobility ping over UDP, enter this command to display the mobility control packet:

debug mobility handoff enable

Note We recommend using an ethereal trace capture when troubleshooting.

CHAPTER 146

Configuring Dynamic Anchoring for Clients with Static IP Addresses

- Dynamic Anchoring for Clients with Static IP, on page 1015
- Restrictions on Dynamic Anchoring for Clients With Static IP Addresses, on page 1016
- Configuring Dynamic Anchoring of Static IP Clients (GUI), on page 1016
- Configuring Dynamic Anchoring of Static IP Clients (CLI), on page 1017

Dynamic Anchoring for Clients with Static IP

At times you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they could try associating with other controllers. If the clients try to associate with a controller that does not support the same subnet as the static IP, the clients fail to connect to the network. You can now enable dynamic tunneling of clients with static IP addresses.

Dynamic anchoring of static IP clients with static IP addresses can be associated with other controllers where the client's subnet is supported by tunneling the traffic to another controller in the same mobility group. This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses.

How Dynamic Anchoring of Static IP Clients Works

The following sequence of steps occur when a client with a static IP address tries to associate with a controller:

1. When a client associates with a controller, for example, WLC-1, it performs a mobility announcement. If a controller in the mobility group responds (for example WLC-2), the client traffic is tunneled to the controller WLC-2. As a result, the controller WLC 1 becomes the foreign controller and WLC-2 becomes the anchor controller.
2. If none of the controllers responds, the client is treated as a local client and authentication is performed. The IP address for the client is updated either through an orphan packet handling or an ARP request processing. If the IP subnet of the client is not supported in the controller (WLC-1), WLC-1 sends another static IP mobile announce and if a controller (for example WLC-3) that supports the client's subnet responds to that announcement, the client traffic is tunneled to that controller, that is WLC-3. As a result, the controller WLC 1 becomes the export foreign controller and WLC-3 becomes the export anchor controller.
3. Once the acknowledgment is received, the client traffic is tunneled between the anchor and the controller (WLC-1).

Note If you configure WLAN with an interface group and any of the interfaces in the interface group supports the static IP client subnet, the client is assigned to that interface. This situation occurs in local or remote (static IP Anchor) controller.

When AAA override is used along with the interface group that is mapped to WLAN, the source interface that is used for DHCP transactions is the Management interface.

If the interface group that you add to a WLAN has RADIUS Server Overwrite interface enabled and a client requests for authentication, the controller selects the first IP address from the interface group as the RADIUS server.

Note A security level 2 authentication is performed only in the local (static IP foreign) controller, which is also known as the exported foreign controller.

Restrictions on Dynamic Anchoring for Clients With Static IP Addresses

- Do not configure overridden interfaces when you perform AAA for static IP tunneling, this is because traffic can get blocked for the client if the overridden interface does not support the client's subnet. This can be possible in extreme cases where the overriding interface group supports the client's subnet.
- The local controller must be configured with the correct AAA server where this client entry is present.

The following restrictions apply when configuring static IP tunneling with other features on the same WLAN:

- Auto anchoring mobility (guest tunneling) cannot be configured for the same WLAN.
- FlexConnect local authentication cannot be configured for the same WLAN.
- The DHCP required option cannot be configured for the same WLAN.
- You cannot configure dynamic anchoring of static IP clients with FlexConnect local switching.
- We recommend that you configure the same NTP/SNTP servers on the Cisco WLCs. If the NTP/SNTP servers are different, ensure that the system time on all Cisco WLCs is the same when NTP/SNTP is enabled. If the system time is not in sync, seamless mobility might fail in some scenarios. Also, a Cisco WLC that has the lagging time with NTP/SNTP enabled drops the mobile announce messages.

Configuring Dynamic Anchoring of Static IP Clients (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN on which you want to enable dynamic anchoring of IP clients. The WLANs > Edit page is displayed.

Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4 Enable dynamic anchoring of static IP clients by selecting the **Static IP Tunneling** check box.

Step 5 Click **Apply** to commit your changes.

Configuring Dynamic Anchoring of Static IP Clients (CLI)

config wlan static-ip tunneling {enable | disable} *wlan_id*— Enables or disables the dynamic anchoring of static IP clients on a given WLAN.

To monitor and troubleshoot your controller for clients with static IP, use the following commands:

- **show wlan** *wlan_id*—Enables you to see the status of the static IP clients feature.

```
.....
Static IP client tunneling.............. Enabled
.....
```

- **debug client** *client-mac*
- **debug dot11 mobile** enable
- **debug mobility handoff** enable

CHAPTER 147

Configuring Foreign Mappings

- Information About Foreign Mappings, on page 1019
- Configuring Foreign Controller MAC Mapping (GUI), on page 1019
- Configuring Foreign Controller MAC Mapping (CLI), on page 1019

Information About Foreign Mappings

Auto-Anchor mobility, also known as Foreign Mapping, allows you to configure users that are on different foreign controllers from different physical location to obtain IP addresses from a subnet or group of subnets based on their physical location.

Configuring Foreign Controller MAC Mapping (GUI)

Step 1 Choose **WLANs**.

The WLANs page appears listing the available WLANs.

Step 2 Click the blue drop-down arrow for the desired WLAN and choose **Foreign-Maps**.

The foreign mappings page is displayed. This page also lists the MAC addresses of the foreign controllers that are in the mobility group and interfaces/interface groups.

Step 3 Choose the desired foreign controller MAC and the interface or interface group to which it must be mapped and click **Add Mapping**.

Configuring Foreign Controller MAC Mapping (CLI)

Procedure

- To add foreign controller mapping, enter this command:

  config wlan mobility foreign-map add *wlan-id foreign-ctlr-mac-addr interface-or-interface-grp-name*

CHAPTER 148

Configuring Proxy Mobile IPv6

- Proxy Mobile IPv6, on page 1021
- Restrictions on Proxy Mobile IPv6, on page 1023
- Configuring Proxy Mobile IPv6 (GUI), on page 1023
- Configuring Proxy Mobile IPv6 (CLI), on page 1025

Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in an IP mobility-related signaling scenario. The mobility entities in the network track the movements of the mobile node, initiate mobility signaling, and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The Cisco Wireless LAN Controller (WLC) implements the MAG functionality.

In the Cisco 5508 WLC, Cisco WiSM2, and Cisco 8510 WLCs, PMIPv6 MAG support for integration with LMA such as Cisco ASR 5000 Series in cellular data networks.

For PMIPv6 clients, Cisco WLC supports both central web authentication and local web authentication.

PMIPv6 is supported for clients with 802.1X authentication. After the 802.1X authentication is complete, a Cisco AP starts PMIPv6 signaling for the corresponding client.

Dynamic AAA Attributes

The dynamic AAA attributes that are supported are listed below:

Type	Attribute	Value	Description	Cisco WLC Behavior
89	Chargeable-User-Identity	String	Chargeable User Identity RFC-4372	If present, the attribute is copied into the MSCB and used in accounting reports; no other usage.

Type	Attribute	Value	Description	Cisco WLC Behavior
26/104 15/13	3GPP-Charging-Characteristics	String	Rules for producing charging information	If present, the attribute is copied to the MSCB and passed to the L2 attach triggers to the MAG. The attribute is used to send to the local mobility anchor (LMA) as an option in the proxy binding update (PBU).
26/9/1	Cisco-Service-Selection	String	Service Identifier (APN)	If present, the attribute overrides the locally configured APN.
26/9/1	Cisco-Mobile-Node-Identifier	String	Mobile Node Identifier	If present, the attribute is used for the network access identifier (NAI).
26/9/1	Cisco-MSISDN	String	Mobile Subscriber ISDN Number	If present, the attribute is used to pass to MAG code with a new parameter in the L2 attach trigger.
26/9/1	Cisco-MPC-Protocol-Interface	ENUM: "none" "PMIPv6" "GTPv1" "PMIPv4"	Mobile Node Service Type	Only IPv4 and simple IP clients are supported.
26/9/1	Cisco-URL-REDIRECT	String	HTTP URL of the Captive Portal	Existing attribute used for web authentication; no changes required.
26/9/1	Cisco-URL-REDIRECT-ACL	String	Specific Redirect Rule	Existing attribute used for web authentication; no changes required.
26/9/1	Cisco-Home-LMA-IPv4-Address	IP Address	Mobile node's Home LMA IPv4 address	If present, this attribute is used as the LMA for the client. **Note** The GRE tunnel creation is still static.

PMIPv6 AAA Attributes

The PMIPv6 AAA attributes that are supported are listed below:

Type	Attribute	Value	Description	Cisco WLC Behavior
89	Chargeable-User-Identity	String	Chargeable User Identity RFC-4372	If present, the attribute is copied into the MSCB and used in accounting reports; no other usage.
26/104 15/13	3GPP-Charging-Characteristics	String	Rules for producing charging information	If present, the attribute is copied to the MSCB and passed to the L2 attach triggers to the MAG. The attribute is used to send to the local mobility anchor (LMA) as an option in the proxy binding update (PBU).
26/9/1	mn-network	String	Service Identifier (APN)	If present, the attribute overrides the locally configured APN (Mandatory)

Type	Attribute	Value	Description	Cisco WLC Behavior
26/9/1	mn-nai	String	Mobile Node Identifier	If present, the attribute is used for the network access identifier (NAI).
26/9/1	cisco-msisdn	String	Mobile Subscriber ISDN Number	If present, the attribute is used to pass to MAG code with a new parameter in the L2 attach trigger.
26/9/1	cisco-mpc-protocol-interface	ENUM: "None" "PMIPv6"	Mobile Node Service Type	Only PMIPv6 clients are supported. (Mandatory)
26/9/1	home-lma-ipv4-address	IPv4 Address	Mobile node's Home LMA IPv4 address	If present, this attribute is used as the LMA for the client. The LMA should also be configured in WLC (Mandatory). **Note** The GRE tunnel creation is still static.
26/9/1	mn-service	ENUM: "IPv4"	Type of client	Only IPv4 is supported.

Restrictions on Proxy Mobile IPv6

- IPv6/dual stack clients are not supported. Only IPv4 is supported with PMIPv6.
- You must enable DHCP Proxy before you can connect to a PMIPv6-enabled WLAN.
- PMIPv6 is not supported on local switching WLANs with FlexConnect mode APs.
- PMIPv6 on FlexConnect ACL with local switching is not supported.

Configuring Proxy Mobile IPv6 (GUI)

Step 1 Choose **Controller > PMIPv6 > General**. The **PMIPv6 General**window is displayed.

Step 2 Enter the values for the following parameters:

- **Domain Name**—Name of the PMIPv6 domain. The domain name can be up to 127 case-sensitive, alphanumeric characters.
- **MAG Name**—Name of the MAG.
- **Maximum Bindings Allowed**—Maximum number of binding updates that the Cisco WLC can send to the MAG. The valid range is between 0 and 40000.
- **Binding Lifetime**—Lifetime, in seconds, of the binding entries in the Cisco WLC. The valid range is between 10 and 65535. The default value is 3600. The binding lifetime should be a multiple of 4.

- **Binding Refresh Time**—Refresh time, in seconds, of the binding entries in the Cisco WLC. The valid range is between 4 and 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4.
- **Binding Initial Retry Timeout**—Initial timeout, in milliseconds, between the Proxy Binding Updates (PBUs) when the Cisco WLC does not receive the Proxy Binding Acknowledgments (PBAs). The valid range is between 100 and 65535. The default value is 1000.
- **Binding Maximum Retry Timeout**—Maximum timeout between the PBUs when the Cisco WLC does not receive the PBAs. The valid range is between 100 and 65535. The default value is 32000.
- **Replay Protection Timestamp**—Maximum amount of time, in milliseconds, difference between the timestamp in the received PBA and the current time of the day. The valid range is between 1 and 255. The default value is 7.
- **Minimum BRI Retransmit Timeout**—Minimum amount of time, in milliseconds, that the Cisco WLC waits for before retransmitting the BRI message. The valid range is between 500 and 65535. The default value is 1000.
- **Maximum BRI Retransmit Timeout**—Maximum amount of time, in milliseconds, that the Cisco WLC waits for before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 and 65535. The default value is 2000.
- **BRI Retries**—Maximum number of times that the Cisco WLC retransmits the BRI message before receiving the Binding Revocation Acknowledgment (BRA) message. The valid range is between 1 to 10. The default value is 1.

Step 3 Click **Apply**.

Note To clear your configuration, click **Clear Domain**.

Step 4 To create the LMA, follow these steps:

a) Choose **Controller > PMIPv6 > LMA** and click **New**.
b) Enter the values for the following parameters:
   - **Member Name**—Name of the LMA connected to the Cisco WLC.
   - **Member IP Address**—IP address of the LMA connected to the Cisco WLC.
c) Click **Apply**.

Step 5 To create a PMIPv6 profile, follow these steps:

a) Choose **Controller > PMIPv6 > Profiles** and click **New**.
b) In the **PMIPv6 Profile > New** window, enter the values for the following parameters:
   - **Profile Name**—Name of the profile.
   - **Network Access Identifier**—Name of the Network Access Identifier (NAI) associated with the profile.
   - **LMA Name**—Name of the LMA to which the profile is associated.
   - **Access Point Node**—Name of the access point node; APN identifies a particular routing domain for user traffic.
c) Click **Apply**.

Step 6 To configure PMIPv6 parameters for a WLAN, follow these steps:

a) Choose **WLANs > WLAN ID**. The **WLANs > Edit** window is displayed.
b) Click the **Advanced** tab.
c) Under **PMIP**, from the **PMIP Mobility Type** drop-down list, choose the mobility type from the following options:

- **None**—Configures the WLAN with simple IP
- **PMIPv6**—Configures the WLAN with only PMIPv6

d) From the **PMIP Profile** drop-down list, choose the PMIP profile for the WLAN.
e) In the **PMIP Realm** field, enter the default realm for the WLAN.
f) Click **Apply**.

Step 7 Click **Save Configuration**.

Configuring Proxy Mobile IPv6 (CLI)

Step 1 Configure a PMIPv6 domain name by entering this command:

config pmipv6 domain *domain-name*

Note This command also enables the MAG functionality on the Cisco Wireless Controller (WLC).

Step 2 Configure MAG by using these commands:

- Configure the maximum binding update entries that are allowed by entering this command:

  config pmipv6 mag binding maximum *units*

- Configure the binding entry lifetime by entering this command:

  config pmipv6 mag lifetime *units*

- Configure the binding refresh interval by entering this command:

  config pmipv6 mag refresh-time *units*

- Configure the initial timeout between PBUs if PBA does not arrive by entering this command:

  config pmipv6 mag init-retx-time *units*

- Configure the maximum initial timeout between PBUs if PBA does not arrive by entering this command:

  config pmipv6 mag max-retx-time *units*

- Configure the replay protection mechanism by entering this command:

  config pmipv6 mag replay-protection {**timestamp window** *units* | **sequence-no** | **mobile-node-timestamp**}

- Configure the minimum or maximum amount of time, in seconds, that the MAG should wait for before it retransmits the binding revocation indication (BRI) message by entering this command:

  config pmipv6 mag bri delay {**min** | **max**} *units*

- Configure the maximum number of times the MAG should retransmit the BRI message before it receives the binding revocation acknowledgment (BRA) message by entering this command:

  config pmipv6 mag bri retries *units*

- Configure the list of LMAs for the MAG by entering this command:

config pmipv6 mag lma *lma-name* **ipv4-address** *ip-address*

Step 3 Add a profile to a PMIPv6 domain by entering this command:

config pmipv6 add profile *profile-name* **nai** {*user@realm* | *@realm* | *} **lma** *lma-name* **apn** *apn-name*

Note nai stands for network access identifier, while apn stands for access point name.

Step 4 Delete a PMIPv6 entity by entering this command:

config pmipv6 delete {**domain** *domain-name* | **lma** *lma-name* | **profile** *profile-name* **nai** {*user@realm* | *@realm* | *}}

Step 5 Configure the PMIPv6 parameters for the WLAN by using these commands:

- Configure the default realm for the WLAN by entering this command:

  config wlan pmipv6 default-realm {*realm-name* | **none**} *wlan-id*

- Configure the mobility type for a WLAN or for all WLANs by entering this command:

  config wlan pmipv6 mobility-type {**none** | **pmipv6**} {*wlan-id* | **all**}

- Configure the profile name for a PMIPv6 WLAN by entering this command:

Step 6 Save your changes by entering this command:

save config

Step 7 See the PMIPv6 configuration details by using the following **show** commands:

- See the details of a profile of a PMIPv6 domain by entering this command:

  show pmipv6 domain *domain-name* **profile** *profile-name*

- See a summary of all the PMIPv6 profiles by entering this command:

  show pmipv6 profile summary

- See global information about the PMIPv6 for a MAG by entering this command:

  show pmipv6 mag globals

- See information about MAG bindings for LMA or NAI by entering this command:

  show pmipv6 mag bindings {**lma** *lma-name* | **nai** *nai-name*}

- See statistical information about MAG by entering this command:

  show pmipv6 mag stats domain *domain-name* **peer** *peer-name*

- See information about PMIPv6 for all clients by entering this command:

  show client summary

- See information about PMIPv6 for a client by entering this command:

  show client details *client-mac-address*

- See information about PMIPv6 for a WLAN by entering this command:

show wlan *wlan-id*

CHAPTER 149

Configuring New Mobility

- Information About New Mobility, on page 1029
- Restrictions for New Mobility , on page 1029
- Configuring New Mobility (GUI), on page 1030
- Configuring New Mobility (CLI) , on page 1031

Information About New Mobility

New Mobility enables Cisco WLCs to be compatible with converged access controllers with Wireless Control Module (WCM) such as the Cisco Catalyst 3850 Series Switches and the Cisco 5760 Series Wireless LAN Controllers. New Mobility provides the ability to run Mobility Controller (MC) functionality on a Cisco WLC in the Converged Access mode with a Catalyst 3850 mobility agent (MA)

The Mobility Controller is a part of a hierarchical architecture that consists of a Mobility Agent and Mobility Oracle.

A group of Cisco Catalyst 3850 Series Switches' Mobility Agents can form a switch peer group. The internal Mobility Agent of Cisco WLCs form an independent switch peer group. The Mobility Controller, Mobility Agent, and Mobility Oracle can be in a single Cisco WLC. Each Mobility Controller forms a subdomain that can have multiple switch peer groups. The Cisco WLCs are Mobility Agents by default. However, Cisco Catalyst 3850 Series Switch can function both as Mobility Agent and Mobility Controller, or only as a Mobility Agent.

By default, New Mobility is disabled. When you enable or disable new mobility, you must save the configuration and reboot the controller.

Note With Release 8.1 in a New Mobility environment, Cisco WLCs running Cisco Wireless software cannot function as mobility controllers (MC). However, the Cisco WLCs can function as guest anchors.

Restrictions for New Mobility

- The keepalives between Mobility Controller and Mobility Oracle are not DTLS encrypted.
- For seamless mobility, the controller should either use new mobility or old mobility (flat mobility).

- Interoperability between two types of mobility is not supported. When you downgrade the controller from Release 7.5 to a controller software release that does not support new mobility, such as Releases 7.4.100.0, 7.3.101.0, 7.2, 7.0, or earlier (all releases prior to 7.3.112.0), the controller automatically transits to flat mobility (old mobility). This is due to the difference in mobility architecture and noninteroperability between flat mobility (EOIP tunnels) and new mobility(CAPWAP tunnels).
- High availability for Mobility Oracle is not supported.
- When a client associates for the very first time as local, then in the Cisco WLC, the MA sends a 'handoff complete' message to the MC to update the client database in the MC. However, the 'handoff complete' message is sent in a 'DHCP REQD' state because of which the IP address of the client is 0.0.0.0 for the very first time. This event is triggered by timer expiry.
- IPv6 is not supported with new mobility.

Configuring New Mobility (GUI)

Step 1 Choose **Controller > Mobility Management > Mobility Configuration** to enable and configure new mobility on the controller.

Note When you enable or disable new mobility, you must save the configuration and reboot the controller.

Step 2 To configure new mobility, select or unselect the **Enable New Mobility (Converged Access)** check box.

Note When you enable new mobility, you must save the configuration and reboot the controller.

Step 3 To configure the controller as Mobility Oracle, select or unselect the **Mobility Oracle** check box.

Note Mobility Oracle is optional; it maintains the client database under one complete mobility domain.

Step 4 To configure multicast mode in a mobility group, select or unselect the **Multicast Mode** check box.

Step 5 In the **Multicast IP Address** text box, enter the multicast IP address of the switch peer group.

Step 6 In the **Mobility Oracle IP Address** text box, enter the IP address of the Mobility Oracle.

You cannot enter a value for this field if you have checked the **Mobility Oracle** check box.

Step 7 In the **Mobility Controller Public IP Address** text box, enter the IP address of the controller, if there is no network address translation (NAT).

Note If the controller has NAT configured, the public IP address will be the network address translated IP address.

Note New mobility does not support IPv6.

Step 8 In the **Mobility Keep Alive Count** text box, enter the number of times a ping request is sent to a peer controller before the peer is considered to be unreachable. The range is from 3 to 20. The default value is 3.

Step 9 In the **Mobility Keep Alive Interval** text box, enter the amount of time, in seconds, between each ping request sent to an peer controller. The range is from 1 to 30 seconds. The default value is 10 seconds.

Step 10 In the **Mobility DSCP** text box, enter the DSCP value that you can set for the mobility controller. The range is from 0 to 63. The default value is 0.

Note While configuring the Mobility DSCP value, the mobility control socket (i.e control messages exchanged between mobility peers only and not the data) is also updated. The configured value must reflect in the IPV4 header TOS field. This is a global configuration on the controller that is used to communicate among configured mobility peers only.

Step 11 Click **Apply**.

Step 12 Choose **Controller > Mobility Management > Switch Peer Group** to add or remove members to and from the switch peer group.

This page lists all the switch peer groups and their details, such as bridge domain ID, multicast IP address, and status of the multicast mode. Click the name of the switch peer group to navigate to the **Edit** page and update the parameters, if required.

Step 13 Choose **Controller > Mobility Management > Mobility Controller** to view all the mobility controllers and their details, such as IP address, MAC address, client count, and link status.

Step 14 Choose **Controller > Mobility Management > Mobility Clients** to view all the mobility clients and their parameters.

Step 15 In the **Client MAC Address** and **Client IP Address** text boxes, enter the MAC address and IP address of the mobility client, respectively.

Step 16 In the **Anchor MC IP Address** and **Anchor MC Public IP Address** text boxes, enter the IP address and public IP address of the anchor Mobility Controller, respectively.

Step 17 In the **Foreign MC IP Address** and **Foreign MC Public IP Address** text boxes, enter the IP address and public IP address of the foreign MC, respectively.

Step 18 In the **Client Association Time** text box, enter the time at which the mobility client should be associated with the Mobility Controller.

Step 19 In the **Client Entry Update Timestamp** text box, enter the timestamp at which the client entry should be updated.

Configuring New Mobility (CLI)

Procedure

- Enable or disable new mobility on the controller by entering this command:

  config mobility new-architecture {**enable** | **disable**}

Note When you enable or disable new mobility, you must save the configuration and reboot the controller.

- Enable the Mobility Oracle or configure an external Mobility Oracle by entering this command:

  config mobility oracle {**enable** | **disable** | **ip** *ip_address*}

  Here, *ip_address* is the IP address of the Mobility Oracle. The Mobility Oracle maintains the client database under one complete mobility domain. It consists of a station database, an interface to the Mobility Controller, and an NTP/SNTP server. There can be only one Mobility Oracle in the entire mobility domain.

- Create or delete switch peer groups by entering this command:

config mobility switchPeerGroup {**create** | **delete**} *peer-group-name*

Here, *peer-group-name* is the name of the switch peer group.

- Configure the MAC address of the member switch for compatibility between the flat (old) and new mobility by entering this command:

  config mobility group member add *ip_address* {[*group-name*] | *mac-address* | [*public-ip-address*]}

  where *ip_address* is the IP address of the member.

  group-name is the member switch group name, if it is different from the default group name.

  mac-address is the MAC address of the member switch.

Note If the controller has NAT configured, the public IP address will be the network address translated IP address.

Note New mobility does not support IPv6.

- Add or remove members and configure the bridge domain ID and multicast address of the switch peer group by entering this command:

  config mobility switchPeerGroup {**bridge-domain-id** *peer-group-name bridge domain id* | **member** {**add** | **delete**} *IP_address* [*public_IP_address*] *peer-group-name* | **multicast-address** *peer-group-name multicast_IP_address*}

  Here, *peer-group-name* is the name of the switch peer group.

  IP_address is the IP address of switch peer group member.

  public_IP_address is the public IP address of the switch peer group member.

- View the details of the mobility controllers according to the Mobility Oracle by entering this command:

  show mobility oracle summary

- View the summary and details of the Mobility Oracle client database by entering this command:

  show mobility oracle client {**summary** | **detail**}

- Verify the mobility statistics by entering this command:

  show mobility statistics

- Verify the mobility configuration by entering this command:

  show mobility summary

- Save your changes by entering this command:

  save config

- Enable or disable debugging of mobility packets by entering this command:

  debug mobility packet {**enable** | **disable**}

- Enable or disable debugging of the Mobility Oracle events and errors by entering this command:
  debug mobility oracle {**events** | **errors**} {**enable** | **disable**}

INDEX

11n Mode parameter 77
1250 series access points 841, 842, 843
  and PoE Status field 843
  operating modes when using PoE 841
  transmit power settings when using PoE 842
7920 AP CAC parameter 623
7920 Client CAC parameter 623
7920 support mode 622
  configuring 622
  described 622
7921 support mode 622
802.11a (or 802.11b) > Client Roaming page 125
802.11a (or 802.11b) > Voice Parameters page 149, 151, 158
802.11a (or 802.11b/g) > EDCA Parameters page 160
802.11a (or 802.11b/g) Global Parameters page 69, 898
802.11a (or 802.11b/g) Network Status parameter 69, 80, 81
802.11a/n (or 802.11b/g/n) Radios page 153, 890
802.11a/n Radios page (from Monitor Menu) 722
802.11g Support parameter 69
802.11h Global Parameters page 81
802.11h, described 80
802.11n 77, 847
  clients 847
  devices 77
802.1Q VLAN trunk port 298
802.1Q-in-Q VLAN Tag 656
802.1Q-in-Q VLAN Tagging 657
  configuring using CLI 657
  configuring using GUI 657
802.1X 582, 594
  configuring 582
  described 594
  dynamic key settings 582
802.1X authentication for access points 729, 732, 733
  configuring 732, 733
    the switch 733
    using the CLI 732, 733
  described 729
802.1x Authentication parameter 731
802.3 bridging 101, 102
  configuring using the CLI 102
  configuring using the GUI 101, 102
802.3 Bridging parameter 102
802.3 frames 101
802.3X flow control, enabling 102

A

Access Control List Name parameter 441
access control lists (ACLs) 282, 439, 440, 444, 445, 446, 958
  applying to the controller CPU 445, 446
    using the CLI 445, 446
  configuring 444, 445
    using the CLI 444, 445
  counters 440, 445
    configuring using the CLI 445
    configuring using the GUI 440
  rules 439, 445, 958
  using with the debug facility 282
Access Control Lists > Edit page 442, 960
Access Control Lists > New page 440
Access Control Lists page 440
Access Mode parameter 92, 212
access point core dumps, uploading 755
  using the GUI 755
access point count, approved tiers for 5500 series controllers 52
access point event logs, viewing 262
access point groups 653, 655, 656
  assigning access points to 655
    using the CLI 655
    using the GUI 655
  creating 655
    using the CLI 655
  removing 653, 655
    using the CLI 655
    using the GUI 653
  viewing 656
access point monitor service, debugging 291
access point radios, searching for 723
access points 124, 250, 715, 716, 740, 741, 746, 750, 751, 760
  assisted roaming 124
  authorization list 746
  authorizing 740, 741
    using LSCs 741
    using MICs 741
    using SSCs 740
  LEDs 250
    interpreting 250
  priming 715
  supporting oversized images 760
  verifying that they join the controller 716

access points *(continued)*
viewing join information 750, 751
using the GUI 750, 751
Accounting Server parameters 670
ACL Name parameter 443
ACL. See <Default Para Font>access control lists (ACLs) 439, 957
Action parameter 442, 960
active exploits 541
Add AP button 967
Add New Rule button 441
Admin Status parameter 329, 330
administrator access 210
Admission Control (ACM) parameter 149
AES-CCMP 594
Aggregated MAC Service Data Unit (A-MSDU) 79
aggregation method, specifying 79
AirMagnet Enterprise Analyzer 288
Aironet IE parameter 644
Airopeek 288
All APs > Access Point Name > VLAN Mappings page 951
All APs > Details for (Advanced) page 712, 755, 836
configuring link latency 836
All APs > Details for (Credentials) page 727, 731
All APs > Details for (FlexConnect) page 950
All APs > Details for (General) page 950
All APs > Details for (High Availability) page 795, 812
All APs page 717, 886
AnchorTime parameter 868
Anonymous Provision parameter 417
Antenna Gain parameter 890
Antenna parameter 890
Antenna Type parameter 890
AP > Clients > Traffic Stream Metrics page 153
AP Authentication Policy page 451
AP Core Dump parameter 755
AP Ethernet MAC Addresses parameter 743
AP Failover Priority parameter 812
AP Group Name parameter 653
AP Groups > Edit (APs) page 654
AP Groups page 653, 676
AP local authentication 954
Using GUI 954
AP Local Authentication on a WLAN 954
Using the CLI 954
AP Mode parameter 288, 776, 886, 950
AP Name parameter 654
AP Primary Discovery Timeout parameter 794
ap-count evaluation licenses, activating 61, 62
using the CLI 61, 62
using the GUI 61
AP-manager interface 301, 311
and dynamic interfaces 301
described 311
AP801 access point 735
described 735
using with a controller 735
Applying ACLs to a WLAN 444
Applying ACLs to the controller CPU 443
Assignment Method parameter 891
authenticated local authentication bind method 408, 410
Authority ID Information parameter 417, 968, 970
Authority ID parameter 417, 968
Authorize LSC APs against auth-list parameter 745
Authorize MIC APs against auth-list or AAA parameter 745
auto-anchor mobility 1003, 1005
configuring 1005
using the GUI 1005
overview 1003
AutoInstall 35, 36, 37, 38, 39
described 35, 39
example operation 38
obtaining 36
DHCP addresses for interfaces 36
TFTP server information 36
selecting configuration file 37
using 35, 36
Average Data Rate parameter 132, 136, 619
Average Real-Time Rate parameter 132, 136, 619
Avoid Cisco AP Load parameter 868
Avoid Foreign AP Interference parameter 868, 996, 1000
Avoid Non-802.11a (802.11b) Noise parameter 868

B

Back-up Primary Controller Name field 794
Back-up Secondary Controller Name parameter 794
Beacon Period parameter 69
Bind Username parameter 408
browsers supported 26
Burst Data Rate parameter 132, 136, 619
Burst Real-Time Rate parameter 132, 136, 619

C

CA Server URL parameter 742
CAC 151, 152, 153, 622
configuring for 7920 phones 622
enabling 151, 152
using the CLI 152
using the GUI 151
viewing using the CLI 153
capacity adder license. See <Default Para Font>licenses 51
CCKM 595, 964
configuring 595
FlexConnect groups 964
CCX 644, 831
configuring Aironet IEs 644
using the CLI 644
described 644
link test 831

CCX *(continued)*
viewing a client's version 644
using the GUI 644
CCX Layer 2 client roaming 124, 125, 126, 127
configuring 126
using the CLI 126
debugging using the CLI 127
described 124, 125
obtaining information using the CLI 126
CCX radio management 897
features 897
flexconnect considerations 897
CCX Version parameter 644
CCXv5 Req button 278
CDP > AP Neighbors > Detail page 168
CDP > Interface Neighbors > Detail page 167
CDP > Traffic Metrics page 168
CDP Advertisement Version parameter 165
CDP AP Neighbors page 168
CDP Protocol Status parameter 165
CDP State parameter 166
Certificate Authority (CA) certificates 195, 196, 197, 415, 418
downloading 196, 197
using the CLI 196, 197
using the GUI 196
overview 195
using with local EAP 415, 418
Certificate File Name parameter 218
Certificate File Path parameter 218
Certificate Issuer parameter 417
Certificate Password parameter 194, 218
Certificate Type parameter 745
Change Rules Priority parameter 487
Channel Announcement parameter 81
Channel Assignment Leader parameter 869
Channel Assignment Method parameter 867
Channel parameter 288, 890
Channel Quiet Mode parameter 81
Channel Scan Duration parameter 872
Channel Width Parameter 869
Check Against CA Certificates parameter 417
Check Certificate Date Validity parameter 417
chokepoints for RFID tag tracking 174
CIDS Sensor Add page 510
CIDS Shun List page 510
ciphers 594, 595, 596
configuring 595, 596
described 594
Cisco 3300 Series Mobility Services Engine (MSE), using with wIPS 523
Cisco 5508 Wireless Controller 297
ports 297
Cisco 5508 WLC 315
multiple AP-manager interfaces 315
Cisco 5508 WLCs 313
multiple AP-manager interfaces 313
Cisco 7921 Wireless IP Phones 621
Cisco AV-pairs 667, 668
Cisco Centralized Key Management (CCKM). See<Default Para Font> CCKM 594
Cisco Clean Access (CCA) 674
Cisco Discovery Protocol (CDP) 163, 165, 166, 167, 169
configuring 165, 166, 167
using the CLI 166, 167
using the GUI 165, 166
described 163
enabling using the GUI 165, 166
supported devices 163
viewing neighbors 167, 169
using the CLI 169
using the GUI 167, 169
viewing traffic information 169
using the CLI 169
Cisco Discovery Protocol parameter 165
Cisco Licensing website 65
Cisco Logo parameter 223
Cisco Unified Wireless Network (UWN) Solution 5
described 5
Cisco Wireless Solution 1
described 1
Clear Filter link 550, 719, 751
Clear Stats button 997, 1000
Clear Stats on All APs button 751
CLI 31, 32, 34, 35, 49, 255
enabling wireless connections 49
logging into 32
logging out 34
navigating 34
troubleshooting commands 255
using 31, 35
Client Certificate Required parameter 417
client location, using Prime Infrastructure 7, 8
Client Protection parameter 451
client reporting 278
described 278
client roaming, configuring 127
Client Type parameter 789
clients 644, 645, 847, 848, 955
connecting to WLANs 955
viewing 847, 848
using the CLI 848
using the GUI 847, 848
viewing CCX version 644, 645
using the CLI 645
using the GUI 644
Clients > AP > Traffic Stream Metrics page 153
Clients > Detail page 789
viewing client details 789
viewing the status of workgroup bridges 789
Commands > Reset to Factory Defaults page 177
Community Name parameter 92

conditional web redirect 667
described 667
Conditional Web Redirect parameter 669
Configuration File Encryption parameter 202
configuration files 201, 202, 205
downloading 201, 202
using the GUI 201, 202
editing 205
configuration wizard 11, 23
CLI version 23
described 11
Configuration Wizard - 802.11 Configuration page 21
Configuration Wizard - Miscellaneous Configuration page 17
Configuration Wizard - Set Time page 22
Configuration Wizard - SNMP Summary page 14, 16
Configuration Wizard - System Information page 13
Configuration Wizard - Virtual Interface Configuration page 18
Configuration Wizard Completed page 23
Configuration Wizard-Management Interface Configuration 16
Configuration Wizard-System Information 15
Configure Dynamic Anchoring of Static IP Clients 1017
Using the CLI 1017
Configure option for RRM override 890
Configure RF Group 863
Using CLI 863
Configure RF Group Mode 863
Using GUI 863
Configuring a Spectrum Expert 931
Configuring ACLs - GUI 440
Configuring Cisco Cleanair 915
Using the CLI 915
Configuring Cisco CleanAir 913
Using the GUI 913
Configuring Client Exclusion Policies (CLI) 455
Configuring Client Exclusion Policies (GUI) 455
Configuring Controller (GUI) 12
Configuring Country Codes (CLI) 821
Configuring Country Codes (GUI) 820
Configuring Coverage Hole Detection on a WLAN (GUI) 670
Configuring Dynamic Anchoring of Static IP Clients 1016
Using the GUI 1016
Configuring FlexConnect APs using the CLI. 953
configuring for the debug facility 284
Configuring Sniffing on an Access Point 288
Using the GUI 288
Configuring Web Redirect (GUI) 669
Control and Provisioning of Wireless Access Points protocol (CAPWAP) 709, 710, 713, 714
debugging 714
described 709
restrictions 710
viewing MTU information 713
Controller Time Source Valid parameter 451
controllers 3, 4, 7, 8, 204, 714
configuration 204
saving 204
controllers *(continued)*
discovery process 714
multiple-controller deployment 4
overview 7
platforms 7, 8
single-controller deployment 3
core dump files 268
uploading from a 5500 series controller to a TFTP or FTP server 268
Core Dump page 266
Country Code parameter 821
country codes 819, 822
described 819
viewing using the CLI 822
Country page 821
Coverage Exception Level per AP parameter 871
coverage hole detection 670, 870, 871, 876
configuring per controller 870, 871, 876
using the CLI 876
using the GUI 870, 871
disabling on a WLAN 670
described 670
coverage hole detection and correction 861
Coverage Hole Detection Enabled parameter 671
crash files 264
uploading 264
using the CLI 264
Creating Multiple AP Manager Interfaces - CLI 340
Creating Multiple AP-Manager Interfaces (GUI) 340
Custom Signatures page 518

D

data encryption 712, 713, 779
and OfficeExtend access points 779
configuring 712, 713
using the CLI 713
using the GUI 712
Data Encryption parameter 712, 776
Data Path parameter 1005
Data Rates parameter 70
date 39
configuring through NTP server 39
DCA Channel Sensitivity parameter 868
DCA Channels parameter 869
debug commands, sending 753
debug facility 282, 283
described 282, 283
default enable password 725
Default Mobility Group parameter 992
Default Routers parameter 564
default-group access point group 652
Description parameter 400
Destination parameter 441, 959
Destination Port parameter 442, 960
Detect and Report Ad-Hoc Networks parameter 475

device certificates 193, 194
downloading 193, 194
using the GUI 193, 194
overview 193
DHCP Addr. Assignment Required parameter 560
DHCP option 43, in controller discovery process 715
DHCP option 52, in controller discovery process 715
DHCP option 82 435, 436
configuring 436
using the GUI 436
described 435
example 435
DHCP Option 82 format parameter 436
DHCP Option 82 Remote ID Field Format parameter 436
DHCP Parameters page 86, 87
DHCP proxy 85, 87
configuring 87
using the CLI 87
described 85
DHCP Scopes page 564
DHCP Server IP Addr parameter 559
DHCP servers 557
internal 557
DHCP Timeout 87
configurie using GUI 87
diagnostic channel 273
configuring 273
using the GUI 273
described 273
Diagnostic Channel parameter 273
directed roam request 125
Direction parameter 442
disabled clients, configuring a timeout 571
discovery request timer, configuring 796
distribution system ports 298
Diversity parameter 890
DNS Domain Name parameter 564
DNS IP Address parameter 758
DNS Servers parameter 564
Domain Name parameter 758
domain name server (DNS) discovery 715
Download button 194, 196, 232
downloading a CA certificate 196
downloading a customized web authentication login page 232
downloading a device certificate 194
Download File to Controller page 191, 196, 202, 231
downloading a customized web authentication login page 231
downloading CA certificates 196
downloading configuration files 202
downloading login banner file 191
Download SSL Certificate parameter 218
Download Third-Party Certificate 215, 216
using the CLI 216
using the GUI 215
DSCP parameter 442, 960
DTIM 575
DTLS 51
DTLS data encryption. See <Default Para Font>data encryption 710
DTPC Support parameter 70
Dynamic Anchoring for Clients with Static IP Addresses 1015
Configuring 1015
dynamic AP management 308, 326
for dynamic interface 326
for the management interface 308
Dynamic AP Management parameter 307, 325
for dynamic interface 325
for management interface 307
dynamic channel assignment (DCA) 859, 869, 870, 874, 876
40-MHz channelization 869
configuring 870, 874, 876
using the CLI 874, 876
using the GUI 870
described 859
dynamic interface example 314
dynamic transmit power control, configuring 70
Dynamic WEP Key Index parameter 416

E

EAP Profile Name parameter 418
EAP-Broadcast Key Interval 416
EAPOL-Key Max Retries parameter 416
EAPOL-Key Timeout parameter 416
EDCA Profile parameter 160
Edit QoS Profile page 132
Edit QoS Role Data Rates page 136
Egress Interface parameter 243
Email Input parameter 243
Enable AP Local Authentication parameter 967
Enable Check for All Standard and Custom Signatures parameter 519
Enable Counters parameter 440
Enable Coverage Hole Detection parameter 870
Enable CPU ACL parameter 443
Enable CPU IPv6 ACL 443
Enable DHCP Proxy parameter 86
Enable Dynamic AP Management parameter 340
Enable EAP-FAST Authentication parameter 967
Enable LEAP Authentication parameter 967
Enable Least Latency Controller Join parameter 777
Enable Link Latency parameter 777, 836
Enable Low Latency MAC parameter 161
Enable LSC on Controller parameter 742
Enable NAT Address parameter 306
Enable OfficeExtend AP parameter 776
Enable Password parameter 727
Enable Server Status parameter 408
Enable Tracking Optimization parameter 825
Encryption Key parameter 604
end-user license agreement (EULA) 54, 55
enhanced distributed channel access (EDCA) parameters 161
configuring using the CLI 161

enhanced neighbor list 124
described 124
request (E2E) 124
Enter Saved Permission Ticket File Name parameter 66
EoIP port 1013
epings 1014
error codes, for failed VoIP calls 630
Ethernet connection, using remotely 34
evaluation licenses 52
installed on 5508 WLCs 52
Expedited Bandwidth parameter 149
Expiration Timeout for Rogue AP and Rogue Client Entries parameter 474
Extensible Authentication Protocol (EAP) 418, 419, 421
setting local timers 418, 419
timeout and failure counters 421
per access point 421
per client 421

F

factory default settings 177
resetting using the GUI 177
failover priority for access points 811, 812
configuring 811, 812
using the CLI 812
using the GUI 811
described 811
viewing using the CLI 812
failover protection 9, 10
Fallback Mode parameter 370
fast heartbeat timer 793, 794, 796
configuring 794, 796
using the CLI 796
using the GUI 794
described 793
fast SSID changing 99
configuring using the GUI 99
fault tolerance 937
File Compression parameter 755
File Name to Save Credentials parameter 65
file transfers 9
File Type parameter 181, 191, 193, 196, 198, 200, 202, 231, 270
downloading a CA certificate 196
downloading a configuration file 202
downloading a customized web authentication login page 231
downloading a device certificate 193
Login Banner 191
upgrading controller software 181
uploading a configuration file 200
uploading packet capture files 270
uploading PACs 198
filter, using to view clients 847, 848
Fingerprint parameter 510
FlexConnect 939, 940, 942, 949, 954
authentication process 939, 942
FlexConnect *(continued)*
bandwidth restriction 940
debugging 949, 954
FlexConnect groups 963, 964, 965
backup RADIUS server 964
CCKM 964
described 963
local authentication 965
FlexConnect Mode AP Fast Heartbeat Timeout parameter 794
Fragmentation Threshold parameter 70

G

General (controller) page 335, 884
configuring an RF group 884
enabling link aggregation 335
General (security) page 397
General page 415
Generate Rehost Ticket button 66
generating CSR 213
Global AP Failover Priority parameter 811
Global Configuration page 794, 811
configuring backup controllers 794
configuring failover priority for access points 811
global credentials for access points 727
overriding 727
using the CLI 727
using the GUI 727
Group Mode parameter 885, 995, 999
Group Name parameter 966, 993
Guest LAN parameter 242
guest user accounts 210
viewing 210
using the CLI 210
using the GUI 210
Guest User parameter 400
Guest User Role parameter 400
guest WLAN, creating 209
GUI 25, 26
guidelines 26
using 25
Guidelines and Limitations for Predownloading 187

H

Headline parameter 223
hex2pcap sample output 285
Holdtime parameter 165
HTTP Access parameter 27
HTTP Configuration page 27
HTTPS Access parameter 27
Hysteresis parameter 126

I

Identity Request Max Retries parameter 415
Identity Request Timeout parameter 415
IDS sensors 509
  described 509
IDS signatures 515, 519, 521
  described 515
  frequency 519
  MAC frequency 519, 521
  measurement interval 519
  pattern 519
  quiet time 519, 521
  tracking method 519
IGMP Snooping 681
IGMP Timeout parameter 107
IKE Diffie Hellman Group parameter 370
IKE Phase 1 parameter 370
Index parameter for IDS 510
Ingress Interface parameter 243
Injector Switch MAC Address parameter 843
inline power 841
Install License button 54
inter-controller roaming 123
  described 123
inter-release mobility 991
inter-subnet roaming 124
  described 124
Interface groups 344
Interface Name parameter 654, 675, 676
Interface parameter 559
interfaces 300, 323
  overview 300, 323
Interfaces > Edit page 340
  creating multiple AP-manager interfaces 340
interference 860
Interference threshold parameter 871
Interferences 906
Internal DHCP server 563
  described 563
Internet Group Management Protocol (IGMP) 104, 107, 108
  configuring 107, 108
    using the CLI 108
    using the GUI 107
  snooping 104
Interval parameter 868
intra-controller roaming 123
  described 123
Inventory page 829
Invoke Channel Update Now button 868
Invoke Power Update Now button 865
IP address-to-MAC address binding 129
  described 129
IP Mask parameter 92
IPSec parameter 369
IPv6 ACL Name 443

J

Japanese country codes 820

K

Keep Alive Count parameter 1005
Keep Alive Interval parameter 1005
Key Encryption Key (KEK) parameter 369
Key Index parameter 604
key permutation 603, 604, 605
  configuring 604, 605
  described 603
Key Size parameter 604
Key Wrap Format parameter 369
Key Wrap parameter 369

L

LAG Mode on Next Reboot parameter 335
Last Auto Channel Assignment parameter 869
Layer 2 6
  operation 6
Layer 2 Security parameter 595, 604, 669
Layer 3 6, 364
  operation 6
  security 364
    described 364
Layer 3 Security parameter 243, 608, 614, 669
  for VPN passthrough 614
  for web authentication 608
  for web redirect 669
  for wired guest access 243
LDAP 409
  choosing server priority order 409
  configuring 409
    using the GUI 409
LDAP server 409
  assigning to WLANs 409
LDAP Servers page 408
LDAP Servers parameter 418
Lease Time parameter 564
LEDs 249, 850
  configuring 850
  interpreting 249
License Commands page 54
License Detail page 55, 60
licenses 52, 53, 54, 55, 56, 64, 65, 66, 67
  installing 54, 55
    using the CLI 54, 55
    using the GUI 54
  obtaining 52, 54
  rehosting 64, 65, 66
    described 64
    using the GUI 65, 66

licenses *(continued)*
removing 55
using the CLI 55
using the GUI 55
saving 54, 55
using the CLI 55
using the GUI 54
SKUs 53
transferring to a replacement controller after an RMA 67
viewing 56
using the CLI 56
Licenses page 55, 60
Lifetime parameter 209, 400
lightweight mode, reverting to autonomous mode 739
link aggregation (LAG) 333, 334
described 333
illustrated 334
link latency 779, 835
and OfficeExtend access points 779
described 835
Link Status parameter 329
link test 831, 832
performing 832
using the CLI 832
using the GUI 832
types of packets 831
Link Test 832
button 832
option 832
Link Trap parameter 329
load-based CAC 146, 149
described 146
enabling 149
using the GUI 149
Lobby Ambassador Guest Management > Guest Users List page 209
Local Auth Active Timeout parameter 415
Local Authentication on a WLAN 954
using the GUI 954
local authentication, local switching 940
local EAP 414, 420, 422
debugging 422
example 414
viewing information using the CLI 420
Local EAP Authentication parameter 418
Local Management Users > New page 208
Local Management Users page 208
Local Mode AP Fast Heartbeat Timer parameter 794
Local Net Users > New page 400
local significant certificate (LSC) 741, 743
configuring 741, 743
using the GUI 741, 743
described 741
Local Significant Certificates (LSC) - AP Provisioning page 742
Local Significant Certificates (LSC) - General page 742
local user database, capacity 207
location 898
calibration 898
login banner file 190, 191, 192, 193
clearing 192, 193
described 190
downloading 191, 192
using the CLI 192
using the GUI 191
logs 264, 265, 280
RSNA 280
uploading 264, 265
using the CLI 265
using the GUI 264
LWAPP-enabled access points 739, 740, 753, 754, 755, 757
debug commands 753
disabling the reset button 757
retrieving radio core dumps 753
reverting to autonomous mode 739, 740
sending crash information to controller 753
uploading 754, 755
access point core dumps 755
radio core dumps 754, 755

M

MAC address of access point 757
displayed on controller GUI 757
MAC filtering 567, 571
configuring on WLANs 567, 571
Management Frame Protection parameter 451
management interface 305
described 305
Management IP Address parameter 776
management over wireless 431
described 431
Master Controller Configuration page 716
Master Controller Mode parameter 716
Max RF Bandwidth parameter 149, 151
Max-Login Ignore Identity Response parameter 416
maximum local database entries 397
configuring using the GUI 397
Maximum Local Database Entries parameter 397
MCS data rates 77
Member MAC Address parameter 993
memory 9
types 9
memory leaks, monitoring 271
Message Authentication Code Key (MACK) parameter 369
message logs 255, 258, 262
configuring 255
using the GUI 255
viewing 258, 262
using the CLI 262
using the GUI 258
Message parameter for web authentication 223

Metrics Collection parameter 150
MFP Client Protection parameter 451
MIC 603
Min Failed Client Count per AP parameter 871
Minimum RSSI parameter 125
MMH MIC 604, 605
configuring 604, 605
Mobility Anchor Create button 1005
Mobility Anchors option 1005
mobility anchors. See <Default Para Font>auto-anchor mobility 1003
mobility groups 881, 987
difference from RF groups 881
illustrated 987
mobility ping tests, running 1013
MODE access point button 757
Mode parameter 125, 898
monitor intervals, configuring using the GUI 872
Monitoring 926
mpings 1014
multicast client table, viewing 110
Multicast Groups page 109
multicast mode 103, 105, 106
described 103, 105
guidelines 106
Multicast Optimization 349
Multicast page 107
Multicast VLAN 349
using the GUI 349
multiple country codes 821, 822
configuring 821, 822
using the CLI 822
using the GUI 821

N

NAC in-band mode 674
NAC out-of-band integration 673, 675
diagram 675
guidelines 673
NAC out-of-band support 676, 677
configuring for a specific access point group 676, 677
using the CLI 677
using the GUI 676
NAC State parameter 676
NAT address 306, 309, 325, 326
for dynamic interface 325, 326
for management interface 306, 309
Native VLAN ID parameter 950
Neighbor Discovery Packet 861, 879
Neighbor Packet Frequency parameter 872
Netbios Name Servers parameter 564
Netmask parameter 564
Network Mobility Services Protocol (NMSP) 174
Network parameter 564
New Mobility: GUI configuration 1030
NTP/SNTP server 40
configuring to obtain time and date 40
Number of Attempts to LSC parameter 742
Number of Hits parameter 442

O

OfficeExtend Access Point Home page 781
OfficeExtend access points 765, 766, 774, 776, 778, 782
and NAT 766
configuring 776, 778, 782
a personal SSID 782
using the GUI 776, 778
described 765
firewall requirements 774
supported access point models 766
typical setup 765
viewing statistics 782
OfficeExtend Access Points 292
LEDs 292
positioning 292
OfficeExtend AP parameter 777
online help, using 26
operating system 5
security 5
software 5
Order Used for Authentication parameter 371, 391
Over-ride Global Credentials parameter 727, 731, 732, 777
Override Global Config parameter 234, 243
Override Interface ACL parameter 444
Overview of CleanAir 905

P

P2P Blocking parameter 578
packet capture files 268, 269, 270, 271
described 268
sample output in Wireshark 269
uploading 270, 271
using the CLI 270, 271
Params parameter 742
Passive clients 679
password guidelines 731
Password parameter 198, 400, 726, 731
for access point authentication 731
for access points 726
for local net users 400
for PACs 198
passwords 255
viewing in clear text 255
PEAP parameter 416
peer-to-peer blocking 577
described 577
Physical Mode parameter 329
Physical Status parameter 329

ping link test 831
ping tests 1013
PMK cache lifetime timer 596
PMKID caching 596
PoE Status parameter 843
Pool End Address parameter 564
Pool Start Address parameter 564
Port Number parameter 242, 329, 369, 391, 408
  for controller 329
  for LDAP server 408
  for RADIUS server 369
  for TACACS+ server 391
  for wired guest access 242
Port parameter for IDS 510
ports 329
  configuring 329
Ports page 329
Power Injector Selection parameter 843
Power Injector State parameter 843
Power Neighbor Count parameter 865
Power over Ethernet (PoE) 9, 843, 844
  configuring 843, 844
    using the CLI 844
    using the GUI 843, 844
  described 9
Power Over Ethernet (PoE) parameter 330
Power Threshold parameter 865
preauthentication access control list (ACL) 229, 946
  for external web server 229, 946
Preauthentication ACL parameter 444, 669
Predownloading an image 185
Primary Controller parameters 795
Primary RADIUS Server parameter 966
Priority Order > Local-Auth page 415
Priority Order > Management User page 371, 391
Privacy Protocol parameter 212
proactive key caching (PKC), with mobility 990
probe requests, described 827
product authorization key (PAK) 52, 53
  obtaining for license upgrade 52
  registering 53
Profile Name parameter 243, 548, 648, 783
protected access credentials (PACs) 197, 198, 199, 415, 968
  overview 197
  uploading 198, 199
    using the CLI 198, 199
    using the GUI 198
  using with local EAP 415, 968
Protection Type parameter 451, 887
Protocol parameter 441, 960
Protocol Type parameter 133
PSK 594
  described 594
PSK Format parameter 595

Q

QBSS 622
QoS 131, 617
  levels 131, 617
QoS profiles 132, 133, 134, 617
  configuring 132, 133, 134, 617
    using the CLI 133, 134
    using the GUI 132, 133, 617
QoS roles 135, 136
  configuring 135, 136
    using the CLI 136
    using the GUI 135, 136
Quality of Service (QoS) parameter 618
Quarantine parameter 324, 675
  for dynamic interface 324
  NAC out-of-band integration 675
quarantined VLAN 325, 676, 942, 947
  configuring 325
  using 947
  with FlexConnect 942
  with NAC out-of-band integration 676
Query Interval parameter 510

R

radio core dumps 753, 754
  described 753
  uploading 754
    using the GUI 754
radio measurement requests 897, 898, 899
  configuring 898, 899
    on the CLI 899
    on the GUI 898
  overview 897
  viewing status using the CLI 899
radio resource management (RRM) 861, 864, 867, 870, 872, 877, 883, 886, 889, 890, 895, 897
  CCX features. See <Default Para Font>CCX radio management 897
  configuring 872
    monitor intervals using the GUI 872
  coverage hole detection 861, 870
    configuring per controller using the GUI 870
    described 861
  debugging 877
  disabling dynamic channel and power assignment 895
    using the CLI 895
  overriding RRM 889
  specifying channels 867, 870
  statically assigning channel and transmit power settings 890
    using the GUI 890
  update interval 883, 886
  Wireless > 802.11a/n (or 802.11b/g/n) > RRM > TPC parameter 864

radio resource management (RRM) settings 877
viewing using the CLI 877
radio resource monitoring 858
RADIUS 372, 374, 964
FIPS standard 372
KEK parameter 372
MACK parameter 372
server fallback behavior 374
using FlexConnect 964
RADIUS authentication attributes 376
RADIUS authentication attributes, Airespace 378
rc4-preference, configuring for web administration 28
Re-sync button 511
Redirect URL After Login parameter 223
Refresh-time Interval parameter 165
Regenerate Certificate button 218
Rehost Ticket File Name parameter 66
rehosting a license. See <Default Para Font>licenses 64
Remote Authentication Dial-In User Service. See<Default Para Font>
RADIUS 365
Request Max Retries parameter 416
Request Timeout parameter 416
Reserved Roaming Bandwidth parameter 149
Reset Link Latency button 836
Reset Personal SSID parameter 776
resetting the controller 206
RF Channel Assignment parameter 894
RF group leader 882
described 882
RF group name 883
described 883
RF Group support 883
RF groups 881, 882, 883, 884, 885
cascading 882
configuring 884
using the GUI 884
overview 881, 883
pinning 882
viewing status 885
using the CLI 885
using the GUI 885
RF-Network Name parameter 884
RFID tags 173, 175
described 173
tracking 175
debugging using the CLI 175
RFID tracking on access points, optimizing 826
using the GUI 826
RLDP. See <Default Para Font>Rogue Location Discovery Protocol
(RLDP) 472
roam reason report 125
roaming and real-time diagnostics 279, 280
described 279
logs 279, 280
described 279
viewing 280
rogue access points 475, 478, 887
alarm 887
automatically containing 475, 478
using the CLI 478
using the GUI 475
rogue detection 476, 778
and OfficeExtend access points 778
Rogue Detection parameter 474, 776
Rogue Location Discovery Protocol parameter 474
Rogue Policies page 474
rogue states 483
Role Name parameter 136
Role of the Controller 906
Role parameter 400
RRM. See <Default Para Font>radio resource management (RRM) 857
RSNA logs 279, 280
configuring 280
described 279

S

Save and Reboot button 196
Save Licenses button 54
saving configuration settings 204
Scan Threshold parameter 126
Scope Name parameter 564
SE-Connect 932
Search AP window 722, 751
Search WLANs window 550, 717
Secondary Controller parameters 795
Secondary RADIUS Server parameter 966
security 363
overview 363
Select APs from Current Controller parameter 967
self-signed certificate (SSC) 740
used to authorize access points 740
Sequence parameter 441, 959
serial number for controller, finding 66
serial number of controller, finding 65
Server Address parameter 510
Server Index (Priority) parameter 368, 390, 408
Server IP Address parameter 288, 368, 390, 408
for LDAP server 408
for RADIUS server 368
for TACACS+ server 390
for wireless sniffer 288
Server Key parameter 417, 968
Server Status parameter 369, 391
Server Timeout parameter 369, 391, 409
service port 299
service-port interface 307, 318, 319
configuring 307, 318
using the GUI 307, 318
described 319
Set Priority button 60

Set to Factory Default button 872
Severity Level Filtering parameter 256
Shared Secret Format parameter 368, 390
Shared Secret parameter 368, 391
Short Preamble Enabled parameter 423
shunned clients 509
described 509
Signature Events Summary page 520
Sniff parameter 288
sniffing. See <Default Para Font>wireless sniffing 287
SNMP engine Id 91
SNMP NAC State parameter 654
SNMP Trap Receiver 94
SNMP v1 / v2c Community page 91
SNMP v3 users 212, 213
changing default values using the GUI 212, 213
SNMP V3 Users page 212
SNMP, configuring 91
software, upgrading 179, 180, 182
guidelines 179
using the CLI 182
using the GUI 180
Source parameter for ACLs 441, 959
SpectraLink NetLink phones 423
overview 423
Spectrum Expert 931
configuring using GUI 931
Splash Page Web Redirect parameter 669
SSH 46, 48, 289, 777, 779
and OfficeExtend access points 777, 779
configuring 46
using the CLI 46
troubleshooting access points 48, 289
using the GUI 48, 289
SSH parameter 48, 290
SSID 547, 548, 549
configuring 548, 549
using the CLI 549
using the GUI 548
described 547
SSL certificate 29, 30
loading 29, 30
using the CLI 30
using the GUI 29, 30
SSL Protocol 27
SSLv2 for web authentication, disabling 223
SSLv2, configuring for web administration 28
State parameter 510, 519
stateful DHCPv6 IP addressing 637
static CAC 146, 150
described 146
enabling 150
using the CLI 150
Static CAC 149
enabling 149
using the GUI 149
static IP address 758
configuring 758
using the GUI 758
Static IP address 757
described 757
Static IP parameter 758
Status parameter 92, 243, 548, 564, 649, 783
for DHCP scopes 564
for guest LANs 243
for SNMP community 92
for WLANs 548, 649, 783
Summary page 46
Switch IP Address (Anchor) parameter 1005
symmetric mobility tunneling 1011, 1012
illustrated 1011
overview 1011
verifying status 1012
using the CLI 1012
Symmetric Mobility Tunneling Mode parameter 1012
syslog 280, 281
described 280
logs 280, 281
Syslog Configuration page 256
Syslog Facility parameter 257
syslog server 256
removing from controller 256
severity level filtering 256
Syslog Server IP Address parameter 256
system logging 255
configuring 255
using the GUI 255
system logs, viewing using the CLI 262
System Messages 250
System Resource Information page 253
system resources 253, 254
viewing using the CLI 254
viewing using the GUI 253

T

TACACS+ 387, 388, 392
accounting 388
authentication 387
authorization 387
configuring 392
using the GUI 392
described 387
TACACS+ (Authentication, Authorization, or Accounting) Servers > New page 390
TACACS+ (Authentication, Authorization, or Accounting) Servers page 390
TACACS+ Administration .csv page (on CiscoSecure ACS) 393, 395
Telnet 48, 289, 290
troubleshooting access points 48, 289, 290
using the CLI 48, 290
using the GUI 48, 289, 290

Telnet parameter 48, 290
Telnet sessions 44, 46
configuring 44, 46
using the GUI 44, 46
Telnet-SSH Configuration page 45
Tertiary Controller parameters 795
text2pcap sample output 286
Time to Live for the PAC parameter 417, 968
time zone 41, 42
configuring using the CLI 42
configuring using the GUI 41
time-length-values (TLVs), supported for CDP 163, 164
time, configuring 39
using the NTP server 39
timestamps, enabling or disabling in log and debug messages 262
traffic specifications (TSPEC) request 146
examples 146
traffic stream metrics (TSM) 148, 153, 154, 155
described 148
viewing statistics 153, 154, 155
using the CLI 154, 155
using the GUI 153
Transfer Mode parameter 181, 194, 196, 198, 200, 202, 231, 270
downloading a CA certificate 196
downloading a configuration file 202
downloading a customized web authentication login page 231
downloading a device certificate 194
upgrading controller software 181
uploading a configuration file 200
uploading a PAC 198
uploading packet capture files 270
Transition Time parameter 126
transmit power 891
statically assigning using the CLI 891
statically assigning using the GUI 891
transmit power levels 891
transmit power threshold, decreasing 873
trap logs 775
for OfficeExtend access points 775
Trap Logs page 626
troubleshooting 254, 272, 748, 753
access point join process 748, 753
CCXv5 clients 272
problems 254
Troubleshooting OEAPs 292
tunnel attributes and identity networking 463
Tx Power Level Assignment parameter 894
Type parameter 243, 548, 648, 783

U

U-APSD 147, 153, 154
described 147
viewing status 153, 154
using the CLI 154
U-APSD *(continued)*
viewing status *(continued)*
using the GUI 153
UDP port 1013
UDP, use in RADIUS 366
unicast mode 103
unique device identifier (UDI) 829, 830
described 829
retrieving 829, 830
using the CLI 830
using the GUI 829, 830
Upload button 198, 264, 270, 518
Upload CSV File parameter 967
Upload File from Controller page 198, 200, 270, 754
USB console port, using on a 5500 series controller 331, 332
Use AES Key Wrap parameter 368
User Access Mode parameter 208
User Attribute parameter 409
User Base DN parameter 408
User Credentials parameter 409
User Name parameter 400
User Object Type parameter 409
User parameter 198
User Profile Name parameter 212
Username parameter 726, 731
Using CLI to monitor the Air quality 927
Using GUI to monitor air quality 926
Using OpenSSL 213
using the GUI 443

V

Validate Rogue Clients Against AAA parameter 474
Validity parameter 198
VCI strings 748
Verify Certificate CN Identity parameter 417
virtual interface 317
described 317
VLAN ID parameter 675, 951
VLAN Identifier parameter 312, 325
for AP-manager interface 312
for dynamic interface 325
VLAN Select 343
VLANs 303, 323
described 323
guidelines 303
Voice RSSI parameter 871
voice settings 150
configuring 150
using the GUI 150
voice-over-IP (VoIP) telephone roaming 124
VoIP calls, error codes 630
VoIP snooping 625
described 625
VoIP Snooping and Reporting parameter 626

VPN passthrough 614
configuring using the GUI 614

W

Web Auth Type parameter 234, 243
web authentication 217, 218, 220, 222, 223, 608
certificate 217, 218
obtaining using the GUI 217, 218
configuring a WLAN for 608
using the GUI 608
described 220
process 223
successful login page 222
web authentication login page 222, 224, 225, 229, 232
choosing the default 224, 225
using the CLI 224, 225
customizing from an external web server 229
using the GUI 229
default 222
modified default example 229
previewing 224, 232
Web Authentication Type parameter 223, 230, 232
Web Login page 230
web mode 27
described 27
Web Policy parameter 444, 669
Web Session Timeout parameter 27
web-browser security alert 221
webauth bundle 230
webauth.tar files 234
WEP keys, configuring 582
WGB parameter 789
WGB Wired Clients page 789
wired guest access 241, 242
configuration overview 242
described 241
wireless intrusion prevention system (wIPS) 523
described 523
wireless sniffing 288
configuring 288
using the GUI 288
supported software 288
WLAN ID parameter 548, 648, 783
WLAN mobility security values 1009
WLAN Profile parameter 400
WLAN SSID parameter 209, 654, 676
configuring for guest user 209
mapping an access point group to a WLAN 654, 676
WLANs 547, 548, 549, 571, 582, 649, 783, 955
checking security settings 582
connecting clients to 955
creating 649, 783
using the GUI 649, 783
deleting 547, 549
using the CLI 549
using the GUI 547
enabling or disabling 548, 549
using the CLI 549
using the GUI 548
session timeout 571
described 571
viewing 549
using the CLI 549
WLANs > Edit (Advanced) page 273, 670
configuring the diagnostic channel 273
WLANs > Edit (Security > AAA Servers) page 234, 670
choosing RADIUS or LDAP servers for external authentication 234
disabling accounting servers on a WLAN 670
WLANs > Edit (Security > Layer 3) page 669
configuring web redirect 669
WLANs > Edit page 243, 548, 648, 783
WLANs page 547, 548, 554, 648, 783, 1005
WMM 145, 622, 623
configuring 623
described 622
with CAC 145
WMM parameter 161
workgroup bridges (WGBs) 766, 776, 785, 788, 789
debugging 789
described 785
illustrated 766, 776, 785
sample configuration 788
viewing status 789
using the CLI 789
using the GUI 789
world mode 70, 71
WPA2 Policy parameter 595
wplus license. licenses 51
wplus license. See <Default Para Font>licenses 51